# LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

*DISCLAIMER*

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

*Date of last check: 26 June 2026*

On the basis of Article 82 paragraph 1 item 2 and Article 91 paragraph 1 of the Constitution of Montenegro, Parliament of Montenegro of the 28th convocation, at the Fifth Sitting of the Second Ordinary (Autumn) Session in 2023, on 11 December 2023, adopted the

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

## I. BASIC PROVISIONS

### Subject matter

### Article 1

This Law shall regulate measures and actions undertaken for the purpose of preventing and detecting money laundering and terrorist financing, as well as the tasks, powers and manner of operation of the organisational unit within the organisational unit of the state administration authority responsible for internal affairs which performs police affairs (hereinafter referred to as: Police), which performs tasks relating to the prevention and detection of money laundering and terrorist financing (hereinafter referred to as: Financial Intelligence Unit), and other matters of importance for preventing and detecting money laundering and terrorist financing.

### Money Laundering
### Article 2

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 1)*

[1] Official Gazette of Montenegro 110/23 of 12 December 2023, 065/24 of 5 July 2024, 024/25 of 12 March 2025, 041/26 of 24 March 2026 and 059/26 of 4 May 2026

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

1) conversion or transfer of money or other property, knowing that such money or other property were derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person involved in the commission of such activity to evade the legal consequences of the actions of that person;

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

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

4) participation in, association for the purpose of committing, attempt to commit and aiding, abetting, facilitating and counselling the commission of the acts referred to in items 1, 2 and 3 of this paragraph.

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

Activities referred to in paragraph 1 of this Article shall also be considered money laundering when the money or other property subject to money laundering was acquired in the territory of another country, provided that the activities through which it was acquired would constitute criminal activity in Montenegro or another country.

## Terrorist Financing

### Article 3

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 1)*

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

providing, making available or collecting funds or property, in any way, directly or indirectly, with the intention that they be used or knowing that they will be used, in whole or in part, for the commission of a terrorist act, or attempting to provide, make available or collect funds or property, in any way, directly or indirectly, with the intention that they be used or knowing that they may be used, in whole or in part:

for preparing or committing a terrorist act within the meaning of this Law,

for financing organisations whose aim is to commit the acts referred to in indent 1 of this item or members of those organisations or individuals whose aim is to commit such acts, or

- for financing travel by natural persons for the purpose of committing, planning, preparing or participating in terrorist acts, or for providing or attending training for the commission of a terrorist act, or

by terrorists or by terrorist organisations for any purpose;

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

## Obliged entities

### Article 4

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 2)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 1)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 2)*

Measures for preventing and detecting money laundering and terrorist financing shall be implemented prior to, during and after the completion of all operations involving the receipt, investment, conversion, safekeeping or other disposal of money or other property, or transactions.

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

1) credit institutions and branches of foreign credit institutions;

2) entities carrying out the following activities:

- purchase of claims;
- financial leasing;
- renting safe-deposit boxes;
- factoring;
- issuance of guarantees and other sureties;
- granting loans and providing credit intermediation where the entity manages the loan funds;
- exchange services;

3) payment service providers and institutions dealing with electronic money in line with the law regulating provision of payment services and issuance of electronic money;

4) Post of Montenegro;

5) companies for the management of investment funds;

6) pension fund management companies;

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

- investment services on the capital market in Montenegro which include: the reception and transmission of orders in relation to one or more financial instruments; the execution of orders on behalf of customers; dealing on own account; portfolio management; investment advice; underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis; placing of financial instruments without a firm commitment basis; operation of multilateral trading facility (hereinafter referred to as: “the MTF”) as well as the operation of organised trading facility (hereinafter referred to as:“the OTF”),
- ancillary services on the capital market in Montenegro which include: safekeeping and administration of financial instruments for the account of customers, including custodianship and related services such as cash/collateral management; granting credits or loans to an investor to allow him to carry out a transaction in one or more financial instruments, where the transaction involves the company which grants credit or loan; providing general recommendations on capital structure, business strategy and related matters and services relating to mergers and acquisitions of holdings in companies; foreign exchange services where these are connected to the provision of investment services; research and financial analysis or other forms of 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 services related to underlying assets contained in financial derivatives, if connected with investment and ancillary services;

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

9) insurance brokerage companies, insurance agency companies and sole proprietors – insurance agents, in respect of life insurance;

10) organisers of games of chance;

11) pawnshops;

12) crypto-asset service providers;

13) legal persons, business organisations, sole proprietors and natural persons carrying out activities or business involving:

- forfaiting;
- auditing, activities of a certified auditor, accounting and provision of tax advisory services, or undertaking to provide, directly or through other related persons, material or other assistance or advice on tax matters;
- providing services of founding legal persons and other business organisations, as well as business or fiduciary services;
- management of property for third persons;
- renting and mediation in renting real estate in transactions where the monthly rent is EUR 10,000.00 or more or the equivalent of this value;
- construction of residential and commercial buildings, construction or assembly of prefabricated residential and commercial buildings;
- issuance and management of payment instruments (e.g. cheques, traveller's cheques, credit cards, bank promissory notes, payment orders, debit cards), which are not considered payment instruments in line with the law governing payment operations;
- granting loans and mediation in contracting granting loans activities;
- investment, trade and mediation in real estate trade;
- trade of motor vehicles if the payments are made or received in the amount of EUR 10,000.00 or more, regardless of whether it is one transaction or several linked transactions;
- trade of vessels and aircraft, as well as related service activities, if the payments are made or received in the amount of EUR 10,000.00 or more regardless of whether it is a single transaction or several linked transactions;
- trade or intermediation in trade, including organising and conducting auctions, in cultural property, precious metals and precious stones, products made of precious metals and precious stones, wristwatches and clocks, where payments are made or received in the amount of EUR 10,000 or more, whether in a single transaction or several linked transactions;
- storage or safekeeping of cultural property, or trade or intermediation in trade in cultural property, where such activities are carried out in ports, free zones or warehouses and payments are made or received in the amount of EUR 10,000 or more, whether in a single transaction or several linked transactions;

14) founders and operators of free zones and port operators within free zones.

For the purposes of this Law, a lawyer shall also be considered an obliged entity when:

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

- purchasing or selling of real estate or a business organisation,
- managing money, securities or other property of a customer,
- opening or managing a bank account, savings deposit or the account for dealing with securities,
- collecting funds for founding, dealing with or managing a business organisation,
- founding, dealing with or managing an institution, fund, business organisation or other similar form of organisation;

2) Executing a financial transaction or transaction concerning real estate in the name and for the account of a customer.

For the purposes of this Law, a notary shall also be considered an obliged entity when preparing notarial acts and certifying documents related to the activities referred to in paragraph 3 of this Article, as well as documents related to a loan agreement.

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

Government may exempt organisers of certain games of chance, except for casinos, from the obligation to apply all or certain measures and actions defined by this Law in respect of a specific part of their business or activity when, following a risk assessment, a lower risk of money laundering and terrorist financing has been established.

Risk assessment referred to in paragraph 6 of this Article shall be based on the nature, manner of carrying out the activity, payment methods and volume of business of the entities referred to in paragraph 6 of this Article.

## Exceptions to the Application

### Article 4a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 2)*

Provisions of this Law governing 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 participating in liquidation or bankruptcy proceedings, except in the case of a plan to support the orderly redemption of any asset-referenced token applied in the event of bankruptcy, liquidation, resolution or withdrawal of the authorisation of the holder;
3) European Central Bank, the central bank of a European Union Member State when acting in its capacity as a monetary authority and other public authorities of EU Member States;
4) European Investment Bank and its subsidiaries;
5) European Financial Stability Facility and the European Stability Mechanism;
6) international organisations within the meaning of public international law.

## Use of Gender-Sensitive Language

**Article 5**

Terms used in this Law for natural persons in the masculine gender shall also include the corresponding terms in the feminine gender.

**Definitions**

**Article 6**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 3)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 3)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 3)*

Terms used in this Law shall have the following meanings:

1) terrorist act shall be an act defined in the Protocols listed in the Annex to the International Convention for the Suppression of the Financing of Terrorism, as well as the criminal offence of terrorism and criminal offences related to terrorism prescribed by the Criminal Code of Montenegro, and any other act intended to cause death or serious bodily injury to a civilian or any other person who does not actively participate in hostilities in a situation of armed conflict, where 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 organisation to do or abstain from doing any act;

2) terrorist is a person who:

- alone or with other persons intentionally attempts to commit or commits a terrorist act by any means, directly or indirectly,
- alone or with other persons intentionally incites 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 organisation shall be a group of two or more persons or terrorists, established for a longer period and acting in an organised manner for the purpose of committing criminal offences of terrorism, whose members 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 inciting or assisting in the commission of a terrorist act,
- for the purpose of organising 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 shall be any criminal offence whose commission resulted in the acquisition of proceeds which may be the subject of the criminal offence of money laundering;

5) financial sector, for the purposes of this Law, shall comprise obliged entities referred to in Article 4 paragraph 2 items 1 to 9 and item 12 of this Law;

5a) non-financial sector, for the purposes of this Law, shall comprise obliged entities referred to in Article 4 paragraph 2 items 10, 11, 13 and 14 and paragraphs 3 and 4 of this Law;

6) customer shall be a domestic or foreign legal person, business organisation, sole proprietor, natural person, trust, other person or an entity equivalent to it to which an obliged entity provides services in the course of its professional activity or with which it establishes a business relationship or carries out a transaction;

7) other person or an equivalent entity shall be a person that pools or will pool money or other property for a specific purpose;

8) compliance officer for the prevention of money laundering and terrorist financing shall be a person designated by an obliged entity, with powers and responsibilities for implementing measures and actions undertaken for the purpose of preventing and detecting money laundering and terrorist financing;

9) credit institution means a business organisation established and operating in line with the law governing credit institutions;

10) financial institution shall be an obliged 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 its registered office is in Montenegro, a Member State of the European Union or another country;

11) financial group means a group consisting of:

- the parent company with registered office in Montenegro, subsidiaries and companies in which these companies have a direct or indirect participation in the capital or voting rights of at least 20% and are included in the annual consolidated financial statement in line with the law,
- companies that are interconnected by joint management,
- legal or natural persons who have a direct or indirect participation in the capital or voting rights of at least 20% in legal persons from the financial sector;

12) reasons for suspicion shall be a set of facts and circumstances based on the lists of indicators referred to in Articles 82 and 83 of this Law or on information from publicly available sources or observations, on the basis of which a natural person may suspect, assume or reasonably conclude that a certain transaction, funds or other property do not originate from lawful sources, that such funds or other property do not constitute lawfully acquired property or that they are intended for purposes punishable by law;

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

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

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

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

17) collective custody account shall be an account opened by a participant member (user of the clearing and settlement system) in the system of the Central Clearing and Depository Company in the course of providing ancillary services in line with the law governing the capital market, in which the ownership positions of individual owners, customers of the participant member, are recorded as a single aggregate position;

18) transaction shall mean receiving, investing, converting, safekeeping or otherwise disposing of money or other property;

18a) payment transaction shall mean the payment, withdrawal or transfer of funds initiated by the payer, on behalf of the payer or by the payee, regardless of the obligations between the payer and the payee;

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

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

21) suspicious transaction shall be any transaction or attempted transaction involving funds or property for which it is assessed, on the basis of indicators for recognising suspicious customers and transactions in line with this Law, bylaws adopted under this Law and the internal acts of obliged entities or on the basis of other objective circumstances and facts, that there are reasons for suspicion that such funds or property constitute proceeds of crime, are subject to money laundering or are intended for terrorist financing;

21a) suspicious business shall be a set of transactions (which are not individually suspicious transactions) or activities carried out by a customer in relation to funds or other property, in respect of which an obliged entity, having analysed all relevant facts, including the characteristics of the customer and its business, the size and type of the transaction or activity, the relationship between several transactions or activities, the origin, destination or use of funds or any other circumstance known to the obliged entity, including the consistency of the transaction or activity with the business and risk profile of the customer, has reasons for suspicion that they constitute proceeds of crime or are connected with money laundering or terrorist financing, regardless of their amount;

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 shall be a relationship:

- in which one credit institution, as correspondent, provides banking services to another credit institution, as respondent, including maintaining current or other liability accounts and providing related services such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services, and
- between and within credit institutions and financial institutions, including where similar services are provided by a correspondent institution to a respondent institution, including relationships established for securities transactions or funds transfers or relationships established for transactions involving crypto-assets or transfers of crypto-assets;

24) shell (fictitious) bank shall be a credit institution or financial institution, or another similar institution carrying out activities equivalent to those carried out by a credit institution or financial institution, which is registered in a country in which it has no business presence, does not carry out any activity, has no business premises, employees, governing bodies or management and is not affiliated with a financial group subject to supervision for the purpose of preventing and detecting money laundering and terrorist financing;

25) property shall mean property rights of any kind, regardless of whether they relate to tangible or intangible goods, movable or immovable property, securities, crypto-assets and other documents (in any form, including electronic or digital form) evidencing property rights;

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

- money, cheques, monetary claims, bills of exchange, monetary remittances and other means of payment,
- funds invested with an obliged entity,
- financial instruments, specified in the law governing capital market, which are traded through appropriate offering, including shares and stakes, certificates, debt instruments, bonds, guarantees and derivative financial instruments,
- other documents evidencing rights to financial means or other financial resources,
- interest, dividends and other income from the funds,
- receivables, loans and letters of credit;

26a) physically transferable means of payment shall be cash, bearer securities, cheques, bills of exchange and other physically transferable means of payment, payable to the bearer;

27) money (funds) shall mean cash (domestic and foreign banknotes and coins), funds in accounts and electronic money;

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

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

30) payment service provider shall be a credit institution, electronic money institution or payment institution;

31) transfer of funds shall be any transaction which is executed, at least in part, electronically by a payment service provider on behalf of the payer with the aim of making those funds available to the payee through a payment service provider, regardless of whether the payer and the payee are the same person and whether the payment service provider of the payer and the payment service provider of the payee are the same person, including a payment transaction executed:

- by credit transfer in line with the law governing payment transactions;
- by money remittance, being a payment service in which funds are received from the payer, without opening a payment account in the name of the payer or the payee, solely for the purpose of transferring the corresponding amount to the payee or another payment service provider acting on behalf of the payee, and/or where those funds are received on behalf of the payee and made available to that payee;
- using a payment card, a payment instrument used for disposing of electronic money, a mobile telephone or any other electronic or information-technology device with similar characteristics;
- by direct debit in line with the law governing payment transactions;

32) intermediary in the transfer of funds shall be a payment service provider who is neither the payment service provider of the payer nor the payment service provider of the payee and who receives and transfers funds on behalf of the payment service provider of the payer or the payee, or on behalf of another intermediary in the transfer of funds;

33) business relationship shall be a business, professional or commercial relationship related to the professional activities of an obliged entity, established between an obliged entity and

a customer, including where the relationship is established without a written contract and is expected, at the time of establishment, to be repetitive or permanent in nature, as well as:

- registration of a customer for participation in the system for organising games of chance,

- conclusion of a contract on the purchase of investment units and/or shares in an investment fund, in line with the law governing the operation of investment funds,

- conclusion of a contract on the provision of investment and/or ancillary services, in line with the law governing the capital market;

34) anonymous company shall be a foreign legal person with unknown owners and/or managers;

35) senior manager shall be a natural person who is a member of the management body of an obliged entity, as well as a natural person who performs an executive function and is accountable for that function to the management body, and an employee who possesses sufficient knowledge of the exposure of the obliged entity to money laundering and terrorist financing risk and has the authority to take decisions affecting the exposure of the obliged entity to such risk;

36) group shall be a group of companies comprising a parent company, subsidiaries and companies in which the parent company or a subsidiary has a participation, as well as companies interconnected in line with the law governing accounting;

37) person shall be a citizen of Montenegro, a foreign national, a domestic or foreign legal person or another subject of law;

38) other subject of law shall be an organised group of individuals who pool or have undertaken to pool funds or other property for specific purposes;

39) organiser of games of chance shall be an organiser of games of chance within the meaning of the law governing games of chance, as well as an organiser who has the consent of the competent authority to organise those games via the Internet or other telecommunication means;

40) insurance representative shall be a legal or natural person holding a licence to perform insurance representation activities issued by the regulatory authority responsible for insurance activities;

41) trust shall be a legal arrangement under which a settlor transfers property to a trustee who manages such property for the benefit of one or more beneficiaries, where a person with supervisory or control powers may oversee such management (protector or trust protector);

41a) legal arrangement shall comprise an express trust and another person or an equivalent foreign-law entity (an arrangement with a structure or function similar to a trust, including a fiducie and certain types of Treuhand and fideicomiso arrangements);

41b) trustee shall be a person who is the legal owner of trust property, manages trust property, executes transactions, signs contracts, represents the trust before third parties, appoints its representatives or authorised persons and appoints discretionary beneficiaries;

42) distribution channel means a channel used to deliver products and services to the end user;

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

- monetary value stored on instruments that may be used to purchase goods or services only on the premises used by the issuer of such instrument or under a commercial agreement with the issuer, within a limited network of payment service providers or for a limited range of goods or services,

- monetary value used for payment transactions carried out through a telecommunications, digital or information-technology device, where the purchased goods or services are delivered and used through a telecommunications, digital or information-technology device, provided that the telecommunications, digital or information-technology operator does not act solely 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 for the payer and makes it impossible for the electronic money issuer and the payee to monitor the payment;

45) cash means banknotes and coins in circulation as legal tender;

46) crypto-asset means a digital representation of a value or of a right that can be transferred and stored electronically using distributed ledger technology (DLT) or similar technology, including an electronic money token, but does not refer to crypto-assets that qualify as:

- a financial instrument, in line with the law governing the capital market;
- a deposit, including structured deposits, in line with the law governing deposit protection;
- funds that do not qualify as electronic money tokens;
- securitisation, in line with the law governing the capital market;
- a non-life or life insurance product, within the meaning of the law governing the conditions and manner of conducting insurance activities;
- a pension product whose primary purpose is to provide the investor with retirement income and which grants the right to specific benefits;
- an occupational pension product covered by the law governing pension funds or the law governing insurance and reinsurance;
- a unit of account of voluntary pension funds, in line with the law governing voluntary pension funds;
- pension insurance, in line with the law governing pension and disability insurance;
- a pan-European personal pension product, in line with the law governing such products;
- a social security scheme, in line with a special law;
- individual pension insurance products for which the employer is legally required to make financial contributions and where neither the employer nor the employee can choose the pension product or insurer,
- a crypto-asset that is unique and not interchangeable with another crypto-asset;

47) fiat currency means legal tender issued by a central bank;

48) legal person means a person that may establish a permanent customer relationship with a financial institution or otherwise possess property (e.g. a firm, corporation, foundation, partnership or business association, or another corresponding or similar structure);

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

50) establishing customer identity means a part of the customer identification procedure relating to the collection of data from identity documents of natural persons and comparison of those data with data from independent and objective sources or by any other secure remote or electronic procedures regulated, recognised, approved or accepted by the state, and, for legal persons and business organisations, the collection of data from appropriate documents and comparison of those data with data in the register in which the legal person is registered or with data from other registers of legal persons;

51) verifying customer identity means the part of the customer identification procedure relating to verification of the identity of natural persons by inspecting the photograph in the identity document of the natural person or by verifying data through electronic identification or video-electronic identification in line with this Law and, for legal persons and business organisations, by inspecting the register in which the legal person or business organisation is registered or another appropriate public register, or by inspecting an original or certified photocopy of a document from the register in which the legal person or business organisation is registered or an original or certified photocopy of another document from the appropriate public register;

52) electronic money token means a type of crypto-asset whose value is intended to remain stable by being pegged to the value of a fiat currency;

53) crypto wallet means a wallet used to store a private cryptographic key and allowing users to securely store, 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 within the meaning of this Law, or which, according to data from relevant international organisations, does not meet international standards in the field of prevention of money laundering and terrorist financing;

55) identity document means an identity card or passport, as well as an identity document issued in Montenegro to a person granted asylum or a foreigner under subsidiary protection;

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

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

58) electronic form of a document means any industry-standard file format (PDF, DOCX, etc.);

59) residents mean:

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

60) non-residents mean persons who are not residents;

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

62) electronic identification means shall be a set of data, computer equipment (hardware) or computer programme (software) containing identification data in electronic form or linking a natural person, legal person or authority to such data and 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 trust service provider in line with the law governing electronic identification and electronic signature;

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

66) supervisory officer means an inspector or civil servant who performs inspection activities in line with the law;

67) ICAO Doc 9303 recommendations mean international recommendations recognised in European Union standards relating to the issuance of identification documents;

68) linked transactions means two or more transactions that may be considered linked due to the period in which they were executed, the payee or payer, the manner in which the transactions were carried out, the reason for which they were executed or other factors indicating that the transactions may be considered linked;

69) crypto-asset service provider means a legal person, business organisation, sole proprietor or natural person carrying out an economic activity that provides one or more crypto-asset services to customers on a professional basis;

70) crypto-asset services are:

- custody and administration of crypto-assets on behalf of a customer,
- operation of a trading platform for crypto-assets,
- exchange of crypto-assets for fiat currency,
- exchange of crypto-assets for other crypto-assets,
- execution of orders for crypto-assets on behalf of a customer,
- placing of crypto-assets,
- reception and transmission of orders for crypto-assets on behalf of a customer,
- provision of advice on crypto-assets,
- portfolio management of crypto-assets,
- provision of transfer services for crypto-assets on behalf of customers;

71) custody and administration of crypto-assets on behalf of customers includes the safekeeping or control, on behalf of a customer, of crypto-assets or of the means of access to those crypto-assets, where applicable in the form of private cryptographic keys;

72) operation of a trading platform for crypto-assets means managing one or more multilateral systems that bring together or facilitate the bringing together of multiple third-party buying and selling interests in crypto-assets within the system and in line with its rules, in a manner that results in the conclusion of a contract relating to crypto-assets through the exchange of one crypto-asset for another crypto-asset or the exchange of a crypto-asset for fiat currency that is legal tender;

73) exchange of crypto-assets for fiat currency means entering into contracts with customers for the purchase or sale of crypto-assets in exchange for fiat currency using own capital;

74) exchange of crypto-assets for other crypto-assets means entering into contracts with customers for the purchase or sale of crypto-assets in exchange for other crypto-assets using own capital;

75) execution of orders for crypto-assets on behalf of customers means entering into agreements, on behalf of a customer, to purchase or sell one or more crypto-assets or to subscribe, on behalf of customers, to one or more crypto-assets, and includes entering into

contracts for the sale of crypto-assets at the time of their public offering or admission to trading;

76) placing of crypto-assets means the marketing of crypto-assets to purchasers on behalf of or for the account of the offeror or a party related to the offeror;

77) reception and transmission of orders for crypto-assets on behalf of a customer means receiving an order to purchase or sell one or more crypto-assets or to subscribe to one or more types of crypto-assets and transmitting that order to a third party for execution;

78) advice on crypto-assets includes offering, giving or agreeing to give recommendations to a customer, at the request of the customer or on the initiative of the crypto-asset service provider, concerning one or more transactions related to crypto-assets or the use of crypto-asset services;

79) portfolio management of crypto-assets means managing portfolios in line with mandates given by customers on an individual and discretionary basis, where those portfolios include one or more crypto-assets;

80) provision of transfer services for crypto-assets on behalf of a customer includes the provision of services for transferring, on behalf of a customer, crypto-assets from one distributed ledger address or account to another distributed ledger address or account, as well as the use of crypto ATMs;

81) crypto-asset account means an account held by a crypto-asset service provider on behalf of one or more persons, which may be used for the execution of crypto-asset transfers;

82) originator means a person who has a crypto-asset account with a crypto-asset service provider, a distributed ledger address or a device enabling the storage and transfer of crypto-assets from that account, address or device or, where that person has no such account, address or device, a person who gives an order for or initiates a crypto-asset transfer;

83) crypto-asset beneficiary means a person who is the intended recipient of a crypto-asset transfer;

84) transfer of crypto-assets means any transaction intended to transfer crypto-assets from one distributed ledger address, crypto-asset account or other device enabling the storage of crypto-assets to another such address, account or device, carried out by at least one crypto-asset service provider acting on behalf of the originator or the crypto-asset beneficiary, regardless of whether the originator and the beneficiary are the same person or whether the same crypto-asset service provider acts on behalf of both;

85) batch transfer means a collection of several individual transfers of funds or crypto-assets that are aggregated for the purpose of transmission;

86) unique transaction identifier means a combination of letters, numbers and/or symbols determined by the payment service provider in line with the rules of payment and settlement systems or messaging systems used for the transfer of funds, or determined by the crypto-asset service provider, which enables the transaction to be traced back to the payer and the payee or the transfer of crypto-assets to be traced back to the originator and the crypto-asset beneficiary;

87) person-to-person transfer of crypto-assets means a transfer of crypto-assets carried out without the involvement of any crypto-asset service provider;

88) intermediary crypto-asset service provider means a crypto-asset service provider that is neither the crypto-asset service provider of the originator nor of the crypto-asset beneficiary and that receives and forwards a transfer of crypto-assets on behalf of the crypto-asset service provider of the originator or of the crypto-asset beneficiary, or on behalf of another intermediary crypto-asset service provider;

89) crypto-ATM means a physical or online electronic terminal that enables a crypto-asset service provider to provide, in particular, crypto-asset transfer services on behalf of a customer;

90) distributed ledger address means an alphanumeric identifier designating, on a network using distributed ledger technology (DLT) or similar technology, the address to which crypto-assets can be sent or from which they can be 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 that is not linked to any of the following:

- a crypto-asset service provider,

- an entity that does not have its registered office in Montenegro and provides services similar to those of a crypto-asset service provider,

- an entity that does not have its registered office in the European Union and provides 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, business organisation or natural person that instructs the nominee to act on behalf of the nominator in a certain capacity, including as a director, shareholder or founder, while the nominee is a legal person, business organisation or natural person acting on the instructions of the nominator;

97) Legal Entity Identifier (LEI) means a unique alphanumeric reference code assigned to a legal person in line with ISO 17442;

98) cryptographic algorithm means a mathematical procedure or set of rules used for protecting data, namely for encrypting and decrypting data;

99) electronic cheque means a digital version of a traditional cheque instrument used for payment, but in electronic format.

## II.NATIONAL RISK ASSESSMENT

### Determining the National Risk Assessment

### Article 7

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 4)*

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

identification and assessment of the risk of money laundering and terrorist financing at the state level;

typologies of money laundering and terrorist financing, in line with the

recommendations of the Financial Action Task Force (FATF);

identification of sectors and activities in which obliged entities should apply enhanced customer due diligence and monitoring measures and, where necessary, determination of measures to be taken to prevent money laundering and terrorist financing;

identification of sectors and activities in relation to which the risk of money laundering and terrorist financing has been determined;

determination of appropriate measures to prevent money laundering and terrorist financing on the basis of identified risks and enhancement of efficiency in the allocation of available resources for the control, mitigation and management of identified risks of money laundering and terrorist financing;

proposal for improving existing regulations in the area of prevention and detection of money laundering and terrorist financing for certain sectors and activities or adopting new regulations, in line with identified risks of money laundering and terrorist financing, as well as guidelines for obliged entities in those sectors and activities on preparing an assessment of the risk of money laundering and terrorist financing;

data on the institutional structure and general procedures of the AML/CFT system, including data on the Financial Intelligence Unit, the state administration authority responsible for revenue affairs and the competent State Prosecutor's Office, as well as data on the available financial resources and staffing capacities of those authorities, to the extent to which those data are available;

data on activities undertaken at the state level and data on financial resources and staffing capacities 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.

Government shall determine the National Risk Assessment at least once every three years.

National Risk Assessment shall be updated as necessary, particularly where new risks are identified as a result of the introduction of new products, services, business practices or distribution channels, including the development of new technologies.

**Coordinating body for preparation of the National Risk Assessment**

**Article 8**

Government shall establish a coordinating body for the preparation of the National Risk Assessment and management of identified risks, which shall:

1) prepare the National Risk Assessment;

2) prepare a report on identified national risks of money laundering and terrorist financing;

3) prepare a proposal of measures and an action plan for mitigating and managing identified risks of money laundering and terrorist financing;

4) carry out analyses in the area of prevention of money laundering and terrorist financing, prepare reports on analyses carried out and coordinate cooperation between competent authorities and organisations.

Coordinating body referred to in paragraph 1 of this Article shall have a president, members and a secretary.

Coordinating body referred to in paragraph 1 of this Article shall be established for a period of four years and the same persons may serve as president, members or

secretary of that body no 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.

Detailed composition of the coordinating body, manner of performing its tasks and other matters relevant to the work of the coordinating body referred to in paragraph 1 of this Article shall be prescribed by the Government.

**Publication of data from the National Risk Assessment**

**Article 9**

Certain parts or data from the National Risk Assessment may be marked with an appropriate classification level in line with the law regulating classified information.

Parts or data from the National Risk Assessment which are not marked with an appropriate classification level shall be published on the website of the Financial Intelligence Unit.

For the purpose of facilitating obliged entities in carrying out their own assessment of the risk of money laundering and terrorist financing, the Financial Intelligence Unit may, in addition to the parts or data referred to in paragraph 2 of this Article, publish other data from the National Risk Assessment on its website.

**Report on implementation of the National Risk Assessment**

**Article 10**

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

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 authority responsible for revenue affairs and the competent State Prosecutor's Office, as well as data on the available financial resources and staffing capacities of those authorities, to the extent to which those data are available,
- activities undertaken at the state level, staffing capacities and financial resources spent from those 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 OBLIGED ENTITIES

### 1. Measures and actions undertaken by obliged entities

**Types of measures and actions**

**Article 11**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 4)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 5)*

Obliged entity shall, when conducting its activities, undertake measures and actions in line with this Law, in particular the following:

1) identify risks and assess the risk of money laundering and terrorist financing, establish policies, controls and procedures and undertake activities to mitigate the risk of money laundering and terrorist financing;

2) carry out customer identification, monitor the business relationship and control customer transactions (hereinafter referred to as: "customer due diligence and monitoring measures");

3) establish an appropriate information system, where the obliged entity is a credit institution or another financial institution, providing automated support for assessing money laundering and terrorist financing risk in relation to customers, ongoing monitoring of business relationships with customers, scrutiny of transactions and automatic identification of suspicious customers or suspicious transactions;

4) submit information, data and documentation to the Financial Intelligence Unit in a timely manner;

5) designate a compliance officer for the prevention of money laundering and terrorist financing and their deputy and provide the conditions for their work;

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

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

8) keep records and ensure the protection and retention of information, data and documentation obtained in line with this Law;

9) establish and monitor a system that enables complete and timely response to the requests of the Financial Intelligence Unit and competent state authorities in line with this Law;

10) implement measures for the prevention and detection of money laundering and terrorist financing in business units and companies majority-owned by obliged entities in other countries;

10a) establish and maintain technical conditions for using the internet application of the Financial Intelligence Unit, including the submission of public keys of qualified certificates, in line with the regulation referred to in Article 66 paragraph 15 of this Law;

11) take other measures and activities in line with this Law.

Financial-sector obliged entity which has a collegiate management body shall, in addition to the measures and actions referred to in paragraph 1 of this Article, appoint one member of that body responsible for monitoring compliance with this Law, in particular for:

- establishing internal policies, procedures and internal control mechanisms and ensuring that they are in line with the assessed business risk of the obliged entity;
- ensuring adequate human, technical and material resources necessary for the effective functioning of the system for the prevention of money laundering and terrorist financing by adopting appropriate decisions;
- analysing significant deficiencies in the system for the prevention of money laundering and terrorist financing and taking measures to remedy them without delay, and regularly reporting thereon to the management body;
- supporting and advising the management body when it adopts decisions affecting the exposure of the obliged entity to risk;
- ensuring the independence of the internal audit function and considering its findings relating to the prevention of money laundering and terrorist financing.

## Risk Analysis

**Article 12**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 5)*

Obliged entity shall identify risks and assess the risk of money laundering and terrorist financing in such a manner as to:

- within 60 days from the date of its establishment or commencement of business, prepare an internal act on risk analysis in which it identifies and assesses risks, taking into account risk factors relating to an individual customer, a group of customers, a country or geographical area, a business relationship, a transaction, a product, a service or distribution channel which may be misused for money laundering or terrorist financing (hereinafter: risk analysis), and update and retain it regularly, at least once a year, in line with this Law;
- carry out a risk assessment for new products, services or distribution channels and update the risk analysis on the basis of that assessment;
- determine categories of money laundering and terrorist financing risk;
- on the basis of the risk analysis, reassess the risk relating to an individual customer, a group of customers, a country or geographical area, a business relationship, a transaction, a product, a service or distribution channel which may be used for money laundering or terrorist financing.

Risk analysis shall include an assessment of the measures, actions and procedures which the obliged entity undertakes to prevent and detect money laundering or terrorist financing.

Risk analysis shall include at least an analysis of money laundering and terrorist financing risks relating to the overall operations of the obliged entity and an analysis of those risks for each group or type of customer, business relationship, service provided by the obliged entity to a customer in the course of its business or transaction.

Risk analysis shall be prepared in written and electronic form and shall be proportionate to the size of the obliged entity and the nature and scope of its business.

Obliged entity shall prepare the risk analysis on the basis of risk analysis guidelines established by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, in line 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, in risk analysis guidelines, determine that individual documented risk assessments are not required where certain risks are typical for the sector, clearly defined and easily understood.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may, if they consider it necessary, require the obliged entity to revise its risk analysis, as well as policies, controls and procedures referred to in Article 14 paragraph 1 item 2 of this Law.

Obliged entity shall submit the risk analysis to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law at its request, within three days of the date when the request is received.

## Lower and higher risk of money laundering and terrorist financing

**Article 13**

Should an obliged entity assess that a customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channel presents a lower risk of money laundering or terrorist financing, it may apply simplified customer due diligence and monitoring measures in line with this Law.

Should an obliged entity assess that a customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channel presents a higher risk of money laundering or terrorist financing, it shall apply enhanced customer due diligence and monitoring measures in line with this Law.

## Money laundering and terrorist financing risk management

### Article 14

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 6)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 4)*

Obliged entity shall establish a system for managing the risk of money laundering and terrorist financing which reduces the risks identified through risk analysis and shall include, in particular:

1) risk analysis;

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

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

4) establishing an appropriate internal organisation or organisational structure of the obliged entity proportionate to the scope and nature of its business.

Policies, controls and procedures referred to in paragraph 1 item 2 of this Article shall be proportionate to the scope and nature of the activities of the obliged entity, the size and type of customers and the types of products or services provided by the obliged entity.

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

1) establishing internal policies, controls and procedures relating to:

- objectives, scope and manner of operation of the system for managing the risk of money laundering and terrorist financing,
- customer due diligence and monitoring measures,
- submitting data to the Financial Intelligence Unit in line with the law,
- protection and storage of data and keeping records,
- internal controls in the area of prevention and detection of money laundering and terrorist financing,
- security checks of employees,
- designation of compliance officer for prevention of money laundering and terrorist financing and their deputy;

2) establishing an independent audit function or designating a person for continuous monitoring and supervision of identified money laundering and terrorist financing risks, as well as testing the internal policies and procedures referred to in item 1 of this paragraph, proportionate to the scope and nature of the business of the obliged entity.

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

Obliged entity shall, in proportion to the scope and nature of its activities, designate a compliance officer for the prevention of money laundering and terrorist financing who holds a managerial position.

Obliged entity shall prepare policies, controls and procedures referred to in paragraph 1 item 2 of this Article on the basis of guidelines for establishing the system for managing the risk of money laundering and terrorist financing, established by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law in line with the regulation referred to in Article 15 of this Law and the National Risk Assessment.

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

**Article 15**

Detailed criteria for drafting risk analysis guidelines, depending on the size and manner of organisation of the obliged entity, the scope and type of business, type of customer, product, service or distribution channel provided, criteria for determining risk factors, mandatory elements to be included in the risk analysis and other elements relevant to the assessment of money laundering and terrorist financing risk, as well as detailed criteria for drafting guidelines for establishing the system for managing money laundering and terrorist financing risk, shall be prescribed by the state administration authority responsible for internal affairs (hereinafter referred to as: the Ministry).

Professional basis for drafting the regulation referred to in paragraph 1 of this Article shall be prepared by the Financial Intelligence Unit, together with an opinion obtained from the supervisory authorities referred to in Article 131 paragraph 1 of this Law.

**New products, services or distribution channels**

**Article 16**

Obliged entity shall assess the money laundering and terrorist financing risk relating to a new service, product or distribution channel provided in the course of its business, a new business practice and the manner of providing a new service, product or distribution channel, before its introduction.

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

Obliged entity shall, on the basis of the updated risk analysis, take additional measures to mitigate and manage the money laundering and terrorist financing risks referred to in paragraphs 1 and 2 of this Article.

## 2. Identification of the Customer, Monitoring of the Business Relationship and Control of Customer Transactions

**Customer Due Diligence and Monitoring Measures**

**Article 17**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 6)*

Obliged entity shall implement customer due diligence and monitoring measures, in particular by:

1) identifying the customer;

2) determining the beneficial owner of the customer and identifying the beneficial owner, including measures necessary to determine the ownership structure and

controlling member of the customer in the cases laid down by this Law;

2a) determining whether the customer, representative of the customer or beneficial owner of the customer is a politically exposed person in line with this Law;

3) obtaining and recording data on the purpose, intended use, objective and nature of the business relationship and transaction and other data in line with this Law;

4) regularly monitoring the business relationship and scrutinising transactions undertaken by the customer with the obliged entity during that relationship and verifying their consistency with the nature of the business relationship and the usual scope and type of business of the customer, so as to ensure that transactions are consistent with the knowledge of the obliged entity of the customer, the business profile and the level of money laundering and terrorist financing risk of that customer and, where possible, the source of funds, and that data, information and documentation concerning that customer are up to date.

When implementing the measures referred to in paragraph 1 items 1 and 2 of this Article, the obliged entity shall verify whether the person acting on behalf of the customer is entitled or authorised by the customer to do so and shall identify that person in line with this Law.

Obliged entity shall implement the measures referred to in paragraphs 1 and 2 of this Article to an extent proportionate to the money laundering and terrorist financing risk.

Prior to establishing a business relationship or executing an occasional transaction, the obliged entity shall determine the purpose and intended nature of the business relationship or transaction and, in line with the assessed risk, shall obtain information on:

1) the purpose of entering into and the nature of the business relationship or occasional transaction;

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

3) the source of funds used in the business relationship or transaction;

4) the destination of funds, depending on the type of transaction;

5) the duration of the business relationship; and

6) the consistency of business operations with the purpose of entering into the business relationship.

Obliged entity shall regulate procedures for implementing the measures referred to in paragraphs 1 and 2 of this Article by internal acts.

At the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, the obliged entity shall submit appropriate analyses, documents and other information demonstrating that the measures have been implemented in line with the identified money laundering and terrorist financing risk.

Should the obliged entity be unable to implement one or more measures referred to in paragraph 1 of this Article, it shall notify the Financial Intelligence Unit thereof in the manner prescribed by the regulation referred to in Article 66 paragraph 15 of this Law.

### Cases in which customer due diligence and monitoring measures are implemented

### Article 18

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 7)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 5)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 7)*

Obliged entity shall implement customer due diligence and monitoring measures:

1) when establishing a business relationship with a customer;

2) when executing occasional transactions in the amount of EUR 10,000 or more, regardless of whether these comprise a single transaction or several linked transactions;

3) when executing occasional cash transactions in the amount of EUR 3,000 or more but less than EUR 10,000, regardless of whether these comprise a single transaction or several linked transactions;

4) when executing any occasional transaction constituting a transfer of funds in the amount of EUR 1,000 or more, regardless of whether it comprises a single transaction or several linked transactions within the meaning of Articles 35 through 38 of this Law;

5) when there is suspicion as to the accuracy or authenticity of the obtained identification data concerning the customer or beneficial owner of the customer;

6) when, in connection with a transaction, customer, funds or property, there are reasons for suspicion or grounds for suspicion that the property derives from criminal activity or that money laundering or terrorist financing is involved, regardless of the amount of the transaction;

7) in relation to natural and legal persons trading in goods, when executing occasional transactions in the amount of EUR 10,000 or more, regardless of whether these comprise a single transaction or several linked transactions;

8) when a stake in the amount of EUR 20 or more is paid in the execution of a single transaction or several linked transactions, where the obliged entity is an organiser of games of chance;

9) when executing any occasional transaction constituting a transfer of crypto-assets with a value of EUR 1,000 or more, regardless of whether it comprises a single transaction or several linked transactions.

Obliged entity shall periodically implement customer due diligence and monitoring measures in relation to customers with whom it has already established business relationships, on the basis of the money laundering and terrorist financing risk assessment, or when certain circumstances concerning the customer change, or when the obliged entity is required under any legal obligation during the relevant calendar year to contact the customer in order to verify all relevant information concerning the beneficial owner of the customer, or where it is required to do so in line with the regulation governing tax administration.

Should an obliged entity, in addition to an existing business relationship, enter into an additional business relationship with a customer or execute a transaction referred to in paragraph 1 items 2, 3, 7, 8 and 9 of this Article on the basis of an existing business relationship, it shall verify whether the existing data are up to date and obtain only the data and documentation that are missing, have changed in the meantime or have expired.

Obliged entity may not require a customer to resubmit data and documentation already held in electronic or paper form, provided that such data and documentation remain valid and correspond to the current data concerning the customer.

When implementing customer due diligence and monitoring measures in all cases referred to in paragraph 1 of this Article, the obliged entity shall obtain the data referred to in Article 17 paragraphs 1 and 2 of this Law.

Content and type of data obtained and recorded when implementing the measures and actions referred to in Article 17 paragraphs 1 and 2 of this Law shall be prescribed by Article 117 of this Law.

Notwithstanding paragraphs 1 through 6 of this Article, where an obliged entity has reasons for suspicion of money laundering or terrorist financing and reasonably believes that implementing customer due diligence and monitoring measures would tip off the customer, it shall not be required to implement such measures and shall instead notify the Financial Intelligence Unit thereof without delay.

Obliged entity shall provide the customer with information on the purpose of processing the data obtained when implementing customer due diligence and monitoring measures, in line with the law governing personal data protection.

When implementing the measures referred to in paragraph 1 of this Article, in addition to the person with whom a business relationship is established or a transaction is executed, the following shall also be considered customers:

- the supplier of goods, in the case of obliged entities referred to in Article 4 paragraph 2 item 13 indents 10 through 13 of this Law;

- both parties to the transaction, in the case of obliged entities referred to in Article 4 paragraph 2 item 13 indents 5, 8 and 9, item 14 and obliged entities referred to in Article 4 paragraphs 3 and 4 of this Law.

**Implementation of customer due diligence and monitoring measures prior to establishing a business relationship**

**Article 19**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 8)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 8)*

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

Notwithstanding paragraph 1 of this Article, an obliged entity may implement the measures referred to in Article 17 paragraph 1 items 1, 2 and 2a of this Law while establishing a business relationship with a customer where it considers this necessary in order to avoid interrupting normal business operations and where there is a lower risk of money laundering and terrorist financing.

Should an obliged entity be unable to implement the measures referred to in paragraph 1 of this Article, the business relationship may not be established and, where it has already been established, the obliged entity shall terminate it.

Obliged entity may not establish a business relationship with a customer and, where such relationship has already been established, shall terminate it where it assesses that it cannot effectively manage the money laundering and terrorist financing risk associated with that customer.

Provision of paragraph 3 of this Article shall not apply to obliged entities referred to in Article 4 paragraph 2 item 13 indent 2 and paragraphs 3 and 4 of this Law when ascertaining the legal position of a customer or defending or representing a customer in judicial proceedings or in connection with judicial proceedings.

Obliged entity shall regulate by internal acts the procedures for refusing to establish a business relationship or terminating an existing business relationship referred to in paragraphs 3 and 4 of this Article.

**Implementation of customer due diligence and monitoring measures prior to executing transactions**

**Article 20**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 9)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 6)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 9)*

Obliged entity shall implement the measures referred to in Article 17 paragraph 1 items 1 through 3 of this Law prior to executing a transaction referred to in Article 18 paragraph 1 items 2, 3, 4, 7, 8 and 9 of this Law.

Should an obliged entity be unable to implement one or more measures referred to in paragraph 1 of this Article, the transaction may not be executed, except in the case referred to in Article 19 paragraph 5 of this Law.

**Customer due diligence and monitoring measures in real estate transactions**

**Article 20a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 10)*

Notwithstanding Article 20 paragraph 1 of this Law, an obliged entity engaged in intermediation in the sale and lease of immovable property shall implement the measures referred to in Article 17 paragraph 1 items 1 through 3 of this Law after the seller or lessor accepts the offer and no later than prior to executing the transaction or transferring the property.

**Identification of the beneficiary or beneficial owner under a life insurance policy**

**Article 21**

Obliged 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 under a life insurance policy at or after conclusion of the life insurance contract, but no later than when the beneficiary under the life insurance policy may exercise their rights.

Obliged 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, where:

1) where a natural or legal person is designated as the beneficiary, by obtaining the name and surname or name of the beneficiary;

2) where the beneficiary is designated by characteristics, class or in another manner, by obtaining information on that beneficiary to an extent sufficient to identify the beneficiary at the time of payment.

Identity of the beneficiary or beneficial owner referred to in paragraph 2 of this Article shall be verified at the time of payment.

Should rights under the life insurance policy be transferred to a third party, in part or in full, the obliged entity shall identify the new beneficiary or beneficial owner at the time of transfer of those rights.

Obliged entity referred to in Article 4 paragraph 2 items 8 and 9 of this Law shall regulate by internal acts the procedures for implementing the measure referred to in paragraph 1 of this Article.

**Identification of a natural person**

**Article 22**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 7)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 11)*

Obliged entity shall identify a customer who is a natural person, sole proprietor or

natural person carrying out a business activity in line with Article 18 paragraph 1 item 1 and Articles 19 and 20 of this Law by inspecting an identity document in the presence of the customer.

Obliged entity shall, in the procedure for identifying the customer referred to in paragraph 1 of this Article, inspect the data in the identity document and verify whether the data in that document correspond to the customer.

Obliged entity shall, in the procedure for identifying the customer referred to in paragraph 1 of this Article, obtain a photocopy of the identity document, record the date, time and name and surname of the person who inspected the photocopy of the identity document and retain that photocopy and the collected data in line with this Law.

When identifying the customer referred to in paragraph 1 of this Article, data on the customer, business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 4, 6 and 7 and paragraphs 2 through 6 of this Law shall be obtained.

Should all data referred to in paragraph 4 of this Article not be available, the data shall be obtained by inspecting an original or certified photocopy of another valid public document presented by the customer or by accessing a public register.

Should the legal representative or authorised person of the customer referred to in paragraph 1 of this Article establish a business relationship or carry out a transaction on behalf of that customer, the obliged entity shall:

- identify that legal representative or authorised person in line with paragraphs 1 to 5 of this Article and obtain the data on that person referred to in Article 117 paragraph 1 item 3 of this Law;

- obtain the data on the customer referred to in Article 117 paragraph 1 item 3 of this Law from the written authorisation, in the original or a certified photocopy thereof;

- verify the data on the customer obtained in line with indent 2 of this paragraph.

Should an obliged entity, when identifying the customer referred to in paragraph 1 of this Article or the legal representative or authorised person referred to in paragraph 6 of this Article, suspect that the obtained data are untrue or that the documents or other documentation from which the data were obtained are not authentic, it shall carry out additional checks using independent, credible and reliable sources and request a written statement from that customer, legal representative or authorised person confirming the accuracy of the data.

Obliged entity may, through the Financial Intelligence Unit, verify data from the identity documents of the customer referred to in paragraph 1 of this Article, their legal representative or authorised person by electronically accessing the Central Population Register (hereinafter referred to as: the CPR), the records of issued identity documents and the international database of stolen, lost and invalid documents.

Should the checks referred to in paragraph 8 of this Article establish that data from an identity document are different than those in CPR, the obliged entity shall not establish a business relationship or carry out a transaction.

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

Manner of verification referred to in paragraph 8 of this Article shall be prescribed by the Ministry.

Obliged entity may not verify the data of the customer referred to in paragraph 1 of this Article, the legal representative or authorised person through the Financial Intelligence Unit by accessing the CPR unless it has the original identity document available for inspection at the time of verification.

Act referred to in paragraph 11 of this Article shall be assigned the appropriate

classification level in line with the law governing classified information.

## Electronic identification

### Article 23

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 12)*

Identification of a customer who is a natural person, sole proprietor or natural person carrying out a business activity, their legal representative or authorised person may be carried out without mandatory physical presence, using electronic identification means with a high level of assurance of the electronic identification system or a qualified certificate for electronic signature issued by a qualified trust service provider, in line with the law governing electronic identification and electronic signature (hereinafter referred to as: electronic identification).

Prior to electronic identification, the customer shall provide the obliged entity with a photocopy of an identity document and, in the case of identification of the legal representative or authorised person, also a photocopy of the authorisation proving that capacity, in electronic form.

Prior to identification by electronic means, the obliged entity shall obtain data on the customer referred to in paragraph 1 of this Article, the business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 4, 6 and 7 and paragraphs 2 through 6 of this Law.

Obliged entity shall, through the Financial Intelligence Unit, verify the data referred to in Article 117 paragraph 1 items 2 and 3 of this Law by electronically accessing the CPR, the records of issued identity documents and the international database of stolen, lost and invalid documents, in the manner prescribed by the act referred to in Article 22 paragraph 11 of this Law, by transmitting the customer identification number in line with the law governing electronic identification and electronic signature.

Obliged entity may carry out electronic identification only for a service or product provided within the scope of its activity and for a customer for whom a higher risk of money laundering and terrorist financing has not been identified.

Electronic identification may not be carried out if:

-- the verification referred to in paragraph 4 of this Article establishes that data from the identity document of the person referred to in paragraph 1 of this Article differ from the data in the CPR;

-- the electronic identification means or qualified certificate for electronic signature referred to in paragraph 1 of this Article was issued under a pseudonym;

-There are reasonable grounds to suspect that the means of electronic identification or qualified certificate for electronic signature of the person referred to in paragraph 1 of this Article has been misused, or the obliged entity establishes that circumstances substantially affecting the validity of that means of electronic identification or qualified certificate for electronic signature have changed and the electronic identification service provider or qualified trust service provider has not revoked that means or certificate;

-- the electronic identity document of the person referred to in paragraph 1 of this Article was issued in a high-risk third country.

Should an obliged entity, during electronic identification, doubt the accuracy of the data collected or the authenticity of the documents from which the data were obtained, it shall terminate the electronic identification procedure.

For the purpose of carrying out electronic identification, the obliged entity shall provide:

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

-- technical conditions enabling the collection of data concerning the customer referred to in paragraph 1 of this Article, the business relationship and transaction referred to in Article 117 paragraph 1 items 2, 3, 4, 6 and 7 and paragraphs 2 through 6 of this Law and verification thereof in line with paragraph 4 of this Article;

-- technical conditions for keeping records on electronic identification.

Following electronic identification, the obliged entity shall enter in the records referred to in Article 117 paragraph 1 of this Law information on the manner in which the identification of the person referred to in paragraph 1 of this Article was carried out.

**Video-electronic identification**

**Article 24**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 10)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 8)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 13)*

Identification of a customer who is a natural person, sole proprietor or natural person carrying out a business activity, their legal representative or authorised person may be carried out remotely through a video-identification procedure using means of electronic communication (hereinafter referred to as: video-electronic identification).

Video-electronic identification may be conducted only by an employee of the obliged entity who has completed specialised training for conducting video-electronic identification.

Prior to the start of video-electronic identification, the obliged entity shall obtain the consent of the person referred to in paragraph 1 of this Article for the entire video-electronic identification procedure, in particular for recording the image and sound and retaining the recorded material (hereinafter: the video-audio recording), in line with the law, as well as for collecting data by electronically reading electronic identification documents and transmitting the data read via the internet.

Consent referred to in paragraph 3 of this Article shall be recorded in video and audio format.

Obliged entity shall inform the person referred to in paragraph 1 of this Article of the obligation to obtain the consent referred to in paragraph 3 of this Article and of the fact that the giving of consent will be recorded in video and audio format.

Person referred to in paragraph 1 of this Article shall provide the obliged entity, in electronic form, with a photocopy of the electronic identity document to be used during video-electronic identification.

When carrying out video-electronic identification, the obliged entity shall electronically read the data from the identity document issued by the competent authority, which must not have been issued in a high-risk third country, and obtain the data concerning the person referred to in paragraph 1 of this Article, the business relationship and the transaction referred to in Article 117 paragraph 1 items 2 through 7 and paragraphs 2 through 6 of this Law.

By electronically reading data from the electronic identity document, the obliged entity shall obtain data on the sole proprietor or natural person referred to in Article 117 paragraph 1 items 2 and 3 of this Law, as well as the digital image and digital reproduction of the original signature of the customer in line with the recommendations of ICAO Doc 9303.

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

Obliged entity may verify the data referred to in paragraphs 8 and 9 of this Article electronically through the Financial Intelligence Unit by accessing the CPR, the register of issued identity documents and the international database of stolen, lost and invalid documents, in the manner prescribed by the act referred to in Article 22 paragraph 11 of this Law.

Obliged entity shall retain the video-audio recording made during video-electronic identification in line with this Law.

Legal representative or authorised person of the customer shall, in the case of video-electronic identification prior to establishing a business relationship or carrying out a transaction, show and submit a photocopy of the power of attorney proving their capacity as legal representative or authorised person.

Obliged entity may carry out video-electronic identification only for a service or product provided within the scope of its activity.

Notwithstanding paragraph 13 of this Article, an obliged entity referred to in Article 4 paragraph 2 items 1, 2 and 3 of this Law may carry out video-electronic identification only for a service or product it provides within the scope of its activity and for a customer for whom a higher risk of money laundering and terrorist financing has not been identified.

Obliged entity may not carry out video-electronic identification if the electronic identity document of the person referred to in paragraph 1 of this Article was issued in a high-risk third country.

Obliged entity shall terminate the video-electronic identification if:

- during the check referred to in paragraph 10 of this Article it is established that data from the identity document of the person referred to in paragraph 1 of this Article are different from those in CPR;
- it doubts the accuracy of the data collected or the authenticity of the documents from which the data were obtained;
- adequate transmission of image and sound or high-quality transmission cannot be ensured;
- the premises in which the person referred to in paragraph 1 of this Article is located are poorly lit or noisy, making it impossible to identify that person or clearly hear that person or the employee;
- due to other disturbances in communication, transmission of the image and/or the sound or due to other circumstances, the employee cannot perform identification of the person referred to in paragraph 1 of this Article.

Identification of the person referred to in paragraph 1 of this Article may be carried out in a repeated video-electronic identification procedure only if the previous procedure was terminated due to the circumstances referred to in paragraph 16 of this Article and only after those circumstances have been remedied.

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

Obliged entity shall, in line with the act referred to in paragraph 21 of this Article, regulate by internal acts the manner of carrying out video-electronic identification no later than eight days from the date of service of the decision referred to in Article 25 paragraph 6 of this Law approving the carrying out of video-electronic identification.

Notwithstanding paragraph 2 of this Article, the obliged entity may carry out video-electronic identification without direct communication between the customer and an employee, by using

reliable algorithms to verify whether recorded photographs or video footage match the photograph extracted from the customer electronic identity document.

Detailed conditions and manner of carrying out video-electronic identification, as well as the manner of organising and content of the training referred to in paragraph 2 of this Article, shall be prescribed by the Ministry.

### Customer identity verification using reliable algorithms

### Article 24a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 9)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 14)*

Obliged entity that has conducted video-electronic identification of a customer in line with Article 24 of this Law may perform any subsequent customer identity verification by using reliable algorithms, comparing the facial image extracted from a video recording of the customer with the facial image extracted from the electronic identity document used during the initial identification process under Article 24 of this Law.

Verification referred to in paragraph 1 of this Article may be carried out only if the validity period of the customer electronic identity document from which the data were extracted has not expired at the time of verification.

When performing the verification referred to in paragraph 1 of this Article, the obliged entity may, through the Financial Intelligence Unit, verify the data obtained during the identification process in line with Article 24 of this Law via electronic access to the Central Register of Population (CRS), the register of issued identity documents and international databases of stolen, lost or invalid identity documents, in the manner prescribed by the regulation referred to in Article 22 paragraph 11 of this Law.

Obliged entity may carry out the identity verification referred to in paragraph 1 of this Article only for a service or product that it provides within the scope of its business activity.

Obliged entity shall retain the video recording made during the verification procedure referred to in paragraph 1 of this Article in line with this Law.

### Obligations of the obliged entity concerning data protection and cybersecurity when carrying out electronic identification and video-electronic identification

### Article 24b

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 9)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 15)*

Obliged entity shall prepare a risk analysis of the system and solution used for carrying out electronic identification and video-electronic identification.

Obliged entity shall prepare the risk analysis referred to in paragraph 1 of this Article within eight days of obtaining the authorisation referred to in Article 25 of this Law.

Obliged entity shall use secure communication channels for interaction with the customer during electronic identification and video-electronic identification, using secure protocols and

cryptographic algorithms in line with best practice and industry standards for the purpose of protecting confidentiality, integrity, availability and data protection and for the purpose of cybersecurity.

Obliged entity shall continuously monitor the solution referred to in paragraph 1 of this Article in order to ensure that its functionality remains compliant with this Law and the implementing acts adopted in line with Article 24 of this Law.

Obliged entity shall manage the risks identified in the risk analysis referred to in paragraph 1 of this Article.

Obliged entity shall fulfil the requirement referred to in paragraph 2 of this Article prior to introducing electronic identification or video-electronic identification procedures.

## Authorisation for carrying out electronic identification and video-electronic identification

### Article 25

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 11)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 10)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 16)*

Obliged entity may carry out electronic identification or video-electronic identification of a customer who is a natural person, sole proprietor or natural person carrying out a business activity, their legal representative or authorised person, only if it holds an authorisation to carry out electronic identification or video-electronic identification.

Obliged entity shall submit the application for the authorisation 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 form.

Along with the request referred to in paragraph 2 of this Article, the obliged entity shall submit evidence of fulfilment of the conditions referred to in Article 23 paragraph 8 of this Law, or the conditions prescribed by the act referred to in Article 24 paragraph 21 of this Law.

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

Head of the Financial Intelligence Unit shall establish an interagency commission to determine whether the conditions referred to in paragraph 3 of this Article have been fulfilled.

Head of the Financial Intelligence Unit shall, on the proposal of the Commission referred to in paragraph 5 of this Article and on the basis of the application referred to in paragraph 2 of this Article, adopt a decision authorising or refusing to authorise the obliged entity to carry out electronic identification or video-electronic identification.

Commission referred to in paragraph 5 of this Article shall propose adoption of a decision refusing the application referred to in paragraph 2 of this Article if it establishes that a specific service or product presents a higher risk of money laundering and terrorist financing within the meaning of this Law.

At the proposal of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, the head of the Financial Intelligence Unit may adopt a decision

revoking the decision authorising electronic identification or video-electronic identification.

Decisions referred to in paragraphs 7 and 8 of this Article may be challenged in an administrative dispute.

Commission referred to in paragraph 5 of this Article shall comprise representatives of the Financial Intelligence Unit, other organisational units of the Ministry and the supervisory authorities referred to in Article 131 paragraph 1 of this Law.

Commission referred to in paragraph 5 of this Article shall have a president, members and a secretary.

President, members and secretary of the Commission referred to in paragraph 5 of this Article shall be entitled to a monthly fee equal to 25% of the average gross salary in Montenegro in the previous year, according to data of the administrative authority responsible for statistical affairs, paid in net amount.

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

### Identification of a legal person and business organisation

#### Article 26

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 11)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 17)*

Obliged entity shall identify a customer that is a legal person or business organisation in line with 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 concerning the legal person or business organisation that establishes a business relationship or executes a transaction, or the legal person or business organisation for which a business relationship is established or a transaction is executed.

Obliged entity may obtain the data referred to in paragraph 1 of this Article by inspecting the Central Business Registry (hereinafter referred to as: the CBR) or another appropriate public register, as well as a court, business or other public register in which a foreign legal person or business organisation is registered.

Obliged entity may also obtain the data referred to in paragraph 1 of this Article by inspecting the original or a certified photocopy of a document from the CBR or another appropriate public register, as well as the original or a certified photocopy of a document from a court, business or other public register in which the foreign legal person or business organisation is registered, presented on behalf of the legal person or business organisation by its representative or authorised person and not older than three months from the date of issue.

Obliged entity shall retain the documents referred to in paragraph 3 of this Article in its files.

When accessing the registers referred to in paragraph 2 of this Article, the obliged entity shall save an extract from those registers in electronic form or print it and record thereon the date and time and the name and surname of the person who accessed the register.

Data not contained in the registers referred to in paragraph 2 of this Article or in the documents referred to in paragraph 3 of this Article shall be obtained by inspecting the

original or a certified photocopy of a document or other documentation submitted by the representative or authorised person of the customer referred to in paragraph 1 of this Article.

Should an obliged entity, when establishing the identity of a legal person or business organisation, have doubts as to the accuracy of the data obtained or the authenticity of the documents or other documentation from which the data were obtained, it shall, before establishing a business relationship or carrying out a transaction, also obtain a written statement as to the accuracy of those data and carry out additional checks using independent, credible and reliable sources.

Should the customer be a foreign legal person carrying out activities in Montenegro through its business unit, the obliged entity shall identify the foreign legal person and its business unit.

### Identification of the representative of a legal person or business organisation

### Article 27

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 18)*

Obliged entity shall identify the representative of a customer which is a legal person or business organisation in line with Article 22, 23 or 24 of this Law.

Obliged entity shall obtain the data on all directors of the legal person or business organisation referred to in Article 117 paragraph 1 item 3 of this Law.

When determining and verifying the authority to represent of the representative and all directors referred to in paragraph 2 of this Article, the obliged entity shall obtain evidence of that authority and retain it in its documentation.

Should the obliged entity have updated data on directors referred to in paragraph 2 of this Article, it shall not be required to obtain those data again.

### Identification of an authorised person of a legal person or business organisation

### Article 28

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 19)*

Should an authorised person establish a business relationship or execute a transaction on behalf of the representative of a customer that is a legal person or business organisation and all directors of that legal person or business organisation, the obliged entity shall identify that authorised person in line with Article 22, 23 or 24 of this Law.

Obliged entity shall obtain the data referred to in Article 117 paragraph 1 item 3 of this Law concerning the representative and all directors of the legal person or business organisation.

When determining and verifying the authority to represent of the person referred to in paragraph 1 of this Article, the obliged entity shall obtain those authorisations (powers of attorney) and retain them in its documentation.

Should the obliged entity have up-to-date data concerning the representatives and directors referred to in paragraph 2 of this Article, it shall not be required to obtain such data again.

### Identification of a trust, another person or an equivalent foreign-law entity

**Article 29**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 12)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 12)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 20)*

Should the customer be a trust, another person or an equivalent foreign-law entity, the obliged entity shall:

1) identify and obtain the following data concerning the trustee:

- legal form of the trust and the trust instrument;
- property held in or managed through the trust and data on the property to be managed in the context of the business relationship or occasional transaction;
- addresses of the registered office, place of management, permanent residence and temporary residence, tax identification number and powers governing and legally binding the trust;

2) where the trustee is a natural person, identify that person in line with Article 22, 23 or 24 of this Law;

3) identify the representative or authorised person of the trustee in line with Articles 27 and 28 of this Law;

4) obtain data in line with Article 117 of this Law concerning settlors, trust protectors, beneficiaries or classes of beneficiaries, including named beneficiaries, beneficiaries selected by the trustee (discretionary beneficiaries), future beneficiaries who are already designated or ascertainable (beneficiaries who are not yet active) and other natural persons exercising ultimate direct or indirect control over the trust.

Obliged entity shall obtain and verify the data referred to in paragraph 1 item 1 of this Article by inspecting an extract from the Register of Trusts or another appropriate public register or publicly available relevant databases and by inspecting an original or certified copy of a document from a judicial, business or another public register which may not be older than three months.

Should an obliged entity, when identifying the customer referred to in paragraph 1 of this Article, suspect that the obtained data are untrue or that the documents or other documentation from which the data were obtained are not authentic, it shall carry out additional checks using independent, credible and reliable sources and obtain a written statement confirming the accuracy of such data from the trustee, where the trustee is a natural person, or from the representative or authorised person of the trustee.

When establishing a business relationship with an obliged entity or executing an occasional transaction referred to in Article 18 paragraph 1 items 2, 3, 7 and 9 of this Law, the trustee or the representative or authorised person of the trustee shall inform the obliged entity that it is acting in such capacity in the trust and shall provide the information referred to in paragraph 1 item 4 of this Article.

Trustee shall keep accurate and up-to-date records containing the data prescribed by Article 117 paragraphs 1 and 3 of this Law concerning settlors, trust protectors, beneficiaries or classes of beneficiaries, including named beneficiaries, beneficiaries selected by the trustee (discretionary beneficiaries), future beneficiaries already designated or ascertainable (beneficiaries who are not yet active) and other natural persons exercising ultimate direct or indirect control over the trust, as well as data, where applicable, on representatives, authorised persons, investment advisers or managers, accountants and tax advisers.

Trustee shall retain the records referred to in paragraph 5 of this Article for at least five years after the termination of its engagement in the trust.

Trustee shall ensure that the data referred to in paragraph 5 of this Article are accurate and up to date.

Trustee shall provide the Financial Intelligence Unit and the administrative authority competent for tax collection with direct electronic access to the data referred to in paragraph 5 of this Article where, on behalf of the trust, another person or an equivalent foreign-law entity, it enters into any form of business relationship or acquires immovable property in Montenegro.

**Special cases of customer**

**identification**

**Article 30**

Obliged entity shall identify a customer in line with this Law in the following special cases:

1) when a customer enters premises in which games of chance are organised in a casino;
2) whenever the lessee of a safe-deposit box, their representative or a person authorised by the lessee accesses the safe-deposit box.

When identifying the customer referred to in paragraph 1 item 1 of this Article, an obliged entity shall obtain a photocopy of the identity document of that person in line 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 games of chance in the casino for their own account and in their own name.

Identity of the customer referred to in paragraph 1 item 2 of this Article may be established when the customer accesses the safe-deposit box using an electronic identification card, personal access code, video identification means or means enabling identification of the customer on the basis of their biometric characteristics.

When identifying a customer in line with paragraph 1 of this Article, an organiser of games of chance in a casino or an obliged entity engaged in safe-deposit box rental shall obtain the data on the customer referred to in Article 117 paragraph 1 item 3 and paragraph 2 of this Law.

## Implementation of customer due diligence and monitoring measures through a third party

### Article 31

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 13)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 22)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 21)*

Under the conditions provided for by this Law, when establishing a business relationship with a customer, an obliged entity may entrust implementation of the measures referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law to a third party which meets the requirements defined by this Law. A third party may be:

1) credit institutions and branches of foreign credit institutions;
2) companies for the management of investment funds;
3) pension fund management companies;
4) investment company which operates in line with the law which governs a capital market,
5) life insurance company and branch of foreign life insurance companies;
6) Mediation companies, representation companies, and sole proprietors – insurance representatives in the part related to life insurance;

6a) Post of Montenegro;

6b) notary;

6c) crypto-asset service provider;

6d) accountant;

7) persons referred to in items 1 to 6 of this paragraph which have their registered office in a Member State of the European Union or another country applying measures in the field of preventing and detecting money laundering and terrorist financing prescribed by this Law or more stringent measures.

Prior to entrusting implementation of the measures referred to in paragraph 1 of this Article to a third party, an obliged entity shall determine that the operations of that party are subject to regular supervision concerning compliance with anti-money laundering and counter-terrorist financing requirements established by this Law or the relevant regulations of another country, that the party has mechanisms in place to fulfil the obligations of applying customer due diligence and monitoring measures which are at least equivalent to or more stringent than those prescribed by this Law and that records related to the measures undertaken are kept in line with this Law.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may consider that the operations of an obliged entity which is part of a group are in compliance with the provisions of this Article if:

1) it relies on information provided by a third party that is part of the same group;
2) the group applies enhanced customer due diligence and monitoring measures, record-keeping rules, and anti-money laundering and counter-terrorist financing programmes in line with this Law or a corresponding regulation of another country; and
3) the effective implementation of the measures and procedures referred to in item 2 of this paragraph is supervised at group level by a competent supervisory authority in line with this Law or a corresponding regulation of another country.

Notwithstanding paragraphs 2 and 5 of this Article, for the purposes of video-electronic identification an obliged entity may engage a person that uses reliable algorithms to verify the

identity of a customer on the basis of a video recording of the customer by comparing a photograph taken from that recording with the photograph obtained by electronically reading data from the electronic identity document of the customer, which has its registered office in a European Union Member State or another country applying standards for the prevention and detection of money laundering and terrorist financing equivalent to those laid down by this Law or European Union law and whose services are used by at least one credit institution with its registered office in such a country.

Person referred to in paragraph 4 of this Article may not retain personal data of the customer.

External associates and representatives of the obliged entity who on behalf of the obliged entity, based on the agreement (outsourcing or agency relationship) conduct certain customer due diligence and monitoring measures shall not be considered as a third party for the purpose of this Article.

Obliged entity shall be responsible for the proper implementation of customer due diligence and monitoring measures through a third party.

**Prohibition of implementing customer due diligence and monitoring measures through a third party**

**Article 32**

Obliged entity shall not entrust the implementation of customer due diligence and monitoring measures to a third party which is a shell bank, an anonymous company or a person from a high-risk third country.

**Obtaining data and documents from a third party**

Article 33

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 14)*

Third party carrying out customer due diligence and monitoring measures in line with Article 31 of this Law shall deliver the data and documents obtained on the customer to the obliged entity without delay.

Third party referred to in paragraph 1 of this Article shall, at the request of the obliged entity and without delay, submit photocopies of documents and other documentation on the basis of which it carried out customer due diligence measures, as well as the data collected in line with Articles 23 and 24 of this Law where electronic identification or video-electronic identification was performed.

third party referred to in paragraph 1 of this Article shall keep the obtained photocopies of documents and entire documentation obtained during the implementation of customer due diligence and monitoring measures in line with this Law.

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

**Article 34**

Should the obliged entity assess that there is doubt about the credibility of the implemented customer due diligence and monitoring measures by a third party, that is, about the veracity of the obtained data and documentation about the customer, it shall immediately implement those measures.

Obliged entity shall develop an internal act which determines the procedures on

acceptance of the identification of the customer and the beneficial owner of the customer through a third person.

### 3. Obligations during transfer of funds

#### Obligation of the payment service provider of the payer
#### Article 35

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 15)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 22)*

Payment service provider of the payer shall collect data on the payer and the payee and record it in the payment order form or electronic message accompanying the transfer of funds from the payer to the payee.

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

1) name and surname or title;

2) number of the payment account or a unique designation of the transaction if transfer is performed without opening of the payment account;

3) address or registered office, including the name of the country, identity document number, unique personal identification number or taxpayer identification number or date and place of birth.

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

1) name and surname or title;

2) number of the payment account or a unique designation of the transaction if transfer is performed without opening of the payment account;

Notwithstanding paragraph 2 of this Article, in the case of a collective transfer of funds from one payer, the payment service provider of the payer shall not be required, for individual transfers of funds forming part of the collective transfer, to enter the data referred to in paragraph 2 of this Article in the payment order form or electronic message accompanying the transfer of funds, provided that the data referred to in paragraphs 2 and 3 of this Article are contained in the payment order form or electronic message accompanying the collective transfer and that the form or message for each individual transfer of funds contains at least the payment account number of the payer or, where the transfer of funds is carried out without opening a payment account, the unique transaction identifier.

Exceptionally, paragraph 4 of this Article shall not apply to a collective transfer of funds from one of the payers where the payment service provider of the payer and the payment service provider of the payee have their registered office in Montenegro.

Should the amount of the transaction involving funds, including the amount of payment transactions linked to that transfer, be less than EUR 1,000, payment service provider shall ensure that the transfer of funds contains at least the following data:

1) name and surname or the title of the payer and the payee,

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

Payment service provider shall verify the accuracy of collected data on the payer in line with Articles 22, 23, 24, 26, 27 and 28 of this Law, before the transfer of funds.

Payment service provider of the payer shall be deemed to have verified the accuracy of the collected data concerning the payer prior to the transfer of funds where it had

previously established a business relationship with the payer, identified the payer in the manner prescribed by Articles 22, 23, 24, 26, 27 and 28 of this Law and acts in line with Article 49 of this Law.

Notwithstanding of paragraph 7 of this Article, where transfer of funds, including also the amount of money transaction, linked to that transaction is less than EUR 1,000, payment service provider is not obliged to verify the accuracy of data collected on the payer, unless the payment service provider of the payer:

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

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

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

Payment service provider of the payer shall regulate, by internal act, the procedures for verification of completeness of data collected in line with paragraphs 2 to 8 of this Article.

**Obligation of the payment service provider of the**

**payee**

Article 36

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 13)*

Payment service provider of the payee shall verify whether the data on the payer and the payee have been recorded in the payment order form or electronic message accompanying the transfer of funds in line with Article 35 of this Law.

Should the amount of the transaction be EUR 1,000 or more, regardless of whether it is carried out as one transaction or several linked transactions, the payment service provider of the payee shall, before crediting the account of the payee or making the funds available to the payee, verify the accuracy of the data collected on the payee.

Should the amount of funds, including the amount of payment transactions linked to that transaction, be less than EUR 1,000, the payment service provider of the payee need not verify the accuracy of the data collected on the payee, unless:

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

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

Accuracy of the collected data referred to in paragraphs 2 and 3 of this Article shall be verified in line with Articles 22, 23, 24, 26, 27 and 28 of this Law.

Payment service provider of the payee shall implement effective procedures to verify whether the fields relating to the data on the payer and the payee in message exchanges or in the payment and settlement system used to execute the transfer of funds are filled with letters, numbers, and symbols permitted in line with the rules of that system.

Payment service provider of the payee may, in line with the risk assessment, verify the accuracy of data relating to the payee, regardless of the amount of funds transferred.

**Procedure in the event of failure to provide accurate and**

**complete data**

**Article 37**

Payment service provider of the payee shall, in line with the risk assessment, draw up

an internal act prescribing the procedure, including, where applicable, ex-post or real-time monitoring, where the payment order form or electronic message accompanying a transfer of funds does not contain accurate and complete data referred to in Article 35 of this Law.

Should a transfer of funds not contain accurate and complete data referred to in Article 35 of this Law, payment service provider of the payee shall, in line with the internal act referred to in paragraph 1 of this Article and on the basis of risk assessment, determine when to:

1) refuse the transfer of funds;

2) suspend execution of the transfer of funds until the missing data are received, which the payment service provider 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 not recorded in the payment order form or electronic message accompanying the transfer of funds.

Should the payment service provider of the payer repeatedly fail to submit the accurate and complete data in line with Article 35 of this Law, payment service provider of the payee shall warn the provider and determine the date within which the provider needs to bring their conduct in line with this Law.

Should the payment service provider of the payer fail to act in line with paragraph 3 of this Article, the payment service provider of the payee shall refuse future transfers of funds received 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 of any payment service provider of the payer which repeatedly fails to submit accurate and complete data in line with Article 35 of this Law and of the measures taken against that payment service provider in line with paragraphs 3 and 4 of this Article.

Payment service provider of the payee shall establish 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 establishes that this deficiency constitutes grounds for suspicion, notify Financial Intelligence Unit on that in line with Article 66 paragraphs 6, 8 and 10 of this Law.

Should the payment service provider of the payee establish that the deficiency referred to in paragraph 6 of this Article does not constitute grounds for suspicion of money laundering or terrorist financing, it shall make a note which shall be kept in line with this Law.

### Obligations of the intermediary in transfer of funds

Article 38

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

Intermediary in the transfer of funds shall, using a risk-based approach, draw up an internal act prescribing the procedure, including, where applicable, ex-post or real-time monitoring, where the payment order form or electronic message accompanying the transfer of funds does not contain accurate and complete data referred to in Article 35 of this Law.

Should the transfer of funds not contain the accurate and complete data referred to in Article 35 of this Law, the intermediary in transfer of funds shall comply in line with Article

37 paragraphs 2 to 7 of this Law.

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

Article 39

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 14)*

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

when the transfer of funds is made exclusively for the purchase of goods or services using a payment card, a payment instrument used to dispose of electronic money, a mobile telephone 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 the unique identification designation accompany that transfer of funds in such a manner as to enable access to data on the payer using that number or designation, except where the payment card, payment instrument used to dispose of electronic money, mobile telephone or any other digital or information-technology device with similar features is used to carry out transfers of funds between natural persons;

2) during the transfer of funds if the payer withdraws the cash from their account;

3) when taxes, fines and other public duties are paid by transfer of funds, and the payment service provider of the payer and the payment service provider of the payee have their registered offices in Montenegro;

4) when the payer and the payee are payment service providers who act 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 payment is carried out by the transfer of funds to the payee, exclusively upon delivery of goods or provided services, services of electric supply, water supply, services of collecting, treatment and disposal of waste, maintenance of residential buildings or any other similar permanent services which are subject of concluded service contract, if:

- the payment service provider of the payee is an obliged entity for the purpose of this Law,

- the payment service provider of the payee may, through the payee, using the unique transaction identifier or other data accompanying the transfer of funds, access data on the person who concluded a service contract with the payee or a contract for the payment of goods,

- the amount of funds does not exceed the amount of EUR 500,

- the charges for these services are collected by crediting the payment account of the payee used exclusively for those charges, and

- all conditions referred to in Article 40 paragraph 1 of this Law are met.

**Exceptions to the application of customer due diligence and monitoring measures where electronic money is used**

**Article 40**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 23)*

Obliged entity shall not be required, where electronic money is used, to implement the measures referred to in Article 17 paragraph 1 items 1, 2 and 3 of this Law if, on the basis

of the risk assessment, a low risk of money laundering and terrorist financing has been established and if:

1) the payment instrument cannot be reloaded or has a maximum monthly payment limit of EUR 150 and may be used exclusively in Montenegro;
2) the highest amount of a deposit of deposited electronic money does not exceed the amount of EUR 150;

3) the payment instrument is used solely for purchase of goods or services;

4) anonymous electronic money cannot be deposited to the payment instrument,

5) the issuer of electronic money applies appropriate measures for monitoring business relationships and controlling transactions with a view to 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 redemption of electronic money in cash or to the withdrawal of cash in the value of electronic money in an amount exceeding EUR 50, nor to the initiation of a transaction via the internet or using means of distance communication where the amount of the transaction exceeds EUR 50.

Obliged entity may accept payment using an anonymous payment instrument if that payment instrument meets the conditions referred to in paragraph 1 of this Article and if it does not relate to the redemption of electronic money in cash or the withdrawal of cash in the value of electronic money in an amount exceeding EUR 50.

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

## Crypto-Asset-Related Services

### Register of Crypto-Asset Service Providers

### Article 40a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Legal person, business organisation, sole proprietor or natural person with its registered office in Montenegro or residence or approved permanent stay in Montenegro that intends to provide crypto-asset services in Montenegro shall be registered in the Register of Crypto-Asset Service Providers prior to commencing the provision of those services.

Crypto-asset service provider from a Member State of the European Union that is not on the list of high-risk third countries, which has been authorised by the competent supervisory authority of its home state or is registered in the register of the competent supervisory authority of the state in which it was established and intends to provide those services in Montenegro, shall be registered in the Register of Crypto-Asset Service Providers prior to commencing the provision of those services.

Register of Crypto-Asset Service Providers shall be an electronic database in which data on crypto-asset service providers are recorded and stored.

Register of Crypto-Asset Service Providers shall be kept 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 data from the Register of Crypto-Asset Service Providers.

Everyone shall have the right to access data from the Register of Crypto-Asset Service Providers concerning the name or name and surname of the service providers and the crypto-asset services provided by those service providers.

### Registration in the Register of Crypto-Asset Service Providers

**Article 40b**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 24)*

Application 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 referred to in Article 40a paragraph 1 of this Law shall, together with the application, submit:

- data on the name, address, registered office, registration number or other identification number (tax identification number) for legal persons or business organisations, or the name and surname, unique personal identification number, address, and municipality of residence or permanent stay in Montenegro for sole proprietors or natural persons engaged in activity;
- proof of appointment of an compliance officer for the prevention of money laundering and terrorist financing in line with Article 69 of this Law;
- a certificate, confirmation or other act issued by the competent authority, proving good repute in the sense of Article 40r of this Law, for the director, members of the company, members of management and executive bodies and the beneficial owner of the legal person or business organisation or for the sole proprietor or natural person engaged in activity, where any of them is not a Montenegrin citizen;
- a statement from the responsible person in the legal person or business organisation, or from the sole proprietor or natural person conducting the activity, confirming their awareness of the obligations under this Law;
- information on all directors of the legal person or business organisation as prescribed in Article 117 paragraph 1 item 3 of this Law;
- a business plan setting out the crypto-asset services that the provider intends to offer, including a plan on how these services will be marketed.

Notwithstanding paragraph 2 indent 3 of this Article, the certificate, confirmation or other official document issued by the competent authorities, proving good repute as defined in Article 40r of this Law, for the director, members of the company, members of management and executive bodies and the beneficial owner of the legal person or business organisation, or the sole proprietor or natural person conducting the activity, in the case they are Montenegrin citizens, shall be obtained ex-officio by the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law.

Crypto-asset service provider referred to in Article 40a paragraph 2 of this Law shall submit, together with the application, the following:

- information on the name, address, registered office, registration number or other identification number (tax identification number) for legal persons or business organisations, or the name and surname, date of birth, country of birth, type, number and country of issuance of identity document, and residence address in Montenegro for sole proprietors or natural persons conducting business activities;
- a confirmation of approval from the competent supervisory authority or an extract from the register of the competent supervisory authority of the state in which the entity was established;
- proof of the crypto-asset services for which the entity is registered in the state of its establishment;
- name and contact details of the competent supervisory authority of the state in which the entity was established;

- a business plan setting out the crypto-asset services that the provider intends to offer, including a plan on how these services will be marketed.

Good repute referred to in paragraph 2 indent 3 and paragraph 3 of this Article shall be established by the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law, in line with Article 40r of this Law.

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 competent authorities in Montenegro, as well as through channels of international cooperation, after which it shall decide on the application for registration in the Register of Crypto-Asset Service Providers.

Legal person or business organisation referred to in Article 40a paragraph 1 of this Law may not be registered in the Register of Crypto-Asset Service Providers unless it is registered in the Register of Beneficial Owners.

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall reject the application for registration in the Register of Crypto-Asset Service Providers if the applicant fails to submit the data and documentation referred to in paragraph 2 or paragraph 4 of this Article, or if the conditions referred to in paragraphs 6 and 7 of this Article are not fulfilled.

Decision rejecting the application for registration in the Register of Crypto-Asset Service Providers may be challenged in an administrative dispute.

**Contents of the Register of Crypto-Asset Service Providers**

**Article 40c**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

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

1) for a legal person or a business organisation: name, registered office (address and city, or municipality for a legal person with its registered office in Montenegro; and country and city for a legal person with its registered office in another state), registration number, indication of whether it is a resident or non-resident, telephone number, email address and the information referred to in Article 44 of this Law;
2) for a sole proprietor: name, registered office (address and city or municipality for a sole proprietor with registered office in Montenegro and, for a sole proprietor with registered office in another country, country and city), unique personal identification number, name and surname, information on whether they are a resident or non-resident, telephone number and e-mail address;
3) for a natural person: name and surname, unique personal identification number, address and municipality of permanent or temporary residence in Montenegro, date of birth, country of birth, nationality, indication of whether the person is a resident or non-resident, telephone number and email address, type, number, country of issuance and expiry date of the identity document; and
4) information on the name of the crypto-asset services it provides in Montenegro.

**Deletion from the Register of Crypto-Asset Service Providers**

**Article 40d**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall issue a decision on the removal of a provider of crypto-asset services from the Register of Crypto-Asset Service Providers if:

1) the provider submits a notification to the supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law stating that it 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) they no longer meet the requirement of good repute within the meaning of Article 40b paragraph 2 indent 3 and paragraph 3 of this Law;

4) they do not meet the obligations set out in Article 40f of this Law; or

5) they do not provide crypto-asset services within 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 it suspects meets any of the conditions for deletion referred to in paragraph 1 items 2 to 5 of this Article and shall notify the service provider thereof.

Deactivation referred to in paragraph 2 of this Article shall remain in effect 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 have been met. If it determines that any of those conditions have been met, the supervisory authority shall delete the crypto-asset service provider from the Register of Crypto-Asset Service Providers. If it determines that none of those conditions have been met, it shall lift the deactivation.

Crypto-asset service provider shall not provide crypto-asset services while its status is deactivated.

Decision on deletion from the Register of Crypto-Asset Service Providers may be challenged in an administrative dispute.

**Provision of Crypto-Asset Services in Montenegro**

**Article 40e**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset services shall be deemed to be provided in Montenegro if any of the following conditions are met, namely if the crypto-asset service provider:

- has its registered office in Montenegro or is a resident or has a place of business in Montenegro from which the services are provided;
- provides crypto-asset services, advertises its services or directs a marketing campaign—regardless of the method of advertising—towards persons having their registered office or residence in Montenegro;
- offers crypto-assets in Montenegro via one or more automated systems;
- distributes its services through one or more distribution channels targeted at persons having their registered office or residence in Montenegro;
- has a mailing address or telephone number in Montenegro or uses the “.me” domain extension on its website.

**Obligations of the Crypto-Asset Service Provider of the Originator**

**Article 40f**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset service provider of the originator shall, at the time of the transfer of crypto-assets, ensure that information on both the originator and the beneficiary of the crypto-assets is provided.

Information on the originator shall include:

1) name and surname or the title;

2) the address or registered office, including the name of the country, the identity document number, the unique personal identification number or registration number of the originator or their date and place of birth;

3) the distributed ledger address, where the transfer of crypto-assets of the originator is recorded on a network using distributed ledger technology (DLT) or similar technology, as well as the crypto-asset account number, if such an account exists and is used to process the transaction;

4) the crypto-asset account number, in cases where the transfer of crypto-assets of the originator is not recorded on a network using DLT or similar technology.

5) the existing Legal Entity Identifier (LEI), where the relevant message format includes a dedicated field and where the originator has provided it to their crypto-asset service provider; in the absence of such a number, any other available and equally reliable official identification of the originator.

Information on the beneficiary of the crypto-assets shall include:

1) name and surname or the title;

2) the distributed ledger address of the beneficiary, where the transfer of crypto-assets is recorded on a network using distributed ledger technology (DLT) or similar technology, as well as the crypto-asset account number, if such an account exists and is used to process the transaction;

3) the crypto-asset account number of the beneficiary, in cases where the transfer of crypto-assets is not recorded on a network using DLT or similar technology;

4) the existing Legal Entity Identifier (LEI), where the relevant message format includes a dedicated field and where the originator has provided it to their crypto-asset service provider; in the absence of such a number, any other available and equally reliable official identification of the originator.

Notwithstanding paragraph 2 item 4 and paragraph 3 item 3 of this Article, where the transfer of crypto-assets is neither recorded on a network using distributed ledger technology (DLT) or similar technology nor made to or from a crypto-asset account of the originator, the crypto-asset service provider of the originator shall ensure that a unique transaction identifier is attached to the crypto-asset transfer.

Information on the originator and the beneficiary referred to in paragraphs 2 and 3 of this Article does not need to be directly included in the crypto-asset transfer.

Information referred to in paragraphs 2 and 3 of this Article shall be transmitted to another crypto-asset service provider of the originator prior to, simultaneously with or in parallel with the execution of the crypto-asset transfer, in a manner that ensures the protection of such data in line with the law governing personal data protection.

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

Crypto-asset service provider of the originator shall, in addition to the measures referred to in Article 53c of this Law and in the case of a transfer exceeding EUR 1,000 to a self-hosted

address, take appropriate measures to assess whether that address is owned or controlled by the originator.

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

Verification of information referred to in paragraphs 2 and 3 of this Article shall be considered to have been carried out if any of the following conditions are met:

1) the identity of the originator of the crypto-assets has been verified in line with Article 17 of this Law and the information obtained through that verification is retained in line with Article 127 of this Law;

2) that Article 18 paragraph 2 of this Law applies to the originator of crypto-assets.

Crypto-asset service provider of the originator shall not initiate or execute the crypto-asset transfer if the conditions set out in paragraphs 1 to 10 of this Article have not been met.

**Transfer of Crypto-Assets via Batch File**

**Article 40g**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Provision of Article 40f paragraph 2 of this Law shall not apply to individual transfers consolidated in a batch file from a single originator, provided that:

1) the batch file contains the information referred to in Article 40f paragraphs 2, 3 and 4 of this Law;

2) the information has been verified in line with Article 40f paragraph 9 of this Law;

3) individual transfers contain the distributed ledger address of the originator, where Article 40f paragraph 3 item 2 of this Law applies;

4) the crypto-asset account number of the originator, where Article 40f paragraph 3 item 3 or paragraph 4 applies, contains a unique transaction identifier.

**Obligations of the Crypto-Asset Service Provider of the Crypto-Asset Beneficiary**

**Article 40h**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset service provider of the crypto-asset beneficiary shall implement effective procedures, including, where appropriate, real-time or post-transfer monitoring, in order to determine whether the information on the originator and the beneficiary referred to in Article 40f paragraphs 2, 3 and 4 of this Law has been included in the crypto-asset transfer, in the batch transfer files or has been submitted subsequently.

Crypto-asset service provider of the crypto-asset beneficiary shall, in the case of a crypto-asset transfer originating from a self-hosted address, obtain and retain the information referred to in Article 40f paragraphs 2, 3 and 4 of this Law and ensure that the crypto-asset transfer is individually identifiable.

Crypto-asset service provider of the crypto-asset beneficiary shall, in addition to the measures set out in Article 53c of this Law and for transfers exceeding EUR 1,000 originating from a self-

hosted address, take appropriate measures to assess whether such address is owned by or under the control of the crypto-asset beneficiary.

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

Verification referred to in paragraphs 2, 3 and 4 of this Article shall be deemed to have been carried out if one of the following conditions is met:

1) the identity of the crypto-asset beneficiary has been verified in line with Article 17 of this Law, and the information obtained through such verification is retained in line with Article 127 of this Law;

2) the provision of Article 18 paragraph 2 of this Law applies to the crypto-asset beneficiary.

**Transfers of Crypto-Assets with Missing or Incomplete Information**

**Article 40i**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset service provider of the crypto-asset beneficiary shall implement effective risk-based procedures, including the measures set out in Article 17 of this Law, to determine whether a transfer of crypto-assets with missing or incomplete required information on the originator and the beneficiary should be executed, rejected, returned or suspended and shall take appropriate follow-up actions.

Should the service provider referred to in paragraph 1 of this Article determine that the information referred to in Article 40f paragraphs 2, 3 and 4 or Article 40g of this Law is missing or incomplete, it shall, on the basis of a risk assessment and without undue delay:

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

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

Should the crypto-asset service provider of the originator persistently fail to provide the required information on the originator or the beneficiary, the crypto-asset service provider of the crypto-asset beneficiary shall:

1) take measures including, in particular, sending warnings and setting deadlines before rejecting, restricting or terminating the business relationship in line with item 2 of this paragraph, if the information remains outstanding; or

2) directly reject all future crypto-asset transfers from that service provider, restrict or terminate the business relationship with it.

Crypto-asset service provider of the crypto-asset beneficiary shall notify the competent supervisory authority of any crypto-asset service provider of the originator who persistently fails to provide accurate and complete information in line with this Article, as well of the measures taken against that service provider in line with paragraphs 1, 2, and 3 of this Article.

**Assessment and Reporting**

**Article 40j**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset service provider of the crypto-asset beneficiary shall determine whether the lack of accurate and complete information referred to in Article 40i of this Law constitutes grounds for suspicion of money laundering or terrorist financing and, if it determines that such lack constitutes grounds for suspicion, shall notify the Financial Intelligence Unit thereof in line with this Law.

**Obligations of Intermediary Crypto-Asset Service Providers**

**Article 40k**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Intermediary crypto-asset service provider shall ensure that all information regarding the originator and the beneficiary of the crypto-asset transfer, which is required to accompany the transfer, is effectively transmitted alongside the crypto-asset transfer.

Intermediary crypto-asset service provider shall keep records of the information referred to in paragraph 1 of this Article and shall make such records available to the competent authorities upon request.

**Determination of Missing Information on the Originator or the Crypto-Asset Beneficiary**

**Article 40l**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Intermediary crypto-asset service provider shall implement effective procedures, including, where appropriate, monitoring during or after the transfer of crypto-assets, in order to determine whether the information 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 has been provided prior to, simultaneously with, or in parallel to the crypto-asset transfer or the transfer via batch files, including in cases where the transfer is carried out from or to a self-hosted address.

**Crypto-Asset Transfers with Missing or Incomplete Information on the Originator or the Crypto-Asset Beneficiary**

**Article 40m**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Intermediary crypto-asset service provider shall establish effective risk-based procedures, including the measures referred to in Article 17 of this Law, to determine whether to execute, reject, return or suspend a transfer of crypto-assets for which the required and complete information on the originator and the beneficiary is missing and to take appropriate measures.

Should the service provider referred to in paragraph 1 of this Article, when receiving a transfer of crypto-assets, determine that the information 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 is missing or incomplete, it shall, on the basis of a risk assessment and without undue delay:

1) reject the transfer or return the transferred crypto-assets, or

2) request the required information on the originator and the beneficiary prior to continuing the transfer of crypto-assets.

Should the crypto-asset service provider persistently fail to provide the required information on the originator or the beneficiary, the intermediary crypto-asset service provider shall:

1) take measures including, in particular, sending warnings and setting deadlines before rejecting, restricting or terminating the business relationship in line with item 2 of this paragraph, if the information remains outstanding, or

2) directly reject all future crypto-asset transfers from that service provider, restrict or terminate the business relationship with it.

Intermediary crypto-asset service provider shall inform the competent supervisory authority of any crypto-asset service providers who persistently fail to provide accurate and complete information and of the measures taken against that service provider in line with paragraphs 1 to 3 of this Article.

**Assessment and Reporting**

**Article 40n**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Intermediary crypto-asset service provider shall determine whether the lack of accurate and complete information referred to in Article 40m of this Law during the transfer of crypto-assets or transactions related thereto constitutes grounds for suspicion of money laundering or terrorist financing and, if it determines that such shortcoming presents grounds for suspicion, it shall notify the Financial Intelligence Unit thereof in line with this Law.

**Exemptions from the Obligation to Collect Data on the Originator and the Crypto-Asset Beneficiary**

**Article 40o**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

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

- the originator and the crypto-asset beneficiary are crypto-asset service providers acting on their own behalf and for their own account; or
- the transfer is a person-to-person transfer of crypto-assets.

**Submission of Information**

**Article 40p**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Crypto-asset service providers shall, fully and without delay, including via the single point of contact referred to in Article 62 paragraph 8 of this Law, submit data collected in line with this Law only to competent authorities and competent supervisory authorities, at the request of those authorities.

Provision of paragraph 1 of this Article shall also apply to payment service providers.

**Reputation**

**Article 40r**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 15)*

Reputation, for the purposes of this Law, shall be attributed to a natural person provided that:

1) no criminal proceedings are conducted against them nor have they been convicted of a criminal offence punishable by a non-suspended imprisonment of one year or more;
2) no criminal proceedings are conducted against them nor have they been convicted of offences under the laws of other states which, by their description and legal nature, correspond to the offences referred to in paragraph 1 item 1 of this Article;
3) they have not, in their capacity as a legal representative of a legal person or business organisation, violated the provisions of this Law;
4) they are not an associate of any person convicted of money laundering and/or terrorist financing;
5) they have not had their consent or authorisation to perform activities revoked or refused by the competent authority due to non-compliance with regulations;
6) they do not currently manage, and at the time of commission of the offence did not manage, a legal person or business organisation that has been finally convicted of offences referred to in paragraph 1 items 1 and 2 of this Article and particularly have not been subject to a security measure prohibiting the exercise of their profession, activity or duty.
7) there is no suspicion that the person has committed the criminal offence of money laundering or terrorist financing.

Term “criminal offence” referred to in paragraph 1 item 1 of this Article shall be considered as any of the following offences: criminal offences against payment transactions and business operations, criminal offences against life and limb, criminal offences against freedoms and rights of individuals and citizens, criminal offences against labour rights, criminal offences against environment and spatial planning, criminal offences against general safety of people and property, criminal offences against security of computer data, criminal offences against legal procedures, criminal offences against intellectual property, criminal offences against official duty.

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall, when assessing the circumstances referred to in paragraph 1 of this Article, take into account all available information related to the type of decision, the stage of the proceedings and any legal remedies invoked, the sanctions imposed, mitigating and aggravating circumstances, the gravity of the offence, the time elapsed since the commission of the offence and the conduct of the natural person during that period, all available information concerning proceedings, supervisory measures and reports submitted by supervisory authorities in line with Article 131 paragraph 1 of this Law or by equivalent supervisory bodies from other states, as well as the fact that the existence of multiple minor offences under this Law collectively may impair the reputation of the natural person, even if individually they do not have such an effect.

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall, when assessing the circumstances referred to in paragraph 1 of this Article, give particular consideration to data and information obtained from the Financial Intelligence Unit.

## 4. Identification of the Beneficial Owner

### Beneficial Owner

### Article 41

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 16)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 25)*

Beneficial owner shall be a natural person who ultimately owns or exercises effective control over a legal person, business organisation, trust, another person or an equivalent entity under foreign law, or a natural person on whose behalf or for whose account a transaction is executed or a business relationship is established.

Beneficial owner of a legal person or business organisation, for the purposes 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 the legal person or business organisation, including the right to a share in profits, other internal resources or the liquidation balance; or
2) directly or indirectly exercises decisive influence over the business operations and decision-making of the legal person or business organisation through an ownership interest; or
3) controls the legal person or business organisation by other means.

Should the holder of at least 25% of shares, voting rights or other rights in a legal person, business organisation, trust, another person or an equivalent entity under foreign law be a legal person, business organisation, trust, another person or an equivalent entity under foreign law, the specific shareholder structure, including whether a natural person exercises control over the shareholder by other means, shall be taken into account when identifying the beneficial owner.

Natural person who is jointly and severally and without limitation liable for claims and other obligations of a partnership or another legal person or business organisation shall be considered the beneficial owner of that legal person or business organisation, regardless of the percentage of shares or voting rights held by that natural person in the legal person or business organisation.

Beneficial owner based on control of a legal person or business organisation by other means shall be identified independently and concurrently with the identification of the beneficial owner referred to in paragraph 2 items 1 and 2 of this Article.

Person shall in any event be deemed to control a legal person or business organisation by other means where that person has:

- a majority of voting rights, regardless of how those rights are divided among natural persons acting jointly;
- the right to appoint or remove the majority of members of the management body, including members of the board of directors, supervisory board, management board or equivalent officers;
- veto rights or other relevant decision-making rights linked to ownership of the legal person or business organisation;

- the right to decide on the distribution of profits or changes in the assets of the legal person or business organisation.

Control of a legal person or business organisation by other means may, depending on its organisational form, include, but shall not be limited to, decision-making rights arising from:

- formal or informal agreements with owners or with the legal person or business organisation, provisions of the articles of association, partnership agreements, syndicate agreements or similar documents or arrangements, depending on the specific characteristics of the legal person or business organisation;
- family relationships;
- use of formal or informal nominee arrangements.

Should no natural person be identified as the beneficial owner after all measures referred to in paragraphs 2 and 3 of this Article have been taken, all persons holding managerial positions in that legal person or business organisation shall be considered beneficial owners.

Beneficial owner of an association, non-governmental organisation, institution, political party, religious community, artistic organisation, chamber, trade union, employers organisation or another business entity shall be any natural person exercising a controlling role in the management of the assets of that entity.

Should no natural person be identified as the beneficial owner after all measures referred to in paragraph 9 of this Article have been taken, beneficial owner of an association, non-governmental organisation, institution, political party, religious community, artistic organisation, chamber, trade union, employers organisation or another business entity shall be any natural person authorised to represent that entity.

Beneficial owner of a trust, another person or an equivalent entity under foreign law shall be:

1) the settlor of the trust;
2) the trustee;
3) the protector of the trust or another person representing the interests of beneficiaries of assets derived from the trust;
4) the beneficiary of assets derived from the management of the assets, future beneficiaries where already designated or ascertainable and, where beneficiaries have not yet been designated, the category of beneficiaries and its general characteristics, whereby beneficiaries within that category shall be considered beneficial owners as soon as they are identified or designated;
5) any other natural person who otherwise directly or indirectly controls the trust assets, including any other natural person exercising ultimate control over the trust through direct or indirect ownership or by other means, including through a chain of control or ownership.

Should any person referred to in paragraph 11 items 1 to 5 of this Article be a legal person, business organisation, trust, another person or an equivalent entity under foreign law, beneficial ownership shall be identified taking into account the specific ownership structure, including whether a natural person exercises control over the owner by other means.

Beneficial owner of a foundation shall be a natural person who:

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

Should the founder of a foundation, a member of its management body or a member of its supervisory body be a legal person, business organisation or arrangement, beneficial owners of

that legal person, business organisation or arrangement shall be deemed to be the beneficial owners of the foundation.

Should a natural person who is a beneficiary of a foundation not be identified, the category of beneficiaries in whose principal interest the foundation was established or operates shall be identified so that beneficiaries within that category are deemed to be beneficial owners as soon as they are identified or designated.

**Manner of identifying a beneficial owner**

**Article 42**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 17)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 26)*

Obliged entity shall identify the beneficial owner of a legal person, business organisation, trust, another person or an equivalent entity under foreign law by obtaining data on those customers and their beneficial owners.

Obliged entity may obtain the data referred to in paragraph 1 of this Article by consulting the registers referred to in Articles 43 and 43a of this Law, the CRPS or another relevant public register, as well as a court, business or other public register in which a foreign legal person or business organisation is registered, and shall retain an extract from that register in electronic form or print it and mark it with the date and time and the name and surname of the person who consulted it.

Obliged entity may also obtain the data referred to in paragraph 1 of this Article by inspecting the original or certified photocopy of a document from the Central Registry of Business Entities or another relevant public register, as well as the original or certified photocopy of a document from the court, business or other public register in which the foreign legal person or business organisation is registered, which must not be older than three months from the date of issue.

Should the obliged entity, when verifying the data on the beneficial owner in line with paragraphs 2 and 3 of this Article, establish that there is a discrepancy in the data, it shall require the customer to correct the data in the register within eight days. Should the customer fail to do so within the prescribed time limit, the obliged entity shall, without delay, submit to the Financial Intelligence Unit and the administrative authority competent for tax collection the data that differ and the data on the persons whom it considers to be the beneficial owners of the customer.

Obliged entity shall obtain data not included in the registers or documents referred to in paragraphs 2 and 3 of this Article by inspecting the original or certified photocopy of the document or other documentation submitted by the representative or authorised person of a customer that is a legal person or business organisation.

Obliged entity shall, in addition to the data referred to in paragraph 1 of this Article, obtain documentation on the basis of which the ownership structure and controlling member of the customer and the data on the beneficial owner can be established.

Obliged entity shall verify the data on the beneficial owner of a legal person, business organisation, trust, another person or an equivalent entity under foreign law which it has obtained in such a manner as to provide a complete and clear insight into the beneficial ownership and management body of the customer in line with the risk assessment and shall not rely solely on data from the register referred to in Article 43 paragraph 1 of this Law.

Obliged entity shall, when identifying the beneficial owner referred to in paragraph 1 of this Article, obtain a photocopy of the personal identification document of the beneficial owner in line with Article 22 paragraph 3 of this Law.

Should an obliged entity, when collecting data referred to in paragraphs 2, 3, 5, 6 and 7 of this Article, suspect that the obtained data are untrue or that the documents or other documentation from which the data were obtained are not authentic, it shall obtain a written statement thereon from the representative or authorised person of the customer.

Obliged entity shall retain the original, certified photocopy and extract referred to in paragraphs 2, 3, 5 and 6 of this Article in its documentation.

Obliged entity shall keep records of the measures it has taken to establish the beneficial owner referred to in paragraph 1 of this Article.

## Register of Beneficial Owners

### Article 43

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 18)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 27)*

Register of Beneficial Owners shall be an electronic database in which beneficial ownership data are recorded and retained for the purpose of ensuring transparency of ownership structures and implementing measures for the prevention of money laundering and terrorist financing.

Administrative authority competent for tax collection shall maintain the Register of Beneficial Owners.

Legal person, business organisation, part of a foreign business organisation, association, non-governmental organisation, institution, political party, religious community, artistic organisation, chamber, trade union, employers organisation, foundation or another business entity, legal person receiving, managing or allocating funds for specific purposes, trust, another person or an equivalent entity under foreign law receiving, managing or distributing assets for specific purposes shall enter data on beneficial owners and changes thereto in the Register of Beneficial Owners within eight days of the date of their entry in the CRPS or the register of taxpayers, or within eight days of a change in beneficial ownership data.

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

- a sole proprietor;

- the public sector within the meaning of the law governing time limits for settlement of financial obligations;

- legal persons and business organisations that are multi-member joint-stock companies whose shares are traded on an organised securities market and that are required to comply with the obligation to disclose beneficial ownership data and information in line with the law governing the rights and obligations of entities on the securities market and another law.

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

Beneficial owner of an entity referred to in paragraph 3 of this Article shall provide that entity with the data referred to in Article 44 paragraph 1 item 2 indents 1, 2 and 4 of this Law for entry in the Register of Beneficial Owners.

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

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

Entities referred to in paragraph 3 of this Article shall designate at least one natural person employed by the entity and having permanent residence or permanent stay in Montenegro, or a business organisation registered in Montenegro that is an obliged entity under Article 4 paragraph 2 item 13 indent 2 and paragraph 3 of this Law, to be authorised to enter data in the Register of Beneficial Owners. Designated person or business organisation shall provide the Financial Intelligence Unit, competent authorities referred to in Article 96 paragraph 1 and supervisory authorities referred to in Article 131 paragraph 1 of this Law with all available beneficial ownership information and shall assist those authorities, at their request, in obtaining additional data and information on beneficial owners.

Trustee referred to in Article 43a paragraph 7 of this Law shall, at the request of the Financial Intelligence Unit, competent authorities referred to in Article 96 paragraph 1 and supervisory authorities referred to in Article 131 paragraph 1 of this Law, provide without delay and no later than three days of the date of receipt of the request all information on the trust, beneficial ownership of the trust and trust assets that the trustee administers or manages.

## Register of Trusts

### Article 43a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 19)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 28)*

Register of Trusts shall be an electronic database in which data on trusts, other persons or equivalent entities under foreign law are recorded and retained.

Administrative authority competent for tax collection shall maintain the Register of Trusts.

Register of Trusts shall contain data referred to in Article 44 paragraph 1 item 3 of this Law.

Data on a trust, another person or an equivalent entity under foreign law shall be entered in the Register referred to in paragraph 1 of this Article where the trustee enters into a business relationship or acquires real estate on behalf of the trust, another person or equivalent entity under foreign law, within five days from the date of entering into the business relationship or acquiring the real estate.

Person with whom the trustee has entered into a business relationship or the notary where the trustee acquires real estate on behalf of the trust, another person or equivalent entity under foreign law shall submit the request for entry in the Register of Trusts to the administrative authority competent for tax collection within five days from the date on which that person entered into the business relationship or the date on which

the notarial deed relating to the acquisition of real estate was drawn up.

Following entry in the Register of Trusts, the trust, another person or equivalent entity under foreign law shall also be entered in the Register of Beneficial Owners.

Trustee shall enter the trust, another person or equivalent entity under foreign law in the Register of Beneficial Owners within eight days from the date of entering into the business relationship or acquiring the real estate.

Notwithstanding paragraph 6 of this Article, where the trustee has a residence or registered office in more than one other state, or where the trustee acquires real estate or establishes multiple business relationships in more than one other state on behalf of the trust, another person or equivalent entity under foreign law, a certificate as proof of registration or an extract containing beneficial ownership information retained in the register of one of those other states may be considered sufficient proof of compliance with the obligation to enter the trust, another person or equivalent entity under foreign law in the Register of Beneficial Owners.

## Content of the Register of Beneficial Owners

### Article 44

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 20)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 29)*

Register of Beneficial Owners shall contain the following data:

1) data on the entity referred to in Article 43 paragraph 3 of this Law:

- name, address, registered office, address of the place of business where it differs from the registered office, registration number or another identification number, tax identification number (hereinafter referred to as: “the TIN”), date of registration and date of deletion from the CRPS or the register of taxpayers,
- data on their status,
- form of organisation,
- codes of activity,
- data on the representative, proxy or authorised person (name and surname, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship),
- data on natural person who is registered as a member of managing authority (name and surname, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship),
- the amount of the basic (registered) capital,
- data on members or founders and percentage of their ownership interest or the number and percentage of their shares (name and surname, unique personal identification number, date of birth, address of permanent or temporary residence, TIN, citizenship, ownership share-percentage of shares and percentage of capital share or data on percentage of direct or indirect of disposal of property or data on percentage on the incomes of the user from the property they manages or the share in the property of the legal person or other foreign subjects),
- graphic representation of the ownership structure, a description of the ownership

structure including the names and TINs of individual entities forming part of that ownership structure and a description of the relationships between them, including information on their ownership interests, where the entity has a complex ownership structure,

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

2) data on the beneficial owner, as follows:

- name and surname, unique personal identification number, date and place of birth, address of permanent or temporary residence, TIN, citizenship, type, number and issuing state of the identity document,
- data on ownership share (percentage of shares or percentage of capital share or data on percentage of direct or indirect disposal of property or data on percentage of income of the user from the property he manages to or property share of the legal person or other foreign subject) or other type of control (data on that whether the owner has deciding influence in property management, whether they directly provide or have provided assets or they have decisive influence to decision making or has a control status in management),
- date of acquisition of the ownership interest or another type of control;
- date of registration, date of change or date of updating and deletion of the beneficial owner from the Register of Beneficial Owners,
- scanned documentation which proves the entered data,

3) data on the beneficial owner of a trust, another person or an equivalent entity under foreign law, namely data on:
- the settlor of the trust;
- the trustee;
- the protector of the trust;
- the beneficiaries of the trust funds;
- persons with an interest in establishing the trust;
- persons who directly or indirectly control the assets of the trust.

Should a person referred to in paragraph 1 item 3 of this Article be a natural person, the data shall comprise name and surname, unique personal identification number, date and place of birth, address of permanent or temporary residence, TIN, citizenship, type, number and issuing state of the identity document. Where that person is a legal person, the data shall comprise name, address, registered office, address of the place of business where it differs from the registered office, registration number or another identification number, TIN, date of registration and date of deletion from the CRPS or the register of taxpayers.

Data referred to in paragraph 1 items 1 and 2 or item 3 of this Article shall be included in an extract from the Register of Beneficial Owners issued by the administrative authority competent for tax collection.

### Entering data in the Register of Beneficial Owners

### Article 45

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 16)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 21)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 30)*

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

1) referred to in Article 44 paragraph 1 item 1 of this Law,

2) about the beneficial owner referred to in Article 44 paragraph 1 item 2 of this Law;

3) data on the beneficial owner of a trust, another person or an equivalent entity under foreign law referred to in Article 44 paragraph 1 item 3 of this Law.

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

- a note on existence of a complex ownership structure of that entity,
- document in electronic form which includes graphics of the ownership structure,
- original or certified photocopy of a document from the CRPS or another relevant public register and an original or certified photocopy of a document from a court, business or other public register in which a foreign legal person or business organisation is entered, not older than three months from the date of issue, in electronic form, for every legal person, trust or legal arrangement included in the ownership structure;
- data on the owner that is a legal person, legal arrangement or another entity under foreign law (name, address, registered office, country of registered office, registration number or another identification number and TIN).

Complex ownership structure, for the purpose of paragraph 2 of this Article, means an ownership structure in which at least one legal person, legal arrangement or another entity under foreign law is the founder or owner of an entity referred to in Article 43 paragraph 3 of this Law.

Manner of entering and updating the data from the Register of Beneficial Owners as well as detailed contents of the scanned documentation shall be defined by the Ministry.

**Maintaining and managing the Register of Beneficial Owners**

**Article 46**

Administrative authority competent for tax collection shall maintain and manage the Register of Beneficial Owners so that:

- in addition to the latest entry of data referred to in Article 44 of this Law, retain all previous entries from the date of registration, as well as all amendments and deletions of data, according to the time and type of change;
- make the latest data entered available to obliged entities whenever they need them;
- provide the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law and other authorities competent for the prevention and detection of money laundering and related predicate offences or terrorist financing with unlimited access to all data retained in the Register of Beneficial Owners;
- make the data available for five years after deletion of an entity referred to in Article 43 paragraph 3 of this Law from the CRPS or the register of taxpayers to the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law and other authorities competent for the prevention and

detection of money laundering and related predicate offences or terrorist financing.

## Access to Data from the Register of Beneficial Owners

### Article 47

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 17)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 31)*

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

1) the Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law and competent authorities referred to in Article 96 paragraph 1 of this Law;

2) obliged 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 in the Register of Beneficial Owners and may exchange them with the Financial Intelligence Unit, supervisory authorities and other competent authorities of other Member States of the European Union in line with this Law, in a timely manner and without charge.

Obliged entities shall have direct electronic access to all data referred to in Article 44 paragraph 1 of this Law for the purpose of identifying the beneficial owner.

Other legal persons 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 on the basis of electronic identification in line with the law regulating electronic identification, namely name and surname, year of birth, citizenship, country of residence, type and extent of the ownership interest.

Entities referred to in Article 43 paragraph 3 of this Law may submit to the administrative authority competent for tax collection a request to restrict or deny legal and natural persons referred to in paragraph 1 item 3 of this Article access to all or part of the data referred to in paragraph 4 of this Article if access to those data would expose the beneficial owner to the risk of fraud, abduction, 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 Financial Intelligence Unit establishes that those circumstances exist, administrative authority competent for tax collection shall restrict or deny access to all or part of the data to which the request referred to in paragraph 5 of this Article relates.

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

Ministry shall prescribe in detail the manner of accessing data in the Register of Beneficial Owners.

## Supervision of Entry of Data

### Article 48

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 22)*

When supervising entities referred to in Article 43 paragraph 3 of this Law, administrative authority competent for tax collection shall verify whether:

- those entities have the data on the beneficial owner referred to in Article 44 paragraph 1 item 2 of this Law and whether those data are complete and identical to data from reliable sources;

- those entities have entered the data referred to in the first indent of this paragraph in the Register of Beneficial Owners within the time limits prescribed by this Law.

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

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

Should, during the supervision referred to in paragraph 1 of this Article, administrative authority competent for tax collection identify discrepancies between data in the Register of Beneficial Owners and data from reliable sources, it shall order the entity referred to in Article 43 paragraph 3 of this Law to correct the errors in the Register and shall, until the errors are corrected, mark the data on that entity in the Register as not updated.

Entity referred to in Article 43 paragraph 3 of this Law shall comply with the order referred to in paragraph 4 of this Article within three working days from the date of receipt of that order.

### International Exchange of Beneficial Ownership Data

### Article 48a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 32)*

Administrative authority competent for tax collection shall connect the Register of Beneficial Owners and the Register of Trusts to the European Central Platform through the system of interconnection of registers and shall ensure that data and documentation from those registers remain available for five years following deletion of the registered entity from those registers.

## 5. Monitoring of the Business Relationship, Scrutiny of Transactions and Repeated Annual Review

### Monitoring of the Business Relationship and Scrutiny of Transactions

### Article 49

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 23)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 33)*

Obliged entity shall implement measures for monitoring the business relationship with the customer, including scrutiny of transactions and monitoring the source of funds used

by the customer in carrying out business, and shall collect data referred to in Article 117 paragraph 1 items 1, 2, 3, 6 and 7 and paragraphs 3 to 6 of this Law, depending on the type of obliged entity.

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

1) verification of compliance of the business of the customer with nature and purpose of the business relationship,

2) verification of transactions according to the risk profile of the customer in relation to money laundering and terrorist financing,

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

4) verification of the source and destination of funds used by the customer in carrying out business or a transaction, in line with the risk of money laundering and terrorist financing relating to the customer;

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

Obliged entity shall ensure and adjust the scope and frequency of implementing measures referred to in paragraph 1 of this Article to the risk of money laundering and terrorist financing to which the obliged entity is exposed when carrying out an individual activity or conducting business with the customer.

Obliged entity may update data on the customer and the beneficial owner of the customer and verify whether the customer or the beneficial owner of the customer has become or ceased to be a politically exposed person by consulting the CRS, records of issued identity documents, the Register of Beneficial Owners, the CRPS, the register referred to in Article 55 paragraph 1 of this Law or another relevant public register or by inspecting an original or certified photocopy of a document from the CRPS or another relevant public register.

Obliged entity shall verify data in the CRS referred to in paragraph 4 of this Article only in respect of its customers.

Obliged entity shall obtain data not contained in the registers, records and documents referred to in paragraph 4 of this Article by inspecting an original or certified photocopy of a document or other documentation submitted by the customer at the request of the obliged entity.

Should, when verifying data referred to in paragraphs 4 and 5 of this Article, obliged entity identify a discrepancy in the data, it may invite the customer to verify all relevant information.

Obliged entity shall ensure that the frequency of monitoring the business relationship with the customer referred to in paragraph 3 of this Article does not exceed one year for a higher-risk customer or five years for a lower-risk customer.

## Annual Review

### Article 50

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 34)*

Obliged entity shall, in addition to monitoring the business relationship and scrutinising transactions in line with Article 49 of this Law, at least once a year and no later than one

year after the last review, review the customer that is:

-a foreign legal person that carries out transactions with the obliged entity referred to in Article 18 paragraph 1 items 2, 3, 4, 6, 7 and/or 9 of this Law;

-a legal person with its registered office in Montenegro in which the foreign capital participation is at least 25% that carries out transactions with the obliged entity referred to in Article 18 paragraph 1 items 2, 3, 4, 6, 7 and/or 9 of this Law.

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

1) obtaining or verifying data referred to in Article 117 of this Law;

2) obtaining or verifying data referred to in Article 44 of this Law;

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

Should a business unit of a foreign legal person carry out transactions referred to in Article 18 paragraph 1 items 2, 3, 4, 6, 7 and/or 9 of this Law on behalf and for the account of the foreign legal person, obliged entity shall, when reviewing the foreign legal person referred to in paragraph 1 indent 1 of this Article, in addition to data referred to in paragraph 2 of this Article, obtain:

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

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

Obliged entity shall obtain data referred to in paragraphs 2 and 3 of this Article by consulting the CRS, records of issued identity documents, the Register of Beneficial Owners, the CRPS and the court, business or another relevant public register in which the foreign legal person is entered, as well as by inspecting an original or certified photocopy of a document from the CRPS or such court, business or other relevant public register.

Obliged entity shall obtain data not contained in the registers, records and documents referred to in paragraph 4 of this Article by inspecting an original or certified photocopy of a document or other documentation submitted by the customer at the request of the obliged entity.

Should, when reviewing the customer referred to in paragraph 2 of this Article, obliged entity identify a discrepancy in the data, it shall invite the customer to verify all relevant information.

Notwithstanding paragraphs 1 to 6 of this Article, in the case referred to in Article 61 paragraph 1 of this Law, obliged entity shall not be required to conduct an annual review of the foreign legal person.

## 6. Special forms of customer due diligence and monitoring measures

### Types of special forms of customer due diligence and monitoring measures

**Article 51**

Obliged entity shall, in addition to customer due diligence and monitoring measures, implement special forms of customer due diligence and monitoring measures depending on the established level of money laundering and terrorist financing risk relating to the customer, as follows:

1) enhanced customer due diligence and monitoring measures;

2) simplified customer due diligence and monitoring measures.

### Cases in which enhanced customer due diligence and monitoring measures are implemented

**Article 52**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 18)*

Obliged entity shall implement enhanced customer due diligence and monitoring measures in the sectors and activities referred to in Article 7 paragraph 1 indent 3 of this Law and in cases where a higher risk of money laundering and terrorist financing has

been identified, as follows:

1) in a correspondent relationship with a credit institution or another financial institution whose registered office is outside Montenegro;

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

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

4) in complex or unusual transactions referred to in Article 58 of this Law;

5) in suspicious transactions;

6) during the establishment of a business relationship or carrying out transactions with persons from high-risk third countries or where a high-risk third country is involved 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 a higher risk of money laundering and terrorist financing has been identified in line with the National Risk Assessment.

Obliged entity shall also implement enhanced customer due diligence and monitoring measures in other cases where it assesses that a higher risk of money laundering and terrorist financing exists or could exist in relation to the customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channel.

Notwithstanding paragraph 1 of this Article, enhanced customer due diligence and monitoring measures need not be applied automatically to branches and majority-owned subsidiaries of obliged entities with registered offices in Montenegro that are located in high-risk third countries, provided that their operations are fully aligned with the policies and procedures of the group to which they belong, in line with the risk assessment of the obliged entity.

### Enhanced customer due diligence and monitoring measures in a correspondent relationship with a credit institution or another financial institution whose registered office is outside Montenegro

### Article 53

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 19)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 24)*

When establishing a correspondent relationship involving the execution of payments with a credit institution or another financial institution that has its registered office outside Montenegro and is the respondent, the obliged entity shall, in addition to the measures referred to in Article 17 of this Law, take the following additional measures:

1) obtain an authorisation to provide banking services, as well as data on the date of issue, name and registered office of the competent authority that issued the authorisation;

2) obtain documentation on internal procedures implemented for the prevention and detection of money laundering and terrorist financing, in particular procedures for customer due diligence, identifying the beneficial owner, reporting suspicious

transactions, activities and customers to competent authorities, record-keeping, internal controls and other procedures established by the credit institution or another financial institution in relation to the prevention and detection of money laundering and terrorist financing;

3) obtain data, information and documentation on the assessment of internal controls concerning the implementation of measures for the prevention and detection of money laundering and terrorist financing at the credit institution or another financial institution;

4) obtain data and information on the legal or institutional framework for preventing and detecting money laundering and terrorist financing applied in the other country in which the credit institution or other financial institution has its registered office or is registered;

5) check whether the credit institution or other financial institution complies with the laws of the country in which it has its registered office or is registered and with the relevant regulations on the prevention and detection of money laundering and terrorist financing, including information on whether it is under investigation in connection with money laundering and terrorist financing or whether measures have been taken against that institution by the competent authorities;

6) determine that the credit institution or other financial institution does not operate as a shell (fictitious) bank;

7) establish that the credit institution or other financial institution has not established and does not establish business relationships or carry out transactions with shell (fictitious) banks;

8) establish that, in relation to a payable-through account, the credit institution or another financial institution has verified the identity of the customer and carried out ongoing customer due diligence and monitoring measures in respect of customers having direct access to the account and is able, at the request of the obliged entity, to provide relevant data concerning those measures;

9) ensure that all information obtained during the procedures for identifying and verifying customer identity, monitoring the business relationship and scrutinising transactions of the customer is made available by the respondent institution without delay.

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

Obliged entity shall regulate their responsibility and the responsibility of the respondent in the contract when concluding a correspondent relationship.

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

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

Obliged entity shall review and amend or, where necessary, terminate a correspondent relationship with a credit institution or another financial institution which is a respondent institution in a high-risk third country.

No obliged entity shall establish or continue a correspondent relationship with a credit institution or another financial institution that has its registered office outside Montenegro if:

1) they previously did not take measures referred to in paragraphs 1 to 4 of this

Article.

2) the credit institution or another financial institution has not established controls for its system for the prevention of money laundering and terrorist financing or does not apply laws and other regulations on the prevention and detection of money laundering and terrorist financing;

3) the credit institution or another financial institution operates as a shell bank (fictitious bank) or establishes or maintains correspondent or other business relationships and carries out transactions with shell banks.

## Guidelines on the application of enhanced customer due diligence and monitoring measures when providing crypto-asset services

### Article 53a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 25)*

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall prescribe guidelines specifying how enhanced customer due diligence and monitoring measures referred to in Articles 51, 52 and 53 of this Law are to be applied by obliged entities when providing crypto-asset-related services, except for crypto-asset advisory services and crypto-asset transfer services, as well as how obliged entities are to collect additional information on the originator and beneficiary of crypto-assets.

## Risk mitigation measures relating to transactions with a self-hosted address

### Article 53b

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 25)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 35)*

Crypto-asset service providers shall identify and assess the risks of money laundering and terrorist financing associated with crypto-asset transfers directed to or originating from a self-hosted address and shall establish internal policies, procedures and controls for that purpose.

Crypto-asset service providers shall apply risk mitigation measures that are commensurate with the identified risks.

Measures referred to in paragraph 2 of this Article shall include at least:

1) risk-based measures to identify and verify the identity of the originator or beneficiary of a crypto-asset transfer conducted to or from a self-hosted address or the beneficial owner of that originator or beneficiary, including reliance on third parties;

2) the requirement to obtain additional information on the origin and destination of the transferred crypto-assets;

3) enhanced ongoing monitoring of those transactions;

4) other measures for mitigating the risks of money laundering and terrorist financing, as well as the risks of failure to implement or circumvention of targeted financial sanctions and targeted financial sanctions related to the financing of the proliferation of weapons of mass destruction and for managing those risks.

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall issue guidelines for determining the measures referred to in paragraphs 2 and 3 of this Article, as well as the criteria and means for identifying and verifying the identity of the originator or beneficiary of a crypto-asset transfer conducted to or from a self-hosted address, in particular by relying on third parties, taking into account the latest technological developments.

**Measures relating to cross-border correspondent relationships involving the provision of crypto-asset services**

**Article 53c**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 25)*

Crypto-asset service provider shall, in addition to the measures referred to in Article 53 of this Law, in relation to cross-border correspondent relationships involving the provision of crypto-asset-related services, except for crypto-asset advisory services, with a respondent that does not have its registered office in Montenegro and provides similar services, including crypto-asset transfers, be required to:

1) verify whether the respondent is authorised to operate or is registered;

2) collect sufficient information on the respondent to fully understand the nature of its business and assess its reputation and the quality of supervision it is subject to, based on publicly available information;

3) assess anti-money laundering and counter-terrorist financing (AML/CFT) controls of the respondent;

4) obtain written approval from senior management prior to establishing a new correspondent relationship;

5) clearly document the responsibilities of each party in the correspondent relationship;

6) in cases involving crypto-asset payable-through accounts, ensure that the respondent has identified and conducted enhanced due diligence and ongoing monitoring of the customers who have direct access to the correspondent accounts, and that the respondent is capable of providing, upon request, relevant information on the due diligence measures undertaken.

Crypto-asset service providers shall document any decision to terminate a correspondent relationship for reasons related to their anti-money laundering and counter-terrorist financing policy.

Crypto-asset service providers shall regularly update the information relating to enhanced due diligence and ongoing monitoring of the correspondent relationship or whenever new risks related to the respondent arise.

Crypto-asset service providers shall take into account the information referred to in paragraph 1 of this Article when determining, based on a risk assessment, the appropriate measures to be applied for mitigating risks associated with the respondent.

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall issue guidelines for determining the criteria and elements that crypto-asset service providers must take into account when conducting the risk assessment under paragraph 1 of this Article and the risk mitigation measures referred to in paragraph 4 of this Article, including the minimum measures to be applied where the respondent is neither registered nor authorised to operate.

**Politically exposed persons**
**Article 54**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 26)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 36)*

Prior to establishing a business relationship with a customer, obliged entity shall check in the Register referred to in Article 55 of this Law whether the customer, legal representative of the customer, authorised person or beneficial owner is a politically exposed person.

Politically exposed person, within the meaning of this Law, is a Montenegrin citizen who holds public office, namely:

1) President of Montenegro, President of the Parliament of Montenegro and the President, a member and Secretary-General of the Government;
2) Member of Parliament,
3) President of a political party and their deputy, member of the presidency of a political party and their deputy, member of the executive board, member of the main board and another official of a political party;
4) State Secretary and Director General in a ministry and Secretary of a ministry;
5) President and judge of the Supreme Court of Montenegro and president and judge of Constitutional Court of Montenegro,
6) Supreme State Prosecutor, Special State Prosecutor and a prosecutor in the Supreme State Prosecutor's Office or Special State Prosecutor's Office;
7) Member of Senate of State Audit Institution and Council of Central Bank of Montenegro,
8) Mayor, president of a municipality, President of the Assembly of the Capital City, President of the Assembly of the Old Royal Capital and president of a municipal assembly;
9) Director of the National Security Agency and Director of the Agency for the Prevention of Corruption;
10) Ambassador, consul, Chief of the General Staff of the Army of Montenegro, general or admiral of the Army of Montenegro;
11) Director, deputy director or assistant director and member of the management or supervisory body of a legal person majority-owned by the state.

Politically exposed person is also a foreign national who holds public office in another state or an international organisation, namely:

1) President of State, Prime Minister, Minister and their deputy;
2) Member of Parliament;
3) Member of managing body of political party;
4) member of a supreme court, constitutional court or another high-level judicial body against whose decision, except in exceptional cases, it is not possible to use an ordinary or extraordinary legal remedy;
5) member of a court of auditors or supreme audit institution and member of the board of a central bank;
6) Ambassador, consul or high-ranked officer of armed forces;
7) member of the management or supervisory body of a legal person majority-owned by the state;

8) director, deputy director or assistant director and member of a board or holder of another equivalent position in an international organisation.

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

Family members of persons referred to in paragraphs 2 and 3 of this Article shall be considered to include a spouse or common-law partner, a partner in a same-sex life partnership, parents and children and their spouses, common-law partners or partners in same-sex life partnerships.

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 ownership and other property rights in a legal person or legal arrangement, an established business relationship or another type of close business relationship with a politically exposed person;
2) a natural person who is the sole beneficial owner of a legal person or legal arrangement known to have been established for the benefit of a politically exposed person.

International organisation carrying out a mission in Montenegro shall publish and update the list of prominent public officials in that international organisation.

Person referred to in paragraphs 2, 3 and 4 of this Article shall continue to be considered a politically exposed person for two years after ceasing to hold public office.

Following expiry of the period referred to in paragraph 8 of this Article, obliged entity shall continue to apply customer due diligence and monitoring measures to the customer on the basis of a risk assessment and determine whether a higher risk of money laundering and terrorist financing continues to exist in relation to that person.

Register of Politically Exposed Persons

**Article 55**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 37)*

Register of Politically Exposed Persons shall be an electronic database in which data on politically exposed persons are retained.

Financial Intelligence Unit, obliged entities and supervisory authorities referred to in Article 131 paragraph 1 of this Law shall have direct electronic access to data in the Register of Politically Exposed Persons.

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

Agency for the Prevention of Corruption shall maintain the Register of Politically Exposed Persons.

Politically exposed person referred to in Article 54 paragraphs 1 and 2 of this Law shall, without delay and no later than eight days from the date of appointment, enter accurate and complete data on themselves and the persons referred to in Article 54 paragraph 4 of this Law in the Register of Politically Exposed Persons.

When supervising entry of data in the Register of Politically Exposed Persons, Agency for the Prevention of Corruption shall verify whether the politically exposed person has acted in line with paragraph 5 of this Article and whether complete and accurate data have been entered.

Agency for the Prevention of Corruption shall prescribe the manner of maintaining and the content of the Register of Politically Exposed Persons.

**Enhanced customer due diligence and monitoring measures for a customer or beneficial owner who is a politically exposed person**

**Article 56**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 27)*

Should the customer or the beneficial owner of the customer be a politically exposed person, obliged entity shall, in addition to the measures referred to in Article 17 of this Law:

1) take adequate measures and establish the source of wealth and funds involved in the business relationship or transaction with that customer;
2) obtain the written consent of senior management to establish a business relationship with that customer prior to establishing the business relationship or, where the business relationship has already been established, obtain written consent of senior management to continue the business relationship;
3) establish whether that customer is the beneficial owner of a legal person, business organisation, trust, another person or an equivalent entity under foreign law or of a natural person with its registered office in another state on whose behalf the business relationship is established, a transaction is carried out or another activity of the customer is performed;
4) after establishing the business relationship, closely monitor transactions and other business activities carried out with the obliged entity by the politically exposed person or by the customer whose beneficial owner is a politically exposed person.

Obliged entity shall, in line with the guidelines referred to in Article 12 paragraph 5 of this Law, regulate by an internal act the risk-based procedures applied when identifying a customer who is a politically exposed person or identifying the beneficial owner of the customer who is a politically exposed person and when monitoring the business of that customer and beneficial owner.

## Measures Relating to Politically Exposed Persons in the Context of Life Insurance

### Article 56a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 20)*

Obliged entity shall undertake appropriate measures to determine whether the beneficiaries of life insurance policies or life insurance policies linked to investment units, as well as the beneficial owners of those beneficiaries, are politically exposed persons.

Measures referred to in paragraph 1 of this Article shall be implemented no later than at the time of payout under the insurance policy or at the time of full or partial transfer of the policy.

Obliged entity shall, in cases of higher risk and in addition to the measures referred to in Article 17 of this Law, take the following additional measures:

1) notify senior management prior to the payout of the insurance policy;

2) apply enhanced customer due diligence and monitoring measures to the policyholder and, where there are grounds for suspicion of money laundering or terrorist financing, inform the Financial Intelligence Unit in line with Article 66 of this Law.

Obliged entity shall also apply measures referred to in paragraph 3 of this Article to family members and close associates of persons referred to in Article 54 paragraphs 2 and 3 of this Law.

## Enhanced customer due diligence and monitoring measures when providing custody services

### Article 57

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

1) take adequate measures and establish the source of wealth and funds involved in the business relationship or transaction with that customer;

2) obtain written consent of senior management to establish a business relationship with that customer prior to establishing the business relationship or, where the business relationship has already been established, obtain written consent of senior management to continue the business relationship;

3) establish whether the customer concludes a contract for the provision of custody services in its own name and for its own account or whether it is a sub-custodian (a credit institution or another legal person that concludes a contract for the provision of custody services with the obliged entity in its own name and for the account of third parties, namely its customers to whom it provides custody services);

4) for each transaction, where a sub-custody arrangement is involved, establish for whose account the sub-custodian carried out the transaction.

Should obliged entity be unable to implement measures referred to in paragraph 1 of this Article, it shall not establish the business relationship or, where the business relationship has already been established, shall terminate it.

## Enhanced customer due diligence and monitoring measures for complex and unusual transactions

### Article 58

Obliged entity shall, in the case of complex or unusually large transactions or transactions carried out in an unusual manner, lacking an obvious economic justification or legal purpose or deviating from the usual or expected business of the customer, where it has not been possible to assess whether the transactions are suspicious, in addition to the measures referred to in Article 17 of this Law:

1) collect and verify additional data on activity of the customer and identification data on the customer and beneficial owner;

2) collect and verify additional data on the nature of the business relationship and the motive and purpose of the announced or executed transaction;

3) collect and verify additional data on financial standing of the customer, source of wealth and source of funds involved in the business relationship or transaction;

4) collect information on the source of funds and source of wealth of the customer and the beneficial owner or beneficial owners;

5) collect information on the reasons for planned or executed transactions;

6) analyse data referred to in items 2 and 3 of this paragraph and draft the results of the analysis in writing, stating clear conclusions indicating that the transaction is such a transaction.

Obliged entity shall, at the request of the Financial Intelligence Unit or competent supervisory 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.

Obliged entity shall establish by an internal act the criteria for identifying transactions referred to in paragraph 1 of this Article.

**Enhanced customer due diligence and monitoring measures in relation to a high-risk third country**

**Article 59**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 21)*

Should a business relationship be established or a transaction be carried out with a person from a high-risk third country or where a high-risk third country is involved in a transaction, in addition to the measures referred to in Article 17 of this Law, obliged entity shall:

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

2) prior to establishing the business relationship, obtain written approval from a senior manager to establish the business relationship with that customer or, where the business relationship has already been established, obtain written approval from a senior manager to continue the business relationship;

Following establishment of a business relationship with a customer from a high-risk third country, obliged entity shall conduct enhanced monitoring of the business relationship and transactions carried out by that customer, by:

- increase the number and frequency of controls carried out and select transaction methods that require further examination;

- ensure more frequent reporting on transactions to the compliance officer for the prevention of money laundering and terrorist financing;

- limit business relationships or transactions with customers from countries on the list referred to in Article 60 of this Law.

Obliged entity shall implement measures referred to in paragraphs 1 and 2 of this Article in line with the money laundering and terrorist financing risk determined in the risk analysis.

When implementing measures referred to in paragraph 2 of this Article, obliged entity shall also take into account relevant assessments or reports by international organisations or experts who set standards in the field of the prevention of money laundering and terrorist financing in relation to the risks that may be posed by individual third countries.

**List of high-risk third countries**

**Article 60**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 22)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 38)*

Financial Intelligence Unit shall establish the list of high-risk third countries.

List referred to in paragraph 1 of this Article shall include all countries published by the intergovernmental body established to develop and promote policies for the prevention of money laundering and terrorist financing and the financing of the proliferation of weapons

of mass destruction (the Financial Action Task Force – FATF).

Financial Intelligence Unit may extend the list referred to in paragraph 1 of this Article to include third countries which it determines to apply the standards for implementing measures for the prevention and detection of money laundering and terrorist financing insufficiently, such as the standards established by this Law or by European Union law, as well as countries included on the European Union list of high-risk third countries.

Financial Intelligence Unit may require an obliged entity to apply countermeasures in relation to third countries that are proportionate to the risks:

- where required by FATF; and

- independently of a FATF requirement, where it considers that the third country has weaknesses in its system for the prevention of money laundering and terrorist financing that pose a threat to Montenegro.

Financial Intelligence Unit shall publish the list referred to in paragraph 1 of this Article on its website.

### Simplified customer due diligence and monitoring measures

### Article 61

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 39)*

Should a lower risk of money laundering and terrorist financing be established, in the cases referred to in Article 18 paragraph 1 items 1, 2, 3, 4 and 7 of this Law, in relation to a customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channel, provided that there are no reasons for suspicion or grounds for suspicion that money or other property originates from criminal activity or that money laundering or terrorist financing is involved and provided that the customer or its beneficial owner is not a politically exposed person, obliged entity may apply simplified customer due diligence and monitoring measures as follows:

1) verify the identity of the customer and establish the beneficial owner after establishing the business relationship, but no later than eight days from the date on which the business relationship was established;

2) reduce the frequency of updating data on customer identity;

3) reduce the extent of ongoing monitoring of transactions if the transaction value does not exceed the threshold which the obliged entity, when preparing the risk analysis, assessed as appropriate to the business of the customer and lower risk of money laundering and terrorist financing;

4) instead of collecting information on the purpose and intended nature of the business relationship and implementing specific measures, draw conclusions about the purpose and intended nature of the business relationship based on the type of transaction or established business relationship.

When applying measures referred to in paragraph 1 of this Article, obliged entity shall regularly monitor and verify whether the conditions for applying simplified measures continue to exist.

Should, after establishing a business relationship with the customer while applying simplified customer due diligence and monitoring measures, reasons for suspicion or grounds for suspicion arise that property originates from criminal activity or that money laundering or terrorist financing is involved, obliged entity shall submit to the Financial Intelligence Unit the data referred to in Article 66 paragraphs 6 and 10 of this Law and implement measures referred to in Article 17 of this Law.

Obliged entity shall, in relation to a customer for whom a lower risk of money laundering and terrorist financing has been established, carry out measures for monitoring the business relationship and transactions to the extent determined in line with paragraph 1 item 3 of this Article.

Obliged entity shall draw up an internal act prescribing the conditions under which services may be provided or transactions carried out by applying simplified measures, which shall include restrictions on the amount, number or type of transactions that may be carried out to ensure that they are in line with the expected standards for the specific business relationship.

## 7. Implementation of measures for the prevention and detection of money laundering and terrorist financing in business units and companies majority-owned by an obliged entity in another country

### Obligation to implement measures for the prevention and detection of money laundering and terrorist financing in business units and companies majority-owned by an obliged entity in another country

**Article 62**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 28)*

Obliged entity shall ensure that measures for the prevention and detection of money laundering and terrorist financing established by this Law are implemented to the same extent in its business units or majority-owned companies having their registered office in another country which is a Member State of the European Union or a country that applies the same standards for implementing measures for the prevention and detection of money laundering and terrorist financing as those established by this Law or by European Union law.

Should the legislation of another country prescribe standards for implementing measures for the prevention and detection of money laundering and terrorist financing that are the same as or higher than the standards established by this Law, obliged entity shall ensure that its business units or majority-owned companies adopt and implement appropriate measures in line with that legislation of that country, including data protection measures.

Should the legislation of another country prescribe standards for implementing measures for the prevention and detection of money laundering and terrorist financing that are lower than the standards established by this Law or where such measures are implemented to a lesser extent than that established by this Law, obliged entity shall ensure that its business units or majority-owned companies implement measures for the prevention and detection of money laundering and terrorist financing in line with this Law, including data protection measures, to the extent permitted by that legislation of that country.

Should the legislation of another country prohibit the application of measures referred to in paragraph 3 of this Article, obliged entity shall immediately inform the Financial Intelligence Unit and the competent supervisory authority referred to in Article 131 paragraph 1 of this Law and take other appropriate measures to mitigate and effectively manage the risk of money laundering and terrorist financing, to the extent permitted by that legislation of that country.

Should the competent supervisory authority referred to in Article 131 paragraph 1 of this Law consider that measures referred to in paragraph 4 of this Article are insufficient, it shall order the obliged entity to implement the following measures in the other country:

1) prohibit the establishment of business relationships;

2) terminate business relationships;

3) prohibit the carrying out of transactions; or

4) where necessary and possible, terminate operations in business units or majority-owned companies of the obliged entity in the other country.

Obliged entity referred to in paragraph 1 of this Article which 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 line with this Law with other members of the financial group in Montenegro, Member States of the European Union and countries that have the same or higher standards for implementing measures for the prevention and detection of money laundering and terrorist financing than those established by this Law or by European Union law, provided that it ensures appropriate protection of the confidentiality of data and information in line with laws governing data secrecy and personal data protection.

Obliged entity referred to in paragraph 1 of this Article which is a member of a financial group may exchange data and information referred to in paragraph 6 of this Article with other members of the financial group in Montenegro, Member States of the European Union and countries that have the same or higher standards for implementing measures for the prevention and detection of money laundering and terrorist financing than those established by this Law or by European Union law even where reasons for suspicion or grounds for suspicion have been reported to the Financial Intelligence Unit that funds or other property constitute proceeds of crime, are subject to money laundering or are intended for terrorist financing, unless the Financial Intelligence Unit restricts or prohibits the exchange of data and information.

Issuers of electronic money, payment service providers and crypto-asset service providers with a place of business in Montenegro that are not branches, are established in Montenegro, have their registered office in another Member State of the European Union and operate on a cross-border basis shall designate a single point of contact in Montenegro which shall, on their behalf, ensure compliance with the rules on the prevention of money laundering and terrorist financing and facilitate supervision by the competent supervisory authority, in particular by providing documents and information at the request of that authority.

## 8. Prohibitions and restrictions in business operations

### Prohibition of providing services that enable the concealment of the customer identity

### Article 63

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 40)*

Obliged entity shall not open or maintain for a customer an anonymous account, anonymous crypto-asset account, anonymous safe-deposit box or savings passbook or coded or bearer securities accounts or provide any other service or product that directly or indirectly enables concealment of the customer identity.

### Prohibition of conducting business with shell

### banks

### Article 64

Obliged entity shall not operate as a shell bank.

Obliged entity shall not establish or maintain a correspondent relationship with a credit institution that operates or could operate as a shell bank or with another credit institution known to permit its accounts to be used by shell banks.

### Restriction on cash transactions

### Article 65

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 29)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 41)*

Legal persons, business organisations, sole proprietors and natural persons shall not receive a payment, make a payment or pay out winnings in cash in the amount of EUR 10,000 or more.

Restriction referred to in paragraph 1 of this Article shall also apply where a payment is made in two or more linked transactions in a total amount of EUR 10,000 or more, including loan transactions.

Payment in the amount referred to in paragraphs 1 and 2 of this Article must be made by payment or transfer to a transaction account opened with a credit institution in Montenegro.

Supervision of persons referred to in paragraph 1 of this Article that are not obliged entities within the meaning of this Law shall be carried out by the administrative authority competent for tax collection.

Obligations referred to in paragraphs 1, 2 and 3 of this Article shall not apply to the deposit of funds with credit institutions and other payment service providers.

Notwithstanding paragraph 5 of this Article, credit institutions and other payment service providers shall apply the restriction on the use of cash under this Article in relation to obliged entities:

- referred to in Article 4 paragraph 2 item 13 indents 6 and 9 of this Law, by not allowing the deposit of takings from real estate transactions, except where the price of the real estate concerned is lower than EUR 10,000;

- referred to in Article 4 paragraph 2 item 13 indents 10 to 13 of this Law, by not allowing the deposit of takings where the amount of an individual invoice is EUR 10,000 or more.

### Restrictions on Transactions in Real Estate

### Article 65a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 42)*

Execution of transactions under contracts or preliminary contracts for the sale and purchase of real estate, as well as other legal transactions whereby ownership or another real right in real estate is acquired or transferred, where the price of the real estate concerned is EUR 10,000 or more, may, where a payment transaction is executed, be carried out only if at least one participant in the legal transaction executes the payment transaction for that transaction to or from a transaction account opened with a credit institution in Montenegro.

Obliged entity referred to in Article 4 paragraph 4 of this Law shall refuse to draw up and certify a notarial deed that would enable avoidance of the use of national payment system of Montenegro in connection with paragraph 1 of this Article.

Should the payment transaction under a contract or preliminary contract for the sale and purchase of real estate or another legal transaction whereby ownership or another real right in real estate is acquired or transferred be executed before certification of the legal transaction, the notary shall obtain proof that the payment transaction was executed.

Mere statement by a participant in the transaction that the payment transaction was executed shall not be considered proof.

## 9. Reporting Obligations

## Reporting to the Financial Intelligence Unit

### Article 66

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 23)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 30)*
*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 43)*

Obliged entity shall submit to the Financial Intelligence Unit accurate and complete data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law, without delay and no later than three working days from the date of execution of the transaction or the date on which it becomes aware that the transaction has been executed, in relation to:
- each non-cash transaction in the amount of EUR 100,000 or more;
- each cash transaction carried out as an occasional transaction in the amount of EUR 3,000 or more but less than EUR 10,000, where the obliged entity is referred to in Article 4 paragraph 2 items 12 and 13 indents 3, 4 and 8 of this Law;
- each cash transaction in the amount of EUR 10,000 or more where the obliged entity is a credit institution or another payment service provider;
- each transaction in the amount of EUR 2,000 or more where the obliged entity is referred to in Article 4 paragraph 2 item 10 of this Law.

Notwithstanding paragraph 1 indent 1 of this Article, an obliged entity referred to in Article 4 paragraph 2 item 13 indents 5, 10, 11, 12 and 13 of this Law shall submit to the Financial Intelligence Unit accurate and complete data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law for each non-cash transaction in the amount of EUR 20,000 or more, without delay and no later than three working days from the date of execution of the transaction.

Obliged entity shall submit to the Financial Intelligence Unit accurate and complete data on customer due diligence and monitoring 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 that is carried out to the accounts of legal and natural persons in high-risk third countries or that involves a high-risk third country, without delay and no later than three days from the date of execution of the transaction or the date on which it becomes aware that the transaction has been executed.

Obliged entity referred to in Article 4 paragraph 4 of this Law shall submit to the Financial Intelligence Unit accurate and complete data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction or acquisition of rights under a preliminary contract or contract relating to real estate with a value of EUR 15,000 or more, as well as under a contract, statement or any instrument relating to a loan with a value of EUR 10,000 or more, without delay and no

later than three days from the date of conclusion of the relevant legal transaction.

Obliged entity referred to in Article 4 paragraph 4 of this Law shall, in addition to the data referred to in paragraph 4 of this Article, submit to the Financial Intelligence Unit a copy of the contract in electronic form and, for contracts performed using cash, a copy of the statement by the natural person who is the buyer concerning the source of that money, as well as the proof referred to in Article 65a paragraph 3 of this Law.

Obliged entity shall refrain from executing a suspicious transaction, regardless of the amount, until the order referred to in Article 93 of this Law is issued and shall, without delay, inform the Financial Intelligence Unit and submit to it data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law.

Obliged entity shall submit the data referred to in paragraph 6 of this Article to the Financial Intelligence Unit before the transactions are executed and specify the period within which the transactions are to be executed.

Should an obliged entity be unable to act in line with paragraph 6 of this Article due to the nature of the transactions or other justified reasons, it shall submit to the Financial Intelligence Unit data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law, without delay and no later than the next working day from the date of execution of the transaction or the date on which it becomes aware that the transaction has been executed.

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

Obliged entity shall, without delay, submit to the Financial Intelligence Unit accurate and complete data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in all cases of suspicious business or in relation to funds or other property which it knows or has reasons to suspect constitute proceeds of crime or are connected with money laundering or terrorist financing.

Should a customer requests advice in relation to money laundering or terrorist financing, obliged entity shall inform the Financial Intelligence Unit of this without delay.

Obliged entity shall inform the Financial Intelligence Unit of any inspection of data, information and documentation carried out at the obliged entity by the supervisory authority referred to in Article 131 paragraph 1 of this Law, no later than three working days from the date of the inspection.

Obliged entity shall submit the data referred to in paragraphs 1 to 6 and paragraph 10 of this Article, the explanation referred to in paragraph 9 of this Article and the notifications referred to in paragraphs 11 and 12 of this Article to the Financial Intelligence Unit electronically and shall sign those data, explanation and notifications with a qualified electronic signature in line with the law governing electronic identification and electronic signatures.

Obliged entity may also communicate the data referred to in paragraphs 6 and 10 of this Article to the Financial Intelligence Unit orally, by telephone or by another available means, but shall also submit those data in line with paragraph 13 of this Article no later than the next working day following the day of communication.

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

Financial Intelligence Unit shall collect and use the data referred to in paragraphs 1 to

5 of this Article for intelligence purposes and analyse it where necessary and in line with the assessed risk, for the purpose of detecting money laundering, terrorist financing or predicate offences related thereto.

### Exemptions from the reporting obligation

### Article 67

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 44)*

Notwithstanding Article 66 paragraph 6 of this Law, an obliged entity referred to in Article 4 paragraph 3 of this Law shall not be required to submit to the Financial Intelligence Unit data on the customer and case files in proceedings for providing legal assistance and representing the customer before the competent court.

Obliged entity referred to in Article 4 paragraph 3 of this Law shall designate a compliance officer for the prevention of money laundering and terrorist financing in line with Article 69 paragraph 1 of this Law where it carries out activities referred to in Article 4 paragraph 3 of this Law.

Compliance officer for the prevention of money laundering and terrorist financing referred to in paragraph 2 of this Article shall not be required to meet the conditions prescribed by Article 70 paragraph 1 items 1 and 2 of this Law.

### Feedback to the obliged entity

### Article 68

Based on the data or notifications submitted in line with Article 66 paragraphs 6, 10 and 11 of this Law, the Financial Intelligence Unit shall conduct a financial analysis in relation to persons, transactions or property and shall inform the obliged entity of the results of that analysis, as well as whether reasons for suspicion continue to exist or grounds for suspicion exist in relation to that person, transaction or property that money laundering or terrorist financing is involved or that the transaction or property constitutes proceeds of crime.

By way of derogation from paragraph 1 of this Article, the Financial Intelligence Unit shall not inform the obliged entity of the results of the analysis or of the existence of reasons for suspicion or grounds for suspicion referred to in paragraph 1 of this Article if it assesses that such notification may have harmful consequences for the course and outcome of the proceedings.

Should the Financial Intelligence Unit establish that there are grounds for suspicion that a transaction or asset represents proceeds of crime or that money laundering or terrorist financing is involved, it may, in the notification referred to in paragraph 1 of this Article, recommend that the obliged entity terminate the business relationship with the customer or refuse to execute the transaction.

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

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

### Article 69

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 45)*

Obliged entity shall, within 60 days from the date of its establishment or commencement of business, designate a compliance officer for the prevention of money laundering and terrorist financing and at least one deputy to that officer and shall, within three working days from the date of designation, submit to the Financial Intelligence Unit a notification containing data on those persons (name and surname; unique personal identification number; number, expiry date and issuing country of the identity document; number and expiry date of the residence permit for a foreign national; job title and contact telephone number) as well as the name or name and surname, TIN and registered office address of the obliged entity.

Obliged entity shall inform the Financial Intelligence Unit of any change in the compliance officer for the prevention of money laundering and terrorist financing or their deputy within three days from the date on which the change was made.

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

Exceptionally, an obliged entity with six or fewer employees shall not be required to designate a deputy compliance officer for the prevention of money laundering and terrorist financing.

At an obliged entity with six or fewer employees, the duties of a compliance officer for the prevention of money laundering and terrorist financing may also be performed by the director, provided that the director meets the requirements referred to in Article 70 of this Law.

Should the duties of a compliance officer for the prevention of money laundering and terrorist financing be performed by the director, obliged entity shall notify the Financial Intelligence Unit thereof and include in the notification the data on the director referred to in paragraph 1 of this Article.

Notwithstanding paragraph 5 of this Article, at a non-financial-sector obliged entity with more than six employees, the duties of the compliance officer for the prevention of money laundering and terrorist financing may also be performed by the director, subject to the prior written consent of the Financial Intelligence Unit, provided that the director meets the requirements referred to in Article 70 of this Law.

Obliged entity may initiate an administrative dispute against the decision referred to in paragraph 7 of this Article.

Notifications referred to in paragraphs 1, 2 and 6 of this Article shall be submitted to the Financial Intelligence Unit electronically and shall be signed with a qualified electronic signature in line with the law governing electronic identification and electronic signature.

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

**Article 70**

***(****Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 31)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 46)*

Person may be designated as the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer provided that the person:

1) has completed training for performing the duties of the compliance officer for the prevention of money laundering and terrorist financing (hereinafter referred to as: the training) and has passed the professional examination for performing those duties (hereinafter referred to as: the professional examination);

2) has a licence for performing the duties of the compliance officer for the prevention of money laundering and terrorist financing;

3) has not been finally convicted of a criminal offence punishable by imprisonment for more than six months; and

4) is employed by the obliged entity.

Person designated as the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer at one financial-sector obliged entity may not be designated as the compliance officer or deputy compliance officer at another obliged entity.

Designation as the compliance officer or deputy compliance officer at one obliged entity shall not preclude the person concerned, in justified circumstances and at a non-financial-sector obliged entity, from also being designated as the compliance officer or deputy compliance officer at one additional non-financial-sector obliged entity.

Notwithstanding paragraphs 2 and 3 of this Article, where the director performs the duties of the compliance officer for the prevention of money laundering and terrorist financing in line with Article 69 paragraph 5 of this Law, that person may be designated as the compliance officer at several obliged entities at which that person is both the director and the sole employee.

## Training and professional examination

### Article 71

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 24)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 32)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 47)*

Training shall be delivered by the organiser of adult education who has a licence, issued in line with regulations which govern education of adults.

Training shall be delivered in line with the curriculum defined by regulations governing adult education, with the prior approval of the Financial Intelligence Unit.

Following completion of the training, the candidate shall take the professional examination before the commission for taking the professional examination, established by Head of the Financial Intelligence Unit.

Depending on the number of candidates, Head of the Financial Intelligence Unit may establish more than one commission at the same time.

Financial Intelligence Unit shall issue a certificate of passing the professional examination on the prescribed form.

President and members of the Commission referred to in paragraph 3 of this Article shall be entitled to remuneration for their work in the amount of 40% of the average net salary in Montenegro in the previous year, for the month in which the candidate took the

examination.

Should a person already employed by the obliged entity take the professional examination, the costs of taking the professional examination shall be borne by the obliged entity.

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

### Licence for performing the duties of a compliance officer for prevention of money laundering and terrorist financing

### Article 72

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 33)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 48)*

Licence for performing the duties of a compliance officer for the prevention of money laundering and terrorist financing (hereinafter referred to as: the licence) shall be issued by the Financial Intelligence Unit.

Licence shall be issued to a person who:

1) has residence or approved stay in Montenegro;

2) submits a certificate, confirmation or other act of a competent authority proving good repute within the meaning of Article 40r of this Law;

3) has completed training and passed the professional examination.

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

Request for issuing the licence shall be submitted to the Financial Intelligence Unit.

Request for renewal of the licence shall be submitted to the Financial Intelligence Unit no later than 30 days before expiry of the period for which the licence was issued.

Licence shall be issued in the prescribed form and its authenticity can be verified.

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

### Expiry of a licence

### Article 73

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 49)*

Licence shall cease to be valid:

1) at the request of the licence holder;

2) upon expiry of the period for which it was issued;

3) if the person to whom the licence was issued no longer meets the good-repute requirements within the meaning of Article 40r of this Law;

4) if the person to whom the licence was issued becomes permanently incapable of performing the duties of a compliance officer for the prevention of money laundering

and terrorist financing or the deputy compliance officer, or loses legal capacity;

5) in the case of negligent performance of duties.

**Negligent business performance**

**Article 74**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 34)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 50)*

Compliance officer for the prevention of money laundering and terrorist financing or the deputy compliance officer shall be considered to perform duties negligently within the meaning of Article 73 paragraph 1 item 5 of this Law if, without justified reason:

1) fails to submit data and information in line with Article 66 of this Law more than four times within a period of two years;
2) fails to submit data and information in a timely manner in line with this Law more than six times within a period of two years;
3) fails to act or fails to act in a timely manner in line with Articles 93 and 95 of this Law more than twice within a period of two years.

Financial Intelligence Unit shall establish the existence of the circumstances referred to in paragraph 1 of this Article on the basis of a report submitted by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, following a request referred to in Article 131 paragraph 10 of this Law.

**Decision on cessation of validity of the licence**

**Article 75**

Decision on cessation of validity of the licence shall be issued by the Financial Intelligence Unit.

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

Financial Intelligence Unit shall, without delay, inform the obliged entity to which the person whose licence has been revoked has been designated as compliance officer for the prevention of money laundering and terrorist financing or their deputy of the termination of the licence.

Obliged entity shall, in the case of termination of a licence, designate another compliance officer for the prevention of money laundering and terrorist financing or their deputy within 15 days from the date on which the decision was adopted.

**Duties of the compliance officer for the prevention of money laundering and terrorist financing or the deputy compliance officer**

**Article 76**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 51)*

Compliance officer for the prevention of money laundering and terrorist financing or the deputy compliance officer shall perform the following duties:

1) Ensure the establishment, operation and development of the system for preventing and detecting money laundering and terrorist financing;

2) Ensure the proper and timely submission of data to the Financial Intelligence Unit and cooperate with the competent inspection authority in inspection supervision proceedings;

3) Draft and regularly update the risk analysis of money laundering and terrorist financing, in line with guidelines referred to in Article 12 paragraph 5 of this Law;

4) Monitor the implementation of policies, controls and procedures for preventing and detecting money laundering and terrorist financing;

5) Initiate and participate in drafting and amending operating procedures and preparing internal acts of the obliged entity relating to the prevention and detection of money laundering and terrorist financing;

6) Participate in drafting internal acts relating to the prevention and detection of money laundering and terrorist financing at the obliged entity;

7) Monitor and coordinate harmonisation of business operation of the obliged entity with this Law;

8) Cooperate in establishing and developing information technology used to prevent and detect money laundering and terrorist financing;

9) Submit initiatives and proposals for improving the system for preventing and detecting money laundering and terrorist financing to the management body or another similar body;

10) When new products, services or distribution channels are introduced at the obliged entity, ensure the implementation of Article 16 of this Law;

11) Prepare programmes for the professional training and development of employees of the obliged entity in the field of preventing and detecting money laundering and terrorist financing;

12) Prepare a report on preventing and detecting money laundering and terrorist financing for the obliged entity once a year and more frequently where necessary or at the request of the supervisory authority referred to in Article 131 paragraph 1 of this Law;

Obliged 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 at its request, within three days from the date of receipt of the request.

Compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer shall be directly responsible to the management body, executive body or another similar body of the obliged entity.

Should a financial-sector obliged entity be a large or medium-sized legal person, the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer shall be functionally and organisationally separate from other organisational units of the obliged entity.

Large or medium-sized legal person referred to in paragraph 4 of this Article means a legal person within the meaning of the law governing accounting.

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

**Article 77**

Obliged entity shall provide the compliance officer for the prevention of money laundering and terrorist financing with, in particular:

1) conditions for the efficient performance of the duties referred to in Article 76 paragraph 1 of this Law;

2) Functional connection with other organisational units of the obliged entity enabling

the prompt, efficient and timely performance of the duties referred to in Article 76 paragraph 1 of this Law;

3) Appropriate material working conditions;

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

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

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

7) Replacement during the absence from work.

Management body of the obliged entity shall provide assistance and support in performing the duties referred to in Article 76 paragraph 1 of this Law to the compliance officer for the prevention and detection of money laundering and terrorist financing and shall inform the compliance officer of facts relevant to preventing and detecting money laundering and terrorist financing.

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

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

## Professional Training and Development

Article 78

Obliged entity shall provide regular professional training and development in the field of prevention and detection of money laundering and terrorist financing for all employees participating in the prevention and detection of money laundering and terrorist financing at that obliged entity.

Professional training and development referred to in paragraph 1 of this Article shall include familiarising employees with this Law and regulations adopted on the basis of this Law, internal acts of the obliged entity in the field of prevention and detection of money laundering and terrorist financing, professional literature on prevention and detection of money laundering and terrorist financing, lists of indicators referred to in Articles 82 and 83 of this Law, regulations governing international restrictive measures, regulations governing the protection of personal data and regulations governing data confidentiality.

Obliged entity shall, by the end of the first quarter of the current year, draft a programme of professional training and development referred to in paragraph 1 of this Article for that year.

Manner of providing professional training and development for employees shall be regulated by an internal act of the obliged entity.

## Rules on Performing Activities Relating to the Prevention and Detection of Money Laundering and Terrorist Financing

### Article 79

Obliged entity shall determine and implement appropriate rules for dealing with customers and ensure reporting, data retention, internal control, risk assessment, risk management and communication for the prevention and detection of money laundering and terrorist financing.

Obliged entity shall determine and ensure implementation of appropriate rules ensuring adequate exchange of information among employees for the efficient performance of

obligations prescribed by this Law.

Obliged entity shall order and supervise application of rules referred to in paragraphs 1 and 2 of this Article in business units and companies majority-owned by the obliged entity and having their registered office in other states.

### Internal Control and Audit

### Article 80

Obliged entity shall ensure regular internal control and audit of implementation of policies, controls and procedures for the prevention of money laundering and terrorist financing and of performance of activities relating to the prevention and detection of money laundering and terrorist financing, in line with the established risk of money laundering and terrorist financing identified in the risk analysis.

Should the law regulating the activity of the obliged entity prescribe an obligation to have an independent internal audit, obliged entity shall also organise independent internal audit within whose scope of work is regular assessment of the adequacy, reliability and effectiveness of the money laundering and terrorist financing risk management system.

Obliged entity shall organise independent internal audit within whose scope of work is regular assessment of the adequacy, reliability and effectiveness of the money laundering and terrorist financing risk management system where it considers this necessary having regard to the scope and nature of its activities.

Internal control and audit referred to in paragraphs 1, 2 and 3 of this Article shall be conducted in such a way as to prevent, detect and correct errors made during implementation of regulations in the field of prevention and detection of money laundering and terrorist financing and improve the policies, controls and procedures of the obliged entity for detecting transactions and persons connected with money laundering and terrorist financing.

Manner of conducting internal control and audit referred to in paragraphs 1, 2 and 3 of this Article shall be regulated by an internal act of the obliged entity.

## IV. LIST OF INDICATORS FOR IDENTIFYING SUSPICIOUS CUSTOMERS AND TRANSACTIONS

### Obligation to Use Lists of Indicators

### Article 81

When establishing reasons for suspicion that property originates from criminal activity or that money laundering or terrorist financing is involved and when considering other circumstances related to such suspicion, obliged entity shall use the lists of indicators referred to in Articles 82 and 83 of this Law and take into account other circumstances indicating the existence of reasons for suspicion of money laundering and terrorist financing.

### List of Indicators for Identifying Suspicious Customers and Transactions

### Article 82

Ministry shall establish the list of indicators for identifying suspicious customers and transactions.

Financial Intelligence Unit shall prepare the professional basis for drafting the list of

indicators referred to in paragraph 1 of this Article, in cooperation with supervisory authorities referred to in Article 131 paragraph 1 of this Law.

### Own List of Indicators for Identifying Suspicious Customers and Transactions

### Article 83

Obliged entity shall draft its own list of indicators for identifying suspicious customers and transactions, taking into account the complexity and volume of transactions executed by that obliged entity, unusual manner of execution, value or interconnection of transactions that have no economic or lawful purpose or are not consistent with or are disproportionate to the usual or expected business activities of the customer, as well as other circumstances relating to the status and other characteristics of the customer of that obliged entity.

List of indicators referred to in paragraph 1 of this Article shall be kept in the documentation of the obliged entity.

## V. ACTIVITIES, POWERS, MANNER OF WORK AND INFORMATION SYSTEM OF THE FINANCIAL INTELLIGENCE UNIT

### Independence and Autonomy in Performing Activities and Exercising Powers

### Article 84

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 35)*

Financial Intelligence Unit shall be a central national unit competent for the prevention and detection of money laundering and terrorist financing, in line with the law.

Financial Intelligence Unit shall be operationally independent and autonomous in exercising powers prescribed by law and autonomous in making decisions concerning the receipt, collection, retention, analysis and submission of data, notifications, information and documentation, as well as the submission of the results of strategic and operational analyses of suspicious transactions to competent authorities, foreign Financial Intelligence Units and international organisations.

Head and officers of the Financial Intelligence Unit shall perform the activities and exercise the powers referred to in paragraph 2 of this Article.

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

### Head of the Financial Intelligence Unit

### Article 85

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 36)*

Person holding the rank of Assistant Director of the Police and meeting the requirements for Assistant Director of the Police shall be appointed as Head of the Financial Intelligence Unit, in line with the law governing internal affairs.

Head of the Financial Intelligence Unit may not simultaneously be Head of another organisational unit in the Police.

Government shall appoint Head of the Financial Intelligence Unit, following a public

competition, on the proposal of the Minister of the Interior.

Government shall submit the proposal for appointing Head of the Financial Intelligence Unit to the competent committee of the Parliament of Montenegro for an opinion.

### Entering into Employment and Employment Requirements

### Article 86

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 37)*

Head of the Financial Intelligence Unit shall participate in the procedure for selecting candidates for employment in the Financial Intelligence Unit, conducted in line with regulations governing civil servants and state employees and the law governing internal affairs.

Officers of the Financial Intelligence Unit shall meet the requirements prescribed by the law governing internal affairs and the act on internal organisation and systematisation of the Ministry.

Police officer or Ministry officer may be assigned to a post in the Financial Intelligence Unit only with the prior consent of Head of the Financial Intelligence Unit.

Minister of the Interior shall issue the decision on employing an officer in the Financial Intelligence Unit, on the proposal of Head of the Financial Intelligence Unit.

Officer of the Financial Intelligence Unit may not be assigned to another post or other duties in the Police or Ministry without the consent of Head of the Financial Intelligence Unit.

### Disposal of the Budget of the Financial Intelligence Unit

### Article 87

Head of the Financial Intelligence Unit shall independently dispose of funds allocated to the Ministry by the budget for the work of the Financial Intelligence Unit, in line with the law governing budget planning and execution and fiscal responsibility.

Head of the Financial Intelligence Unit shall independently dispose of funds allocated to the Financial Intelligence Unit for its work through donations or in another manner.

Within the funds referred to in paragraph 1 of this Article, Head of the Financial Intelligence Unit shall independently make decisions on conducting public procurement and simple procurement procedures as an authorised person of the contracting authority, in line with the law governing public procurement.

### Material and Technical Means of the Financial Intelligence Unit

### Article 88

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

Information system, means of communication, vehicles and other equipment referred to in paragraph 1 of this Article shall not be made available for use by another organisational unit of the Ministry or Police without the written consent of Head of the Financial Intelligence Unit.

Manner of disposing of and using the information system, means of communication, vehicles and other equipment referred to in paragraph 1 of this Article, as well as the premises used by the Financial Intelligence Unit, shall be regulated by Head of the Financial Intelligence Unit by an internal act.

Act referred to in paragraph 3 of this Article shall be marked with the appropriate classification level, in line with the law governing data confidentiality.

**Activities and Powers of the Financial Intelligence Unit**

**Article 89**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 05 July 2024, Article 25)*

Financial Intelligence Unit shall be authorised to:

1) collect, process and analyse data on natural and legal persons, their assets, suspicious, cash and other transactions, suspicious and other business activities, bank accounts and safe-deposit boxes, and prepare and forward financial analyses and other information in line with this Law;

2) receive from obliged 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 of other states or international organisations competent for the prevention and detection of money laundering and terrorist financing or authorities of another state competent for the confiscation of assets, as well as information and data on persons and assets in respect of which there are reasons or grounds for suspicion that money laundering and related predicate offences or terrorist financing are involved or that assets originate from criminal activity, which it may process and use for the purposes specified in this Law;

3) order the obliged entity to temporarily suspend execution of a transaction and continuously monitor the financial operations of the customer;

4) propose amendments to regulations relating to the prevention and detection of money laundering and terrorist financing;

5) conclude cooperation agreements or establish independent cooperation for the exchange of 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, foreign Financial Intelligence Units, competent authorities in other states and international organisations;

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

7) participate in professional training and development of compliance officers for the prevention of money laundering and terrorist financing at obliged entities and their deputies;

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

9) propose to the National Security Council the inclusion of legal and natural persons on the National List of Designated Persons in line with the law governing international restrictive measures;

10) at least once a year, publish a report covering statistical data, trends and typologies in the field of money laundering and terrorist financing, in particular data on the number of suspicious transaction reports submitted to the Financial Intelligence Unit, cases investigated, persons prosecuted, persons convicted of money laundering or terrorist financing offences, assets frozen or confiscated and restricted or prevented access to data referred to in Article 47 paragraph 5 of this Law, and otherwise inform the public in an appropriate manner about manifestations of money laundering and terrorist financing;

11) perform other activities in line with the law.

Head of the Financial Intelligence Unit shall regulate the detailed manner of performing activities and exercising powers referred to in paragraph 1 of this Article by an internal act.

Act referred to in paragraph 2 of this Article shall be marked with the appropriate classification level in line with the law governing data confidentiality.

**Request to an Obliged Entity to Submit Data, Information and Documentation**

**Article 90**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 38)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 52)*

Should the Financial Intelligence Unit assess that there are reasons or grounds for suspicion that funds or other assets of a particular customer originate from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, it may require the obliged entity to submit 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 assets of that customer held by the obliged entity;

3) on the movement of funds and assets of that customer with the obliged entity;

4) on business relationships established with that customer;

5) data, information and documentation obtained in line with this Law in connection with the performance of activities under this Law, as well as other data necessary for monitoring fulfilment of obligations established by this Law.

Request referred to in paragraph 1 of this Article shall state the legal basis for collecting data, the data to be submitted, the purpose of collecting data and the deadline for their submission.

Financial Intelligence Unit may also require submission of data, information and documentation referred to in paragraph 1 of this Article for persons who may reasonably be considered to have cooperated or participated in transactions or business of persons in respect of whom there are reasons or grounds for suspicion that funds or assets they own, dispose of or manage originate from criminal activity or money laundering, related predicate offences or are connected with terrorist financing.

Obliged entity shall, upon a request referred to in paragraphs 1 and 3 of this Article, submit accurate and complete data, information and documentation in its possession without delay, but no later than five working days from the date of receipt of the request.

Should a request referred to in paragraphs 1 and 3 of this Article be marked "URGENT", obliged entity shall submit data, information and documentation to the Financial Intelligence Unit without delay, but no later than 24 hours from receipt of the request.

Financial Intelligence Unit may, due to the volume of data, information and documentation or other justified reasons, upon a reasoned request of the obliged entity, extend the deadline referred to in paragraph 5 of this Article by no more than five working days or verify the data, information and documentation at the obliged entity.

Obliged entities shall submit the data, information and documentation referred to in paragraph 1 of this Article to the Financial Intelligence Unit in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

Submission of data, information and documentation referred to in paragraph 1 of this Article to the Financial Intelligence Unit shall be free of charge.

**Request to Submit Data, Information and Documentation to Persons That Are**

## Not Obliged Entities

### Article 91

Exceptionally, should the Financial Intelligence Unit assess that there are reasons or grounds for suspicion that funds or other assets originate from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, it may require entities referred to in Article 43 paragraph 3 of this Law, as well as natural persons that are not obliged entities under this Law, to make available or submit data, information and documentation in their possession or provide information, for the prevention and detection of money laundering, related predicate offences or terrorist financing, and in particular the following data:

1) on assets or lawful income, as well as on the relationship between income and assets;

2) on assets transferred to third parties or passed to a legal successor, as well as on the manner of acquiring and transferring assets;

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

4) other data relevant to locating and establishing proceeds of crime or establishing the existence of grounds for suspicion that the criminal offence of money laundering or terrorist financing has been committed.

Entities and 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 act referred to in 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 free of charge.

## Request to a State Authority, Competent Authority, Supervisory Authority or Holder of Public Powers to Submit Data, Information and Documentation

### Article 92

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 holders of public powers shall enable the Financial Intelligence Unit to have direct electronic access to all data, information and documentation kept in electronic form.

Should it not be possible to obtain data, information and documentation referred to in paragraph 1 of this Article in the manner referred to in that paragraph, authorities referred to in paragraph 1 of this Article and holders of public powers shall, upon request of Financial Intelligence Unit, submit such data, information and documentation without delay, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

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

## Order on Temporary Suspension of Execution of a Transaction and Temporary Prohibition of Access to a Safe-deposit Box

### Article 93

Should the Financial Intelligence Unit assess that there are reasons or grounds for suspicion that funds or other assets originate from criminal activity or result from money laundering or related predicate offences or are intended for terrorist financing, it may, by an order, require the obliged entity to suspend execution of a transaction and prohibit access to a safe-deposit box for no more than 72 hours.

Financial Intelligence Unit shall, without delay and no later than 24 hours, notify

competent authorities of the order referred to in paragraph 1 of this Article for the purpose of taking measures within their competence.

Should it act on the notification referred to in Article 66 paragraph 6 of this Law, Financial Intelligence Unit shall issue the order referred to in paragraph 1 of this Article within 24 hours from receipt of the notification.

Should the last day of the period referred to in paragraph 1 of this Article fall on a non-working day, the period may be extended by an additional 48 hours by order, provided that the total period of suspension of execution of the transaction or prohibition of access to the safe-deposit box may not exceed seven days.

Obliged entity shall, without delay, take measures in line with paragraphs 1 and 4 of this Article.

Financial Intelligence Unit shall deliver the order referred to in paragraphs 1 and 4 of this Article to the obliged entity in electronic or written form.

Notwithstanding paragraph 6 of this Article, the order referred to in paragraphs 1 and 4 of this Article may, due to urgency or other circumstances concerning execution of transactions, be issued orally, provided that it is delivered in electronic or written form no later than 24 hours from issuing the oral order.

Compliance officer for the prevention of money laundering and terrorist financing at the obliged entity shall draft a note of receipt of the oral order referred to in paragraphs 1 and 4 of this Article.

Competent authorities shall, after receiving the notification referred to in paragraph 2 of this Article, act in line with their powers without delay, but no later than 72 hours from the temporary suspension of execution of the transaction or temporary prohibition of access to the safe-deposit box, and shall notify Financial Intelligence Unit thereof in electronic or written form without delay.

### Termination of the Measure of Temporary Suspension of Execution of a Transaction and Temporary Prohibition of Access to a Safe-deposit Box

### Article 94

Should the Financial Intelligence Unit fail to notify the obliged entity of further action within 72 hours after suspension of execution of the transaction or prohibition of access to the safe-deposit box, obliged entity may, upon expiry of that period, execute the transaction or allow access to the safe-deposit box.

### Request for Continuous Monitoring of the Financial Operations of the Customer

### Article 95

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 53)*

Financial Intelligence Unit may, in electronic or written form, require the obliged entity to continuously monitor the financial operations of the customer or another person who may reasonably be considered to have cooperated with or participated in transactions or business with the customer, where there are reasons or grounds for suspicion that funds or other assets originate from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, and set the period during which the obliged entity shall inform Financial Intelligence Unit of all transactions and submit the requested data.

Obliged entity shall carry out continuous monitoring covertly and without informing the customer thereof.

Obliged entity shall submit the data referred to in paragraph 1 of this Article to the Financial Intelligence Unit prior to execution of the transaction or conclusion of the

business where the transaction exceeds EUR 1,000 for a natural person or EUR 3,000 for a legal person, and state in the notification an estimate of the period within which the transaction is to be executed or the business concluded.

Should the obliged entity be unable, due to the nature of the transaction or business or other justified reasons, to act in line with paragraph 3 of this Article, it shall submit the data referred to in paragraph 1 of this Article to the Financial Intelligence Unit without delay, but no later than the next working day following execution of the transaction or conclusion of the business.

Obliged entity shall, when submitting data in line with paragraph 4 of this Article, give detailed reasons for not acting in line with paragraph 3 of this Article.

Continuous monitoring referred to in paragraph 1 of this Article may last no longer than three months from the date of submission of the request referred to in paragraph 1 of this Article.

Should it be necessary, the period referred to in paragraph 6 of this Article may be extended up to six months from the date of submission of the request referred to in paragraph 1 of this Article.

**Collection of Data, Information and Documentation Based on a Request or Information**

**Article 96**

Financial Intelligence Unit may, on the basis of a reasoned request or information received from another organisational unit of the Ministry or Police, the administrative authority competent for tax collection, the administrative authority competent for customs affairs, the National Security Agency, the Agency for Prevention of Corruption, the State Prosecutor's Office or a court, conduct proceedings for collecting and analysing data, information and documentation should, in relation to a particular person, transaction or assets, there be reasons or grounds for suspicion that money laundering, related predicate offences or terrorist financing is involved or that assets originate from criminal activity.

Head of the Financial Intelligence Unit shall decide whether to act on the request or information referred to in paragraph 1 of this Article.

Financial Intelligence Unit may, on the basis of the request or information referred to in paragraph 1 of this Article, submit a response 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 line with paragraph 1 of this Article.

Should objective reasons exist for assuming that submission of the response referred to in paragraph 3 of this Article would adversely affect the course or outcome of an investigation or analysis conducted by Financial Intelligence Unit, or that disclosure of information would manifestly be disproportionate to the interests of a natural or legal person or would not be relevant having regard to the purposes for which it was requested, Financial Intelligence Unit may refuse to submit the response to the request referred to in paragraph 1 of this Article.

Financial Intelligence Unit shall give reasons for refusing to submit a response to the request referred to in paragraph 1 of this Article.

Competent authorities referred to in paragraph 1 of this Article shall, if they receive the response referred to in paragraph 3 of this Article, provide Financial Intelligence Unit with feedback on the use of the information submitted, as well as with the results of investigations or supervision conducted on the basis of that information.

**Submission of Notification to Competent Authorities Where Grounds for Suspicion Exist That Money Laundering or Terrorist Financing Has Been**

**Committed or That Assets Originate from Criminal Activity**

**Article 97**

Should the Financial Intelligence Unit assess, on the basis of data, information and documentation obtained in line with the law, that there are grounds for suspicion, in relation to a person, transaction, funds or other assets, that the criminal offence of money laundering or terrorist financing has been committed or that assets originate from criminal activity, it shall notify the competent authority in writing and submit the necessary data, information and documentation.

Should the Financial Intelligence Unit have acted on the notification referred to in Article 66 paragraphs 6, 10 and 11 of this Law, the notification referred to in paragraph 1 of this Article shall not state that it was submitted by an obliged entity, identify the employee of the obliged entity who submitted it or include that notification, unless there are grounds for suspicion that the employee committed the criminal offence of money laundering or terrorist financing or the data are necessary for establishing facts in criminal proceedings and the competent court requested their submission in writing.

Competent authority referred to in paragraph 1 of this Article shall provide Financial Intelligence Unit with feedback on the use of the data, information and documentation referred to in paragraph 1 of this Article, as well as the results of investigations or supervision conducted on the basis of that data, information and documentation.

**Submission of a Notification to Competent Authorities Where Grounds for Suspicion Exist That Another Criminal Offence Has Been Committed**

**Article 98**

Should the Financial Intelligence Unit assess, on the basis of data, information and documentation obtained in line with this Law, that grounds for suspicion exist, in relation to a person, transaction, funds or other assets, that another criminal offence prosecutable ex officio has been committed, it shall notify the competent authority in writing, together with the necessary data, information and documentation confirming those grounds, for the purpose of taking measures within its competence.

Should the Financial Intelligence Unit have acted on the notification referred to in Article 66 paragraphs 6, 10 and 11 of this Law, the notification referred to in paragraph 1 of this Article shall not state that it was submitted by an obliged entity, identify the employee of the obliged entity who submitted it or include that notification, unless there are grounds for suspicion that the employee committed a criminal offence prosecutable ex officio or the data are necessary for establishing facts in criminal proceedings and the competent court requested their submission in writing.

Competent authority referred to in paragraph 1 of this Article shall provide Financial Intelligence Unit with feedback on the use of the data, information and documentation referred to in paragraph 1 of this Article, as well as the results of investigations or supervision conducted on the basis of that data, information and documentation.

**Analysis of the Efficiency and Effectiveness of the System for Preventing Money Laundering and Terrorist Financing**

**Article 99**

Financial Intelligence Unit shall, at least once a year, analyse the efficiency and effectiveness of the system for preventing money laundering and terrorist financing.

Analysis of the efficiency and effectiveness of the system for preventing money laundering and terrorist financing shall be carried out on the basis of a comprehensive report drafted by Financial Intelligence Unit on the basis of:

- data referred to in Articles 115 and 120 of this Law;

- data on the size of the obliged 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 resources and personnel capacities allocated to the fight against money laundering and terrorist financing at 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.

Analysis referred to in paragraph 1 of this Article shall in particular include analysis of:

- risk of money laundering and terrorist financing at national level;

- efficiency and effectiveness of the coordinated action of Financial Intelligence Unit, supervisory authorities referred to in Article 131 paragraph 1 of this Law, other competent authorities and obliged entities in preventing money laundering and terrorist financing;

- quality of financial intelligence data, information and documentation obtained through international cooperation and their adequacy for effective action in relation to perpetrators of criminal offences and their assets;

- efficiency and effectiveness of the work of supervisory authorities referred to in Article 131 paragraph 1 of this Law in exercising appropriate supervision, monitoring and regulating the work of obliged entities, with a view to achieving compliance with requirements for preventing money laundering and terrorist financing in proportion to identified risks;

- adequacy of application of measures referred to in Articles 17 and 52 of this Law and reporting of suspicious transactions by obliged entities in proportion to identified risks;

- results achieved in preventing misuse of legal persons for the purposes of money laundering or terrorist financing and availability of information on their beneficial owners to competent authorities;

- efficiency and effectiveness in using financial intelligence data and other data for conducting investigations into money laundering and terrorist financing by competent authorities;

- effectiveness of investigations into criminal offences of money laundering, related predicate offences and terrorist financing, prosecution of perpetrators of those offences and sanctions imposed for those offences;

- assets, income and funds temporarily or permanently confiscated;

- terrorists, terrorist organisations and persons financing terrorism prevented from collecting, transferring and using funds, as well as misuse of the non-governmental sector for those purposes;

- natural and legal persons involved in the proliferation of weapons of mass destruction and results achieved in preventing the collection, transfer and use of funds in line with relevant resolutions of the United Nations Security Council.

Financial Intelligence Unit shall draft a 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

Financial Intelligence Unit shall, in performing activities within its competence, use the information system of the Financial Intelligence Unit when receiving, exchanging, processing, submitting and publishing data, submissions, acts and other documents and other forms of communication with obliged entities, competent authorities, supervisory authorities and competent authorities of other states, as well as in communication among

officers referred to in paragraph 3 of this Article. This information system shall constitute an integrated set of information and communication technologies necessary for collecting, recording, retaining, processing and transmitting data, information and documentation in electronic form (hereinafter: “FIU IS”).

Financial Intelligence Unit shall establish and manage FIU IS.

Only officers of the Financial Intelligence Unit shall have access to data, information and documents referred to in paragraph 1 of this Article, unless otherwise provided by this Law.

**Components of the Information System of the Financial Intelligence Unit**

**Article 101**

FIU IS shall consist of:

- a facility or premises meeting all conditions for the accommodation and operation of computer and communication equipment in line with international standards (data centre);
- a facility or premises in which backup computer systems and related equipment are installed to ensure business continuity and eliminate the possibility of data loss in the event of incidents, and which meets all conditions for the accommodation and operation of computer and communication equipment in line with international standards (disaster recovery centre);
- information and communication infrastructure consisting of a set of information and communication technologies necessary for the operation of FIU IS;
- infrastructure systems consisting of computer programmes implemented at system level;
- application systems consisting of purpose-developed computer programmes for business functions;
- internet systems consisting of purpose-developed computer programmes for providing services on the internet.

Components of FIU IS referred to in paragraph 1 of this Article shall be functionally connected and form a single whole.

**Management of and Access to the FIU IS**

**Article 102**

Financial Intelligence Unit shall manage FIU IS in line with international standards in the fields of project management, process management, information security, operational risk and business continuity and other forms of management.

Financial Intelligence Unit shall develop and improve FIU IS in line with international standards in the field of development and improvement of information systems.

Only officers of the Financial Intelligence Unit authorised to manage FIU IS shall have access to FIU IS.

Notwithstanding paragraph 3 of this Article, professional persons engaged in the maintenance and improvement of FIU IS shall also have access to FIU IS, provided that they shall not have access to data, information and documents in FIU IS.

Professional persons referred to in paragraph 4 of this Article may not stay on the premises or access FIU IS without the presence of an officer referred to in paragraph 3 of this Article.

Head of the Financial Intelligence Unit shall regulate by an internal act the manner of managing and engaging professional persons referred to in paragraph 4 of this Article in

the maintenance and improvement of FIU IS and other matters relevant to the functioning of FIU IS.

Act referred to in paragraph 6 of this Article shall be marked with the appropriate classification level, in line with the law governing data confidentiality.

**Audit of the FIU IS**

Article 103

Financial Intelligence Unit shall audit FIU IS at least once every two years.

Audit referred to in paragraph 1 of this Article shall include verification of:

- functionality of all components of FIU IS;
- reliability of FIU IS;
- security of FIU IS;
- efficiency and effectiveness of the use of FIU IS;
- compliance of the use of FIU IS with applicable regulations and international standards.

Result of the audit referred to in paragraph 1 of this Article shall be submitted to Head of the Financial Intelligence Unit, who shall, on its basis, adopt an action plan for improving and remedying deficiencies in FIU IS.

Act referred to in paragraph 3 of this Article shall be marked with the appropriate classification level, in line with the law governing data confidentiality.

**Electronic Communication Between the Financial Intelligence Unit and Other Entities**

**Article 104**

Financial Intelligence Unit shall use a single official electronic communication address when communicating with obliged 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 of other states and shall publish it on the website of the Financial Intelligence Unit.

Officer in the Financial Intelligence Unit shall use the single official electronic communication address of that officer in official electronic communications.

Financial Intelligence Unit shall assign a single official electronic communication address for its own needs and the needs of its officers.

Subdomain under the domain of a state administration authority shall be opened for the needs of Financial Intelligence Unit (foj.gov.me).

Head of the Financial Intelligence Unit shall regulate by an internal act the manner of opening, changing and cancelling the single official electronic communication address of Financial Intelligence Unit and its officers.

**Information Submission Mechanism**

**Article 104a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 26)*

Financial Intelligence Unit shall establish on its website a mechanism for submitting information about violations of the provisions of this Law and reporting suspicious transactions, in such a way that the identity of the person providing the information is known only to the Financial Intelligence Unit.

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

Detailed manner of operation and implementation of the mechanism referred to in paragraph 1 of this Article shall be regulated by an internal act of Head of the Financial Intelligence Unit, which shall be marked with the appropriate classification level, in line with the law governing data confidentiality.

## VI. INTERNATIONAL COOPERATION

### Establishing International Cooperation
### Article 105

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 25)*

Financial Intelligence Unit may, for the purpose of establishing, conducting and improving international cooperation, conclude agreements with competent authorities of other states and international organisations on the exchange of financial intelligence data, information on bank accounts and safe-deposit boxes, financial information, financial analyses, other information and documentation, which may be used solely for the purposes provided for by this Law, as well as on other matters relevant to the prevention of money laundering and terrorist financing.

Differences in the definitions of predicate offences shall not constitute an obstacle to cooperation, exchange and use of intelligence information between Financial Intelligence Unit and a foreign Financial Intelligence Unit.

### Request to a Competent Authority of Another State to Submit Data, Information and Documentation

### Article 106

Financial Intelligence Unit may request from an authority of another state that performs activities in that state relating to the prevention of money laundering and terrorist financing and other matters relevant to the prevention and detection of money laundering and terrorist financing (hereinafter: 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 persons, transactions and assets relevant to the prevention and detection of money laundering, related predicate offences, criminal activity or terrorist financing.

Financial Intelligence Unit may request from another authority of another state or an international organisation competent for the prevention and detection of money laundering and terrorist financing, or from an authority of another state competent for the confiscation of assets, to submit data, information and documentation referred to in paragraph 1 of this Article.

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

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, should reasons for urgency exist, Financial Intelligence Unit may submit the request referred to in paragraph 2 of this Article to another authority of another state or an international organisation competent for the prevention and

detection of money laundering and terrorist financing, or to an authority of another state competent for the confiscation of assets.

Data, information and documentation may, in the cases referred to in paragraphs 1, 2 and 3 of this Article, be exchanged electronically through secure communication systems of the World Association of Financial Intelligence Units or another international communication system providing the same or a higher level of data protection, or in another appropriate manner in line with an international agreement.

Data, information and documentation obtained in line with paragraphs 1, 2 and 3 of this Article may be used by Financial Intelligence Unit solely for the purpose for which they were obtained and may not, without the prior consent of the foreign Financial Intelligence Unit, another authority of another state or international organisation competent for the prevention and detection of money laundering and terrorist financing, or an authority of another state competent for the confiscation of assets from which they were obtained, be used, submitted or made available to another authority, legal or natural person, or used for administrative purposes, investigations or criminal prosecution, or any other purpose inconsistent with the conditions and restrictions established by that authority or international organisation.

**Submission of Data, Information and Documentation at the Request of an Authority of Another State**

**Article 107**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 28)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 39)*

Financial Intelligence Unit may, upon a request containing reasons or grounds for suspicion that money laundering, related predicate offences or terrorist financing is involved or that assets originate from criminal activity and stating the purpose for which the data are requested, submit in a timely manner to the foreign Financial Intelligence Unit information on bank accounts and safe-deposit boxes, financial information, financial analyses and other data, information and documentation on persons, transactions and assets relevant to the prevention and detection of money laundering, related predicate offences, criminal activity or terrorist financing.

Financial Intelligence Unit may submit the data, information and documentation referred to in paragraph 1 of this Article, upon request, to other authorities of another state or international organisations competent for the prevention and detection of money laundering and terrorist financing, an authority of another state competent for the confiscation of assets and supervisory authorities of another state.

Data, information and documentation may, in the cases referred to in paragraphs 1 and 2 of this Article, be exchanged electronically through secure communication systems of the World Association of Financial Intelligence Units or another international communication system providing the same or a higher level of data protection, or in another appropriate manner in line with an international agreement.

Notwithstanding paragraph 3 of this Article, the Financial Intelligence Unit may, upon a reasoned request of the European Union Agency for Law Enforcement Cooperation (hereinafter: Europol), submit information on bank accounts and safe-deposit boxes, financial information and financial analyses referred to in paragraph 1 of this Article through the network application for the secure exchange of Europol information in cases concerning the prevention, detection and suppression of serious criminal offences within the competence of Europol.

Financial Intelligence Unit may respond to a request of a foreign Financial Intelligence Unit even where the predicate offence or criminal activity is not known at the time of receipt of the request.

Financial Intelligence Unit shall notify the requesting party in writing of the refusal of the request referred to in paragraphs 1, 2 and 4 of this Article and state the reasons for the refusal.

Foreign Financial Intelligence Unit may make available the data, information and documentation obtained under paragraph 1 of this Article to another competent authority or a third party only with the prior consent of Financial Intelligence Unit.

Financial Intelligence Unit shall not submit data referred to in paragraphs 1 and 2 of this Article or give the consent referred to in paragraph 7 of this Article if:

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

2) submission of data, information and documentation would endanger or could endanger the conduct of preliminary investigations or criminal proceedings in Montenegro or otherwise harm the interests of those proceedings;

3) submission of data, information and documentation would not be in line with the fundamental principles of the legal system of Montenegro.

Financial Intelligence Unit shall give written reasons for refusing to give the consent referred to in paragraph 7 of this Article and submit them to the applicant.

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

Financial Intelligence Unit may determine conditions and restrictions on 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 data on bank accounts and safe-deposit boxes, financial information, financial analyses and other data, information and documentation obtained from the Financial Intelligence Unit, upon request and on an individual basis, with other authorities of another state only with the prior consent of the Financial Intelligence Unit and where such data, financial information or financial analyses are necessary for preventing, detecting and suppressing money laundering, related predicate offences and terrorist financing.

Provisions of the law governing the protection of personal data shall apply to the protection of data and information exchanged in line with paragraphs 1, 2, 4 and 12 of this Article.

**Submission of Data, Information and Documentation to an Authority of Another State on Own Initiative**

**Article 108**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 29)*

Financial Intelligence Unit may, without a request and on its own initiative, submit to a foreign Financial Intelligence Unit, other authorities of another state or international organisations competent for the prevention and detection of money laundering and terrorist financing, an authority of another state competent for the confiscation of assets and supervisory authorities of another state, information on bank accounts and safe-deposit boxes, financial information, financial analyses and other data, information and

documentation on persons, transactions and assets in respect of which there are reasons or grounds for suspicion that money laundering, related predicate offences or terrorist financing is involved or that the assets originate from criminal activity, obtained in line with this Law, for the purpose of preventing and detecting money laundering, related predicate offences, criminal activity or terrorist financing.

Financial Intelligence Unit shall promptly forward the suspicious transaction report referred to in Article 66 paragraph 6 of this Law, which concerns a Member State of the European Union, to the Financial Intelligence Unit of that Member State.

When submitting data, information and documentation in line with paragraph 1 of this Article, Financial Intelligence Unit may determine the conditions and restrictions under which such data, information and documentation may be used and further transmitted.

## Temporary Suspension of Execution of a Transaction and Temporary Prohibition of Access to a Safe-deposit Box upon the Initiative of an Authority of Another State

### Article 109

Financial Intelligence Unit may, in line with this Law, upon a reasoned initiative of a foreign Financial Intelligence Unit or another authority of another state competent for the prevention and detection of money laundering and terrorist financing, by order suspend execution of a transaction or prohibit access to a safe-deposit box for no more than 72 hours.

Financial Intelligence Unit shall, in the case referred to in paragraph 1 of this Article, act in line with Article 93 of this Law.

Financial Intelligence Unit may reject the initiative referred to in paragraph 1 of this Article if, on the basis of the facts and circumstances stated in the initiative, it assesses that insufficient reasons or grounds for suspicion exist that funds or other assets originate from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, and shall notify the foreign Financial Intelligence Unit or another authority of another state competent for the prevention and detection of money laundering and terrorist financing thereof, stating the reasons for the rejection.

## Initiative to an Authority of Another State for Temporary Suspension of Execution of a Transaction and Temporary Prohibition of Access to a Safe-deposit Box

### Article 110

Financial Intelligence Unit may, within its activities and powers, submit an initiative for temporary suspension of execution of a transaction or temporary prohibition of access to a safe-deposit box to a foreign Financial Intelligence Unit or another authority of another state competent for the prevention and detection of money laundering and terrorist financing, should it assess that there are reasons or grounds for suspicion that funds or other assets originate from criminal activity or that money laundering, related predicate offences or terrorist financing is involved.

## VII. **OBLIGATIONS OF THE STATE AND OTHER AUTHORITIES AND INSTITUTIONS**

### Authority responsible for customs affairs
### Article 111

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 54)*

State administration authority responsible for customs affairs shall provide the Financial Intelligence Unit with direct electronic access to data on:

-- cross-border transport of physically transferable means of payment in an amount or value of EUR 10,000 or more, no later than three days from the date of that transport;

-- cross-border transport of physically transferable means of payment in an amount or value of EUR 10,000 or more that was not declared or was falsely declared, immediately and no later than three days from the date of that transport;

-- transport or attempted transport of physically transferable means of payment, regardless of the amount, where there are reasons for suspicion of money laundering or terrorist financing in relation to that transport or attempted transport, immediately and no later than three days from the date of that transport or attempted transport;

Cross-border transport of physically transferable means of payment shall be carried out by passengers, by post, by cargo consignments or by other means.

### Temporary retention of physically transferable means of payment

Article 111a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 55)*

State administration authority responsible for customs affairs shall, when supervising cross-border transport of physically transferable means of payment, regardless of the method of transport (by passengers, by post or by cargo consignments) and the amount or value, temporarily retain the physically transferable means of payment if there are reasons for suspicion of money laundering or terrorist financing.

State administration authority responsible for customs affairs shall, in the case referred to in paragraph 1 of this Article, request and collect from the person carrying out the transport additional data on the origin of the physically transferable means of payment.

State administration authority responsible for customs affairs shall issue a certificate of temporary retention of the physically transferable means of payment referred to in paragraph 1 of this Article.

State administration authority responsible for customs affairs shall, without delay, notify the Financial Intelligence Unit of the physically transferable means of payment temporarily retained under paragraph 1 of this Article.

Period of retention of the physically transferable means of payment referred to in paragraph 1 of this Article shall be determined in line with Article 93 of this Law.

Detailed manner of temporary retention, safekeeping and deposit and any return of the physically transferable means of payment referred to in paragraph 1 of this Article shall be prescribed by the state administration authority responsible for financial affairs.

### Registers of accounts and safe-deposit boxes

## Article 112

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 30)*

Central Bank of Montenegro shall maintain registers of accounts and safe-deposit boxes, which constitute an electronic database of open accounts of natural and legal persons and leased safe-deposit boxes, as well as demand deposits and time deposits with credit institutions and branches of foreign credit institutions.

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

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

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

Central Bank of Montenegro shall be responsible for ensuring that the data in the registers of accounts and safe-deposit boxes correspond to the data submitted by credit institutions and branches of foreign credit institutions.

Data from the registers of accounts and safe-deposit boxes shall not be publicly available and their processing, protection and retention shall be governed by regulations governing bank secrecy and protection of personal data.

Exceptionally, data on transaction account numbers and other related data concerning legal persons and sole proprietors shall be publicly available in line with the law governing payment transactions.

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

### Data from the registers of accounts and safe-deposit boxes available to the Financial Intelligence Unit

## Article 113

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 56)*

Financial Intelligence Unit shall have direct electronic access to at least the following data from the registers of accounts and safe-deposit boxes, as well as from the credit register:

for natural persons: name and surname, unique personal identification number for a resident, type, number and issuing state of the identity document for a non-resident, address and city of permanent or temporary residence;

for legal persons: name, registration number, registered office (address, city and country);

type and number of account, name of the credit institution that opened the account, data on account status (active, closed or blocked), and dates of opening and closing the

account;

date of conclusion and expiry of the safe-deposit-box lease agreement and the period for which the agreement was concluded.

Financial Intelligence Unit shall, in addition to the data referred to in paragraph 1 of this Article, have direct electronic access to the following credit-register data: loan amount, number of loan instalments and outstanding loan balance.

Data referred to in paragraph 1 of this Article shall be available to the Financial Intelligence Unit on the basis of data concerning a person or an 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 should they, in carrying out activities within their scope of business, discover facts indicating a possible connection with money laundering, related predicate offences or terrorist financing.

Stock exchanges and clearing and depository companies shall, at the request of the Financial Intelligence Unit, submit data, information or documentation indicating a possible connection with money laundering, related predicate offences or terrorist financing, in line with the law.

Clearing and depository company shall electronically submit on quarterly basis data to the Financial Intelligence Unit on each collective custody account, credit institution or other institution with which that custody account is opened, as well as on the number of transactions and total turnover on that collective custody account.

Provisions of Article 90 paragraphs 4, 5 and 6 of this Law shall apply to the time limits for submitting the data referred to in paragraph 2 of this Article.

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

### State Prosecutor’s Offices, Courts and the State Administration Authority Responsible for Judicial Affairs

### Article 115

For the purpose of carrying out the analysis referred to in Article 99 of this Law, competent State Prosecutor’s Offices, competent courts and the state administration authority responsible for judicial affairs shall regularly submit to the Financial Intelligence Unit data on proceedings concerning misdemeanours and criminal offences related to money laundering or terrorist financing, their perpetrators, as well as the confiscation of assets acquired through the commission of a criminal offence or through criminal activity.

Competent State Prosecutor’s Offices shall submit the following data to the Financial Intelligence Unit:

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

Competent courts shall submit the following data to the Financial Intelligence Unit:

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

State administration authority competent for judicial affairs shall provide the Financial Intelligence Unit with data on received and sent requests for international legal assistance in connection with the criminal offences referred to in paragraph 1 of this Article, as well as data on temporarily and permanently seized property.

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

## VII. RECORDS, DATA PROTECTION AND RETENTION

### 1. Types and contents of records

### Records kept by an obliged entity
### Article 116

Obliged entity shall keep:

1) records on customer due diligence and monitoring measures;
2) records of complex and unusual transactions referred to in Article 58 of this Law;
3) records on data submitted to the Financial Intelligence Unit in line with Articles 66 and 90 of this Law;
4) records of orders on temporary suspension of execution of a transaction or temporary prohibition of access to a safe-deposit box;
5) records of requests for the ongoing monitoring of the financial operations of the

customer;

6) records of access by supervisory authorities referred to in Article 131 paragraph 1 of this Law, to data, information and documentation in connection with which the obliged entity shall act in line with Article 123 paragraph 1 of this Law;

7) Records on the professional training and development of employees of the obliged entity in the field of the prevention of money laundering and terrorist financing.

Obliged entity shall keep the records referred to in paragraph 1 of this Article in a manner ensuring the reconstruction of individual transactions, including the amounts and currency, which could be used in proceedings for detecting criminal activities of customers.

**Content of records kept by obliged entities**

Article 117

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 40)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 57)*

Records of customer due diligence and monitoring measures shall contain the following data:

1) for a legal person: name, registered office (address and city or municipality for a legal person with its registered office in Montenegro and, for a legal person with its registered office in another country, country, address and city), address of the place of business where different from the registered office (address, city or municipality for a legal person with its registered office in Montenegro and, for a legal person with its registered office in another country, country, address and city), registration number, information on whether it is a resident or non-resident, reason for the business relationship (establishing a business relationship, carrying out a transaction, attempting to carry out a transaction, leasing a safe-deposit box, accessing a safe-deposit box, policyholder, beneficiary under an insurance policy, seller or buyer), telephone number and e-mail address;
2) for a sole proprietor: name, registered office (address and city or municipality for a sole proprietor with registered office in Montenegro and, for a sole proprietor with registered office in another country, country and city), unique personal identification number, name and surname, information on whether they are a resident or non-resident, reason for the business relationship (establishing a business relationship, carrying out a transaction, attempting to carry out a transaction, leasing a safe-deposit box, accessing a safe-deposit box, policyholder, beneficiary under an insurance policy, seller or buyer), telephone number and e-mail address;
3) for a natural person: name and surname, unique personal identification number, address and municipality of residence or temporary residence in Montenegro, date of birth, country of birth, citizenship, information on whether the person is a politically exposed person, the basis on which the person is politically exposed, including by virtue of office, as a family member or close associate, information on whether the person is a resident or non-resident, telephone number and e-mail address, type, number, country of issue and expiry date of the identity document, reason for the business relationship (establishing a business relationship, carrying out a transaction, attempting to carry out

a transaction, leasing a safe-deposit box, accessing a safe-deposit box, policyholder, beneficiary under an insurance policy, seller or buyer), information on whether the natural person is a customer, representative, authorised person, beneficial owner, founder, trustee, beneficiary of managed property, insured person, policyholder, beneficiary under an insurance policy, seller or buyer;

4) data on the manner in which the customer was identified (identification in the physical presence of the customer, electronic identification or video-electronic identification);

4a) data referred to in Article 42 paragraph 11 and Article 44 of this Law;

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

6) data on the purpose, intended use, objective and nature of the business relationship and transaction, the basic activity code of the customer and scanned documentation accompanying the business relationship or transaction, data on the source of assets and funds that are or will be the subject of the business relationship or transaction, the date of establishment of the business relationship, or the date and time of entry into the casino or access to a safe-deposit box;

7) transaction data: date and time of execution of the transaction, amount of the transaction in euros, amounts of transactions by currency, transaction order number, policy or contract, depending on the type of obliged entity, information on whether the transaction was executed in full or in part, information on the type of transaction (cash, non-cash or crypto-asset), type of transaction (regular, suspicious, unusual or complex), data on the credit institution of the payer and payee (type and number of account, registration number, name and country of registered office), type of transaction (payment or disbursement), manner of execution of the transaction depending on the type of obliged entity (cash, non-cash, already executed, in instalments, market or non-market), purpose of the transaction and the name of the branch of the obliged entity executing the transaction, the crypto-asset deposit address of the originator and the crypto-asset deposit address of the beneficiary;

Should the obliged entity be an organiser of games of chance or provide safe-deposit-box rental services, records of customer due diligence and monitoring measures shall, in addition to the data referred to in paragraph 1 item 3 of this Article, contain for natural persons data on the conduct of the natural person depending on the type of obliged entity (entry into premises where games of chance are organised, access to games of chance via the Internet or other telecommunications means, access to the cash desk, access to other places or locations where transactions are carried out depending on the type of game of chance, or access to a safe-deposit box).

Should the transaction be related to the obliged entities referred to in Article 4 paragraph 2 item 1 of this Law, the records on the customer due diligence and monitoring 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, namely: type and number of the account, registration number, name and country of the registered office of the credit institution of the account, name and surname, address and city of permanent or temporary residence of the natural person to whom the transaction is intended or name, registered office (address, city and country) of the legal person to whom the transaction is intended, telephone and e-mail address of those persons, SWIFT code of the credit institution, country of destination, name and the country of the registered office of the credit institution that is the correspondent.

Should the transaction be related to the obliged entities referred to in Article 4 paragraph 2 item 7 of this Law, the records on the customer due diligence and monitoring 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, namely: stock exchange

code, security code, number of shares, share price, of the seller broker code, of the buyer broker code, of the seller account number on the stock exchange, as well of the buyer account number on the stock exchange.

Should the transaction be related to the obliged entities referred to in Article 4 paragraph 2 items 8 and 9 of this Law, the record of customer due diligence and monitoring measures, in addition to the data referred to in paragraph 1 item 7 of this Article, shall also contain the following data about the transaction: insurance start date, insurance duration in years, information on the type of the premium (one-time, monthly, quarterly, semi-annual or annual), name and surname of the beneficiary of the insurance policy and information on the reason for the payment (insured event, termination of the contract or expiration of the contract).

Should the transaction be related to the obliged entities referred to in Article 4 paragraph 2 item 13 and paragraph 4 of this Law, the records on the customer due diligence and monitoring 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, namely:

1) for valuable items: information about the type of valuable item (art, precious metal, precious stones, securities, crypto wallet or other valuable items), information about the art (name, value, description, category, subcategory, style, theme, technique and material), data on precious metals (name, value, description, weight, number of carats, colour of the metal, type, clarity, size and type of the metal), data on precious stones (width, clarity of diamond, dimensions of diamond, shape, colour and data on clarity or purity), data on the bearer of securities (symbol, type and status of the security, unique identification mark of the financial instrument in line with the ISO 6166 standard  ISIN), data on the crypto wallet (code of the crypto wallet and service provider crypto wallet), data on other valuable items (name, value and description);

2) for immovable property: information on the type and the value of the immovable property, address, house number, city, postal code, country, immovable property registration number, information on right in rem to that immovable property, the basis for acquiring the right in rem, area, number of floors, date of registration of the right in rem to the real estate cadastre, cadastral municipality, plot number, area, notes, scope of rights and age of the immovable property;

3) for means of transport: information on the type (road vehicle, vessel, aircraft or other means of transport), value, type and registration number, country in which the means of transport is registered, registration validity date, make and model, chassis number, name of the manufacturer, identification number, information on the category, manufacturer, type/model and serial number of the engine of the means of transport, as well as the type or name of the vessel.

Records of complex and unusual transactions shall contain data referred to in paragraphs 1 to 6 of this Article.

Record of data submitted to the Financial Intelligence Unit in line with Articles 66 and 90 of this Law shall contain the 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 the reasons for suspicion that property originates from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, the date on which the data were submitted to the Financial Intelligence Unit and the reasons for executing the transaction (explanation).

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

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

Records of requests for monitoring of the financial operations of the customer shall continuously contain the number of requests, information on the type and number of the customer account, the starting date of monitoring, the extension date of the 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.

Record of the access of supervisory authorities referred to in Article 131 paragraph 1 of this Law to data, information and documentation in connection with which the obliged entity shall act in line with Article 123 paragraph 1 of this Law shall contain the name of the supervisory authority, the name and surname of the supervisory officer, the date and time of data inspection, information and documentation referred to in paragraph 1 items 1, 2 and/or 3 of this Article for the person whose the data, information and documentation were inspected.

Record of professional training and professional development of employees in the field of prevention of money laundering and terrorist financing shall contain the name and surname and workplace of the employee who completed the professional training and professional development, the name and date of the professional training and professional development, the name of the professional training and professional development organiser (employer, professional association, Financial Intelligence Unit or other professional body or organisation in Montenegro or another country).

**Records kept by the customs authority**

**Article 118**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 58)*

State administration authority responsible for customs affairs shall keep:

1) records of transport or attempted transport across the state border of physically transferable means of payment in an amount or value of EUR 10,000 or more that were declared, undeclared or falsely declared;
2) records of cross-border transport of physically transferable means of payment, regardless of the amount, where there are reasons or grounds for suspicion that the assets originate from criminal activity or that money laundering or terrorist financing is involved;
3) records of imports/exports of money-counting machines;
4) records of imports/exports of gaming machines and self-service terminals within the meaning of the law governing games of chance;
5) records of imports/exports of motor vehicles with an invoiced value of EUR 100,000 or more.

**Content of records kept by the state administration authority responsible for customs affairs**

**Article 119**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 59)*

Records of transport or attempted transport across the state border of physically

transferable means of payment in an amount or value of EUR 10,000 or more that was declared, undeclared or falsely declared shall contain the following data:

1) for a natural person who transports or attempts to transport physically transferable means of payment across the state border: name and surname, unique personal identification number, address and city of permanent or temporary residence, citizenship, and type, number, issuing state and expiry date of the identity document;

2) for a legal or natural person on whose behalf physically transferable means of payment are transported across the state border: name, registered office (address and city or municipality for a legal person with its registered office in Montenegro and, for a legal person with its registered office in another country, the country), registration number and TIN of the legal person, or name and surname, unique personal identification number, address and city of permanent or temporary residence and citizenship of the natural person;

3) for a legal or natural person for whom the physically transferable means of payment are intended: name, registered office (address and city or municipality for a legal person with its registered office in Montenegro and, for a legal person with its registered office in another country, the country), registration number and TIN of the legal person, or name and surname, unique personal identification number, address and city of permanent or temporary residence and citizenship of the natural person;

4) amount, currency and data on the type, source and purpose of the physically transferable means of payment being transported or attempted to be transported across the state border;

5) data on the physically transferable means of payment being transported or attempted to be transported across the state border: type of physically transferable means of payment (cash, bearer securities, cheques, bills of exchange and other physically transferable means of payment payable to bearer), data on bearer securities (symbol, type and status of the security and unique identification code of the financial instrument in line with ISO 6166 - ISIN), and data on cheques and bills of exchange (serial number and date and place of issue), depending on data availability;

6) name of the border crossing point at which the transport or attempted transport of physically transferable means of payment across the state border was carried out, date and time of the transport or attempted transport, information on whether it concerns entry into or exit from Montenegro and the name of the country from which or to which the transport is carried out;

7) information on whether the transport of physically transferable means of payment was declared, undeclared or falsely declared to the state administration authority responsible for customs affairs;

8) data on the sender in the case of transport by post, cargo or other means: name and surname, unique personal identification number, address and city of permanent or temporary residence, or name, registered office (address, city/municipality and country), registration number and TIN for a legal person;

9) data on the recipient in the case of transport by post, cargo or other means: name and surname, unique personal identification number, address and city of permanent or temporary residence, or name, registered office (address, city/municipality and country), registration number and TIN for a legal person, and date of receipt of the consignment;

10) data on the carrier/courier service in the case of transport by post, cargo or other means: name, registered office, registration number and TIN;

11) identification data on the consignment itself in the case of transport by post, cargo or other means: waybill number, bill of lading number or another unique consignment identification number, date and place of receipt of the consignment, and country of origin

and country of destination of the assets;

12) data on the contents of the consignment in the case of transport by post, cargo or other means: type, quantity or value;

13) information on whether, in the case of transport by post, cargo or other means, the contents of the consignment (cash, bearer securities, cheques, bills of exchange and other physically transferable means of payment) were declared to the state administration authority responsible for customs affairs.

Records of cross-border transport of physically transferable means of payment, regardless of the amount or value, where there are reasons or grounds for suspicion that the assets originate from criminal activity or that money laundering or terrorist financing is involved, shall contain the data referred to in paragraph 1 items 1 to 13 of this Article, data on indicators for identifying suspicious customers that exist in relation to the specific case and information on whether the transaction was withheld from execution.

Records of imports/exports of money-counting machines and records of imports/exports of gaming machines and self-service terminals shall contain the following data: declaration date, exporter TIN, exporter name, importer TIN, importer name, country of dispatch/export, country of origin, trade name of the goods, serial number of the goods, place of delivery under the applicable trade term, representative TIN, representative name, value of the goods, quantity of the goods, customs value of the goods and statistical value of the goods.

Records of imports/exports of motor vehicles shall contain the following data: declaration date, exporter TIN, exporter name, importer TIN, importer name, country of dispatch/export, country of origin, trade name of the goods, make, model, year of manufacture, chassis number, place of delivery under the applicable trade term, representative TIN, representative name, value of the goods, customs value of the goods and statistical value of the goods.

**Records kept by the Financial Intelligence Unit**

**Article 120**

Financial Intelligence Unit shall keep the following records:

1) Records of the analyses it performs and the cases on which it acts in line with the law;

2) Records of the obliged entities, compliance officers for the prevention of money laundering and terrorist financing, or their deputies;

3) Records of criminal offences and misdemeanours and perpetrators of criminal offences and misdemeanours referred to in Article 115 of this Law;

4) Records on the actions of the supervisory authorities referred to in Article 131 paragraph 1 of this Law towards the obliged entities;

5) Records of Financial Intelligence Unit officers who inspected or accessed data, or to whom data from other authorities was provided in line with Article 126 of this Law.

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

**Content of the records kept by the Financial Intelligence Unit**

Article 121

Record of the analyses it performs and the cases on which it acts in line with this Law shall contain the following data:

- data referred to in Article 117 paragraphs 1 to 6 and paragraphs 8 and 9 of this Law;

- case number, name of the case, number of the received document, name and surname or name of the sender and recipient of the document, date of sending the document, date of delivery of the document, information on whether the document is marked with a classification level, data representing the reasons for temporary suspension of the transaction, data that represent the reasons for continuous monitoring of the financial operations of the customer, the legal qualification of the criminal offence, the result of the operational or strategic analysis, the reasons for not providing a response to the request or information in line with Article 96 paragraphs 4 and 5 of this Law, scanned received and sent documents, scanned documentation attached to documents; and

- data on persons subject to the financial analysis: mobile phone number, International Unique Mobile Device Identifier (IMEI), photograph, scanned page with personal document data, scanned card of deposited signatures, previous personal data (unique personal identification number, name and surname and date of birth ), false personal data (unique identity number, name and surname, date of birth, residential address, citizenship), previous names of the legal person and information about the founder of the legal person (identity number, TIN, name, address, city and country of the registered office, the country legal person is registered in),

-Data on orders for temporary suspension of execution of transactions referred to in Articles 93, 109 and 110 of this Law,

-Data on requests for continuous monitoring of the financial operations of the customer referred to in Article 95 of this Law;

- Data from responses on requests referred to in Articles 91 and 92 of this Law;

- Data from requests, information and notification referred to in Articles 96, 97 and 98 of this Law;

-Data on international requests and information referred to in Articles 106, 107 and 108 of this Law;

-Data taken over from the authority responsible for customs affairs referred to in Article 111 of this Law;

- Data on bank accounts and safe-deposit boxes referred to in Article 113 of this Law;

-Data on delivery of stock exchanges and clearing and depository companies referred to in Article 114 of this Law; and

- Data from documents sent and received.

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

1) For the obliged entity: identification number, TIN, name and registered office (address, city, or municipality for obliged entities based in Montenegro, or country for obliged entities based in another country) and the work permit information (issued, revoked or not required);

2) For the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer: unique personal identification number, name and surname, information on whether the person is a compliance officer or deputy compliance officer, e-mail address, telephone number, mobile telephone number, start and end date of performing the duties of compliance officer or deputy compliance officer, licence number and date of issue and expiry of the licence.

Records on criminal offences and misdemeanour and perpetrators of the criminal offences and misdemeanours referred to in Article 115 of this Law shall contain data referred to in Article 115 paragraphs 2, 3 and 4 of this Law.

Records on the actions of supervisory authorities referred to in Article 131 paragraph

1 of this Law towards the obliged entities shall contain data referred to in Article 135 paragraphs 1, 2, 4 and 5 of this Law.

Records of Financial Intelligence Unit officers who inspected or accessed data or to whom data from other authorities were provided in line with Article 126 of this Law shall contain the unique personal identification number of the officer who inspected or accessed the data or to whom the data were provided, the legal basis, date and time of inspection, access or provision of data, as well as the data inspected, accessed or provided.

### Data records on non-residents

### Article 122

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

## 2. Data Protection

### Prohibition of data disclosure

### Article 123

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 60)*

Obliged entities and their employees, members of management, supervisory or other executive bodies, and other persons to whom data referred to in Article 117 paragraphs 1 to 11 of this Law or Article 66 of this Law are or were available, shall not disclose to a customer or third party that:

1) data have been communicated to the Financial Intelligence Unit, information has been made available for inspection or documentation concerning a customer or transaction, as well as any act, has been submitted in line with Articles 66 and 90 of this Law;
2) Financial Intelligence Unit, pursuant to Article 93 of this Law, has issued an order to temporarily suspend execution of a transaction or prohibit access to a safe-deposit box, or has given instructions to the obliged entity in that regard;
3) Financial Intelligence Unit, pursuant to Article 95 of this Law, has requested continuous monitoring of the financial operations of the customer;
4) a preliminary investigation or investigation has been or could be initiated against the customer or a third party due to grounds for suspicion or well-founded suspicion that the criminal offence of money laundering, a related predicate offence or terrorist financing has been committed.

Attempting to deter the customer from engaging in, carrying out or participating in unlawful activity shall not constitute disclosure within the meaning of paragraph 1 of this Article.

Prohibition of disclosure referred to in paragraph 1 of this Article shall not apply to data that, in line with this Law, is obtained and maintained by the obliged entity and that is necessary for the establishment of facts in criminal proceedings and if the submission of such data in written form is requested or ordered by a competent court or supervisory authority referred to in Article 131 paragraph 1 of this Law for the purpose of implementing

this Law.

Data referred to in paragraph 1 of this Article, notifications on suspicious transactions, financial information, financial analyses, as well as all other data, information and documentation that the Financial Intelligence Unit in line with this Law collected or prepared in order to prevent and detect money laundering, related predicate offences and terrorist financing may not be submitted to other persons for inspection, nor can their existence be confirmed in the records of the Financial Intelligence Unit, unless otherwise provided by this Law.

When there are grounds for suspicion that it is money laundering, related predicate offences and terrorist financing, data referred to in paragraph 4 of this Article shall be marked with an appropriate classification level in line with the law that regulates data confidentiality.

Data, information and documents referred to in paragraph 5 of this Article may be declassified if there is no other way to achieve a timely exchange of data at the national and international level in order to effectively prevent, detect and prosecute money laundering crimes, related predicate offences and terrorist financing, with the obligation to store data in line with Article 130 of this Law.

For the purpose of ensuring effective and timely international cooperation, information, notifications and requests referred to in paragraph 4 of this Article marked with the classification level "INTERNAL" may be submitted to foreign Financial Intelligence Units, other competent authorities of other states and international organisations, including through the communication systems of the World Association of Financial Intelligence Units.

**Exception to the principle of keeping confidentiality**

**Article 124**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 31)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 61)*

Obligation to preserve data confidentiality (business, banking, professional and other secrecy) shall not apply to obliged entities, their employees, members of management, supervisory or other executive bodies, or other persons to whom data referred to in Article 117 paragraphs 1 to 11 of this Law are or were available, holders of public authority, state authorities and their employees when submitting data, information and documentation to the Financial Intelligence Unit in line with this Law, nor to an obliged entity that is a member of a financial group when exchanging data and information with other members of the financial group under the conditions referred to in Article 62 of this Law.

Obligation to maintain the confidentiality of data (business, banking, professional or other secrets) shall not apply in cases of information exchange between obliged entities referred to in Article 4 paragraph 2 item 13 indent 2, and paragraphs 3 and 4 of this Law, from Montenegro, Member States of the European Union, and third countries that apply the same or higher standards for the implementation of anti-money laundering and counter-terrorist financing measures as those established under this Law or under European Union law, regardless of whether the persons concerned are employed by the same legal person or by a larger structure to which the legal person belongs and with which it is connected by common ownership, management, or compliance control.

Obligation to maintain the confidentiality of data (business, banking, professional or

other secrets) shall not apply, in cases involving the same customer and the same transaction where two or more obliged entities participate, between credit and financial institutions or between obliged entities performing professional 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 a Member State of the European Union or in a third country that applies anti-money laundering and counter-terrorist financing measures equivalent to the provisions of this Law;

2) they carry out the same type of activity or belong to the same category of professional activity; and

3) they are subject to obligations concerning the protection of professional and business secrecy and personal data.

Obliged entity and its employees shall not be liable for damage caused to customers or third parties if, in line with this Law, they:

1) provide data, information and documentation on their customers to the Financial Intelligence Unit;

2) obtain and process data, information and documentation on their customers;

3) execute the order of the Financial Intelligence Unit on temporary suspension of transaction or prohibition of access to the safe-deposit box;

4) carry out the request of the Financial Intelligence Unit on continuous monitoring of the financial operations of the customer.

Obliged entity or an employee of the obliged entity shall not be held criminally or disciplinarily liable for breach of the obligation to preserve data confidentiality if they:

1) provide data, information and documentation to the Financial Intelligence Unit, in line with this Law;

2) process data, information and documentation, obtained in line with this Law, with a view to verifying customers and transactions or grounds for suspicion that the property originates from criminal activity or that it is money laundering or terrorist financing.

**Protection of the integrity of the compliance officer for the prevention of money laundering and terrorist financing and employees**

**Article 125**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 32)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 41)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 62)*

Obliged entity shall take the necessary measures to protect the compliance officer for the prevention of money laundering and terrorist financing and other employees who implement the provisions of this Law from threats and other unfavourable or discriminatory actions aimed at their physical or psychological integrity.

Obliged entity shall take the necessary measures to ensure that decisions of the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer are not compromised by the commercial interests of the obliged entity and that such interests do not unduly influence the compliance officer or deputy

compliance officer.

Obliged entity shall, with the prior opinion of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, establish appropriate procedures governing the manner in which employees may report breaches of the provisions of this Law through a dedicated and anonymous channel, in line with the nature and size of the obliged entity.

Paragraph 3 of this Article shall not apply where the obliged entity has only one employee.

**Use of received personal data**

**Article 126**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 33)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 42)*

Financial Intelligence Unit, state authorities, state administration bodies, holders of public authority, obliged entities, and their employees shall use personal data obtained in line with this Law solely for the purpose for which such data is processed, and such data shall not be processed for commercial purposes.

Authorities providing electronic access to data 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 shall keep records of inspections and access by the Financial Intelligence Unit or electronic provision of data to it, including the date and time of commencement and completion of the inspection or access.

For the exchange of personal data between the Financial Intelligence Unit and state authorities, state administration bodies and holders of public authority, a security communication link shall be used, which represents a protected system of data exchange between precisely defined entities.

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

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

**Keeping data**

**Article 127**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 43)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 63)*

Obliged entity shall retain all data, information and documentation obtained in line with this Law, data on the identification number of each customer account, data and documentation on electronic funds transfers, business correspondence and reports for five years after termination of the customer business relationship, execution of an

occasional transaction, refusal to establish a business relationship, refusal to execute an occasional transaction, entry of the customer into a casino or premises where other games of chance are organised or access to a safe-deposit box, unless a longer retention period is prescribed by a special law.

Obliged entity shall retain a photocopy of an identity document, other documents and documentation, as well as written authorisations, in line with paragraph 1 of this Article.

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, on a case-by-case basis, require the extended retention of the data, information and documentation referred to in paragraphs 1 and 2 of this Article, provided that such retention is necessary for the prevention, detection, investigation, or prosecution of money laundering or terrorist financing cases, for a period not exceeding five years from the expiry of the period referred to in paragraph 1 of this Article.

Obliged entity shall retain data and supporting documentation concerning the compliance officer for the prevention of money laundering and terrorist financing or deputy compliance officer, professional training and development of employees in the field of prevention and detection of money laundering and terrorist financing and implementation of internal control and audit measures for four years from the expiry of the licence, completion of professional training and development or completion of internal control and audit, respectively.

Following expiry of the periods referred to in paragraphs 1 to 4 of this Article, the obliged entity shall delete or destroy personal data of the customer.

Should the obliged entity cease to exist, it 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 retain them for five years from the date of receipt.

**Keeping data with the administrative authority responsible for customs affairs**

**Article 128**

Customs authority shall keep data from records referred to in Article 119 of this Law for the period of ten years after the date of obtaining those data.

Following expiry of the period referred to in paragraph 1 of this Article, personal data from the records referred to in Article 119 of this Law shall be deleted.

**Keeping data in the Register of beneficial owners and registers of accounts and safe-deposit boxes**

**Article 129**

Administrative authority competent for tax collection shall retain data in the Register of Beneficial Owners for ten years from the date deemed, in line with the law, to be the date of cessation of existence of the entity referred to in Article 43 paragraph 3 of this Law.

Central Bank of Montenegro shall retain data in the registers of accounts and safe-deposit boxes for ten years after closure of the account or expiry of the safe-deposit-box rental agreement.

Following expiry of the periods referred to in paragraphs 1 and 2 of this Article, personal data from the Register of beneficial owners or registers of accounts and safe-deposit boxes shall be deleted.

**Record keeping at the Financial Intelligence Unit**

**Article 130**

Financial Intelligence Unit shall retain data from the records it keeps in line with this Law for 11 years from the date on which those data were obtained.

Following expiry of the period referred to in paragraph 1 of this Article, data referred to in paragraph 1 of this Article that are in electronic form shall be depersonalised, while data in paper form shall be delivered to the competent recycling centre for destruction.

Financial Intelligence Unit shall not inform a person of the information and data it possesses in relation to them, nor another person, nor allow access before the expiration of 10 years from the date of their recording, unless otherwise provided by this Law.

Person referred to in paragraph 3 of this Article shall have the right to check their personal data after the expiration of 10 years from the date of their recording.

Detailed manner of depersonalisation of data referred to in paragraph 1 of this Article shall be prescribed by the Ministry.

Regulation referred to in paragraph 5 of this Article shall be marked with the appropriate classification level, in line with the law governing classified information.

## VIII. SUPERVISION

### Inspection and other supervision

### Article 131

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 34)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 44)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 64)*

Inspection and other supervision, within the competencies defined by law, shall be done by:

1) Central Bank of Montenegro in relation to obliged entities referred to in Article 4 paragraph 2 items 1, 2 and 3 of this Law, to which it issues a licence or approval for operation;

2) Agency for Electronic Communications and Postal Services in relation to obliged entities referred to in Article 4 paragraph 2 item 4 of this Law;

3) Capital Market Commission of Montenegro in relation to obliged 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) Insurance Supervision Agency in relation to obliged entities referred to in Article 4 paragraph 2 items 8 and 9 of this Law;

5) state administration authority responsible for finance in relation to obliged entities referred to in Article 4 paragraph 2 item 10 of this Law;

6) Competent tax authority responsible for the affairs for tax collection in relation to obliged 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) Ministry, through an authorised person, in relation to the obliged entities referred to in Article 4 paragraph 2 items 13 and 14 of this Law;

8) state administration authority responsible for judicial affairs in relation to obliged

entities referred to in Article 4 paragraphs 3 and 4 of this Law.

Supervisory authorities referred to in paragraph 1 of this Article shall use an approach based on the risks of money laundering and terrorist financing when planning the supervision of obliged entities.

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

- Data related to risks of money laundering or terrorist financing determined in the National Risk Assessment;

- Data related to specific national or international risks of money laundering or terrorist financing related to customers, products, services or distribution channels;

- Data related to risk from a certain obliged entities and other available data;

- Significant events or changes related to authority management of the obliged entity, as well as any change of operations.

Supervisory authorities referred to in paragraph 1 of this Article shall, no later than 14 working days prior to carrying out supervision, inform the Financial Intelligence Unit of the activities they plan to undertake and submit data on the obliged entity at which supervision is planned (registration number, TIN and name), the date on which supervision is planned, information on whether direct or indirect supervision will be carried out and, where necessary, coordinate and harmonise their activities in supervising the implementation of this Law with the Financial Intelligence Unit.

Should the supervisory authority referred to in paragraph 1 of this Article, in the procedure of the supervision over the implementation of this Law, established irregularities in the business of the obliged entity, it shall be authorised to:

- point out the identified irregularities to the obliged entity and set a time limit of eight working days for their rectification;

– Publicly disclose information on the identity of the obliged entity and the responsible person within the obliged entity, as well as the nature of the identified irregularity;

- Issue a misdemeanour order or initiate misdemeanour proceedings against the obliged entity in line with the law that regulates misdemeanour proceedings;

- Suspend or revoke the work permit or take other measures to limit or prohibit the work of the obliged entity, in line with the law;

– temporarily prohibit a responsible person from the management body from performing their function;

– in cases where the elimination of serious, systemic, or repeated irregularities is ordered, determine the amount of funds that the obliged entity must pay to the supervisory authority referred to in paragraph 1 items 1 to 4 of this Article, or to the Budget of Montenegro if the supervisory authority referred to in paragraph 1 items 5 to 8 of this Article is competent, due to a breach of the provisions of this Law;

- Order other measures to the obliged entity in line with the law.

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 its responsibility by delegating 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 closely cooperate in order to

ensure that such sanctions are effective and shall coordinate their actions in cross-border cases.

Supervisory authorities referred to in paragraph 1 of this Article may order an obliged entity to discontinue operations through its branches in another country or reject an application to open a branch in another country where the obliged entity is unable in that country to implement the measures for the prevention and detection of money laundering and terrorist financing laid down by this Law.

Supervisory authority referred to in paragraph 1 of this Article shall exchange information with other supervisory authorities and, at the request of another supervisory authority, submit the necessary data and documentation required by that authority for the purpose of carrying out supervision in line with this Law.

Financial Intelligence Unit may submit a request to the supervisory authorities referred to in paragraph 1 of this Article to carry out supervision over a particular obliged entity or type of obliged entity, on the basis of data, information and documentation available to the Financial Intelligence Unit and on the basis of strategic and operational analyses carried out.

Supervisory authorities referred to in paragraph 1 of this Article shall act upon the request referred to in paragraph 10 of this Article without delay.

Should this be necessary due to the complexity of supervision or the importance of rectifying irregularities, supervisory authorities referred to in paragraph 1 of this Article may, together with the Financial Intelligence Unit, carry out joint inspection supervision over a particular obliged entity or type of obliged entity.

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

Irregularities referred to in paragraph 5 indent 6 of this Article shall be deemed to exist where the obliged entity fails to rectify previously identified irregularities or continues to commit serious, repeated or systemic deficiencies and irregularities, or a combination thereof, in:

1) implementation of customer due diligence and monitoring measures;

2) fulfilment of the obligation to report suspicious transactions;

3) record-keeping, data protection and data retention;

4) implementation of internal control and audit mechanisms;

5) collection and retention of data on the originator and crypto-asset beneficiary;

6) implementation of effective risk-based procedures; and/or

7) ensuring compliance in the context of intermediary provision of crypto-asset services;

Obliged entities shall, at the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, submit electronically accurate and complete data on the basis of which a sectoral assessment of money laundering and terrorist financing risk is carried out, within eight days from the date of receipt of the request.

Detailed manner of submission and content of the data, as well as the manner of submitting the request referred to in paragraph 15 of this Article, shall be prescribed by the Ministry.

**Establishment of the amount of monetary funds**

**Article 131a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 35)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 45)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 65)*

Amount of monetary funds referred to in Article 131 paragraph 5 item 6 of this Law may be determined up to a maximum of twice the amount of the gain obtained through the violation of this Law, if such gain can be determined; if not, the amount shall be at least EUR 1,000,000.

Exceptionally, notwithstanding paragraph 1 of this Article, where the obliged entity is a financial-sector obliged entity, the amount of monetary funds may be determined as follows:

- for a legal person, up to a maximum of at least EUR 5,000,000 or 10% of the total annual turnover according to the most recently available audited financial statements;

- for a sole proprietor or natural person performing a business activity, up to a maximum of at least EUR 5,000,000;

-for a responsible person within a legal person, up to a maximum of at least EUR 1,000,000.

Provisions of Article 131 paragraph 5 of this Law and paragraphs 1 and 2 of this Article, shall also apply to an obliged entity that is a legal person for whose benefit any individual acted—either independently or as part of that legal person—holding the authority to represent it, make decisions on its behalf, or exercise control within that legal person.

When determining the amount of monetary funds referred to in paragraphs 1 and 2 of this Article or when imposing other measures under Article 131 paragraph 5 of this Law, the following factors shall in particular be taken into account:

1) the seriousness and duration of the violations of the provisions of this Law;

2) the degree of responsibility of the obliged entity;

3) the financial condition of the obliged entity;

4) the benefit obtained through the violation of the provisions of this Law, if it can be determined;

5) the damage caused to third parties by the violation of the provisions of this Law, if it can be determined;

6) the degree of cooperation of the obliged entity with the supervisory authority;

7) any previous violations of the provisions of this Law by the obliged entity.

Amount of funds referred to in paragraphs 1 and 2 of this Article shall not be determined if, for the same irregularity, an amount has already been imposed on the obliged entity in line with another law.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may adopt internal acts establishing guidelines for the application of the measures under Article 131 paragraph 5 of this Law, taking into account the provisions of paragraph 4 of this Article.

**Notification of Measures**

**Article 131b**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 35)*

Supervisory authority referred to in Article 131 paragraph 1 of this Law shall publish on its official website a notice on final and binding measures imposed under Article 131 paragraph 5 of this Law.

Notice referred to in paragraph 1 of this Article shall also be submitted by the supervisory authority from Article 131 paragraph 1 of this Law to the Financial Intelligence Unit, which shall publish a consolidated list of final and binding measures on its official website.

Notwithstanding paragraph 1 of this Article, where a measure is imposed on a responsible person of an obliged entity and the supervisory authority assesses that the publication of personal data would not be proportionate to the nature of the breach of the provisions of this Law or that such publication would jeopardise the stability of the financial market or ongoing criminal investigations, the supervisory authority referred to in Article 131 paragraph 1 of this Law may:

1) defer publication until the reasons for non-publication cease to exist;

2) publish the decision in anonymised form, ensuring appropriate protection of personal data;

3) refrain from publication if the options under items 1 and 2 of this paragraph are not sufficient to safeguard financial market stability and the principle of proportionality.

Data referred to in paragraph 1 of this Article must remain available on the website of the supervisory authority from Article 131 paragraph 1 of this Law for five years after publication, unless otherwise prescribed by regulations governing the protection of personal data.

## Supervision

## Article 132

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 36)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 46)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 66)*

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall carry out direct and indirect supervision over the application of this Law.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall ensure adequate financial, staffing and technical resources for carrying out supervision in line with this Law.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall, by internal acts, determine the appropriate work experience and knowledge required for supervisory officers.

Person who has been finally convicted of a criminal offence rendering that person unfit

to perform duties in line with this Law may not be a supervisory officer.

Supervisory officer shall draft a record or report on the supervision referred to in paragraph 1 of this Article.

When carrying out supervision, supervisory officer shall not disclose to the obliged entity that the supervision was initiated by the Financial Intelligence Unit and shall not disclose to the obliged entity that data and reports received from the Financial Intelligence Unit are being used in the supervision procedure.

**Direct supervision**

**Article 132a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 67)*

Direct supervision shall be carried out on the basis of the supervision plan of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, drawn up annually and constituting a business secret.

Provisions of the law governing inspection supervision, or the laws governing the competences of the supervisory authorities referred to in Article 131 paragraph 1 of this Law, shall apply accordingly to the direct supervision procedure.

When carrying out the supervision referred to in paragraph 1 of this Article, the supervisory officer shall identify themselves by official identification and a badge, or by authorisation.

Direct supervision shall be initiated at the official premises of the obliged entity and carried out by inspecting the documentation and records which the obliged entity is required to keep in line with this Law, business books, other documentation and the information system of the obliged entity.

Supervisory officer shall draw up a record at the place of supervision, which shall be signed by the supervisory officer and the obliged entity.

Should the obliged entity refuse to sign the record referred to in paragraph 5 of this Article, the supervisory officer shall record in the record the reasons for the refusal or the refusal to sign the record.

Refusal to sign the record referred to in paragraph 5 of this Article shall not prevent further action by the supervisory officer in line with the law.

Exceptionally, where, due to the scope and complexity of the inspection supervision, its nature and circumstances, it is not possible to draw up the record in line with paragraph 5 of this Article, the record shall be drawn up at the official premises of the supervisory authority referred to in Article 131 paragraph 1 of this Law, within 14 days from the date on which direct supervision was carried out.

Copy of the record shall, in the case referred to in paragraphs 5 and 8 of this Article, be handed to or served on the obliged entity.

Should the record be drawn up at the official premises of the supervisory authority referred to in Article 131 paragraph 1 of this Law, the supervisory officer shall sign the record, deliver a copy to the obliged entity and set a deadline for submitting a statement, which may not be shorter than three days from the date on which the record was served.

Should the obliged entity fail to submit a statement on the record referred to in paragraph 10 of this Article within the prescribed deadline, it shall be deemed to agree with the established facts.

**Indirect supervision**

**Article 132b**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 67)*

Indirect supervision shall be carried out by controlling the data, information and documentation which obliged entities submit to the competent supervisory authorities referred to in Article 131 paragraph 1 of this Law at their request or make available electronically, by analysing reports and data submitted by obliged entities in line with the law, or on the basis of data provided to them by the Financial Intelligence Unit.

During the supervision referred to in paragraph 1 of this Article, compliance with the obligations under this Law shall be established, in particular, in relation to: Article 12 paragraph 1 indent 1, Article 12 paragraphs 2 to 5, Article 14 paragraphs 1, 2 and 4, Article 17 paragraph 5, Article 58 paragraph 3, Article 66 paragraphs 12 and 13, Article 69 paragraphs 1 and 9, Article 76 paragraph 2, Article 78 paragraphs 1 and 3, Article 80 paragraphs 1 and 2, Article 83 paragraph 1, Article 90 paragraphs 4 and 5, Article 127 paragraph 4 and Article 131 paragraph 15 of this Law.

Obliged entity shall, at the request referred to in paragraph 1 of this Article, submit accurate and complete data, information and documentation necessary for carrying out supervision to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law immediately and at the latest within eight days from the date on which the request referred to in paragraph 1 of this Article was served.

Should, during indirect supervision, the supervisory officer establish that the obliged entity has failed to fulfil an obligation in line with this Law, the supervisory officer shall warn the obliged entity in writing to fulfil the obligation within eight working days from the date on which the warning was served.

Warning referred to in paragraph 4 of this Article shall contain a detailed description of the established facts, or a description of deficiencies, unlawful conduct and irregularities in the operations of the obliged entity.

Should the obliged entity fail to comply with paragraph 4 of this Article, or fail to submit evidence contesting the established irregularities within the deadline referred to in paragraph 4 of this Article, the supervisory officer of the non-financial sector supervisory authority referred to in Article 131 paragraph 1 of this Law shall issue a misdemeanour order to the obliged entity.

Non-financial sector supervisory authority referred to in Article 131 paragraph 1 of this Law shall notify the obliged entity where the misdemeanour order referred to in paragraph 6 of this Article is located and that it must collect it within eight days, with an instruction that the misdemeanour order becomes final and enforceable upon expiry of the eighth day from the date on which the notification was received if the obliged entity does not, within that period, submit a request for judicial decision-making.

Supervisory authority shall draw up a report on the supervision referred to in paragraph 1 of this Article and deliver it to the obliged entity.

Administrative dispute may be initiated against the report referred to in paragraph 8 of this Article.

### Special powers of supervisory authorities

### Article 133

When the supervisory authority referred to in Article 131 paragraph 1 of this Law issues work permits to the obliged entity, or approval for the acquisition of participation in the obliged entity, or for the appointment of members of the managing body of the obliged entity, on the basis of the law, it may at any time obtain information on the conviction of persons subject to the verification of fulfilment of conditions for granting the permit, or the approval and their associates, or related persons, in line with the Law.

Associate, or a related person referred to in paragraph 1 of this Article is considered an associate, or a related person, in line with the regulation governing the business of the obliged entity.

Data referred to in paragraph 1 of this Article may be used by the competent authority exclusively for the purposes they were obtained for, and shall not be communicated or made available to third parties.

**International cooperation between supervisory authorities**

**Article 134**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 37)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 47)*

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

1) regulations governing the business of the obliged entity subject to supervision by that authority, as well as other relevant regulations concerning supervision;

2) the sector in which the obliged entity subject to supervision by that authority operates;

3) supervision of the obliged entity;

4) transactions or persons in relation to which there are reasons for suspicion or grounds for suspicion of money laundering, related predicate offences or terrorist financing.

Supervisory authorities referred to in paragraph 1 of this Article, in line with the principles of reciprocity and keeping confidential information, may request mutual assistance in carrying out supervision over the obliged entity that is part of the group and that operates in the country from which assistance is requested.

Manner of delivering data, information and documentation, as well as performing joint supervision referred to in paragraph 2 of this Article, shall be regulated by the authorities referred to in paragraph 1 of this Article by a special agreement in line with the Law.

Authorities referred to in paragraph 1 of this Article may use the data, information and documentation referred to in paragraph 1 of this Article solely:

1) For performing their duties in line with this Law;

2) When filing an appeal or other legal remedies against the decision of the authority responsible for supervision, including court proceedings.

Supervisory authority referred to in paragraph 1 of this Article that has established irregularities referred to in Article 137 of this Law, shall also inform other competent supervisory authorities referred to in Article 131 paragraph 1 of this Law, if these irregularities are of importance for their work.

Supervisory authority referred to in paragraph 1 of this Article may not disclose or share with third parties any data, information, or documentation collected in line with paragraphs 1 to 4 of this Article without the explicit consent of the supervisory authority that provided such data, information, or documentation.

Supervisory authority referred to in paragraph 1 of this Article may not use the data,

information, or documentation collected in line with paragraphs 1 to 4 of this Article for any purpose other than that for which the supervisory authority that provided such data, information, or documentation has granted its consent.

Supervisory authorities referred to in Article 131 paragraph 1 items 1 to 4 of this Law shall cooperate and exchange information with the competent authorities supervising credit and financial institutions in other Member States of the European Union and third countries, in line with this Law or other laws relating to the supervision of credit and financial institutions, regardless of the nature and status of such supervisory authorities, as well as with other authorities of Member States competent for supervision in the area of prevention of money laundering and terrorist financing.

Cooperation referred to in paragraph 8 of this Article also includes the gathering of information on behalf of the competent authority that requested assistance, as well as the exchange of the information collected.

**Submission of data on actions undertaken in the supervision procedure**

**Article 135**

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall submit to the Financial Intelligence Unit, in line with this Law:

- Information about the obliged entity: identification number, TIN, name and the registered office (address, city, or municipality for the obliged entity with registered office in Montenegro, or country for obliged entity with registered office in another country), name and surname, unique identification number of the responsible person in the legal person or name and surname, date of birth and number, date of expiry and country of issuance of the travel document if the responsible person in the legal person is a foreigner;
- Data on the date of control and a description of the established condition;
- Names and surnames of persons who are engaged in the work of preventing money laundering and terrorist financing in the competent supervisory authority referred to in Article 131 paragraph 1 of this Law;
- Report or records on the control in electronic form.

When irregularities in the operations of the obliged entity are determined the supervisory authorities referred to in Article 131 paragraph 1 of this Law shall submit the following data to the Financial Intelligence Unit:

- Date of submission of the misdemeanour order or the request for initiation of misdemeanour proceedings or other imposed measures;
- Misdemeanour order number;
- Description of the offence referred to in Article 137 of this Law;
- Data on the imposed measures;
- Amount of the imposed penalty.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall submit the data referred to paragraphs 1 and 2 of this Article to the Financial Intelligence Unit within eight days from the date on which the supervision was carried out or the imposition of the measure.

Should the supervisory authority referred to in Article 131 paragraph 1 of this Law suspend or revoke a work permit or take other measures to limit or prohibit the operations of an obliged entity in line with the law, it shall notify the Financial Intelligence Unit within eight days from the date on which the measure was imposed.

Should the supervisory authorities referred to in Article 131 paragraph 1 of this Law assess during supervision that, in relation to a person, assets or transaction, there are reasons for suspicion or grounds for suspicion that property derives from criminal activity or that money laundering, related predicate offences or terrorist financing is involved, they shall notify the Financial Intelligence Unit thereof without delay.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall deliver data referred to in paragraphs 1 and 2 and notifications referred to in paragraph 4 and 5 of this Article to the Financial Intelligence Unit in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law.

### Access to Data

### Article 136

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may have immediate access to the data submitted by the obliged entity to the Financial Intelligence Unit in line with Article 66 of this Law in the content submitted to them by the obliged entity.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law shall not have direct access to the data referred to in paragraph 1 of this Article in the content in which they were processed by the Financial Intelligence Unit, however, such data may be delivered to them upon request and if the Financial Intelligence Unit assesses that the request is justified.

Supervisory authorities referred to in Article 131 paragraph 1 of this Law may have direct access to the CPR and criminal records for the purpose of carrying out activities under this Law.

Financial Intelligence Unit may, at the reasoned request of the supervisory authorities referred to in Article 131 paragraph 1 of this Law, for the purposes of carrying out checks for the issuance of licences or approvals issued by that authority in line with the law, submit all relevant data that it can obtain by applying its powers.

## X. PENAL PROVISIONS

### Article 137

(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 38)

(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 48)

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 68)*

Legal person shall be fined EUR 8,000 to EUR 80,000 for a misdemeanour if:

1) fails to establish an appropriate information system where the obliged entity is a credit institution or other financial institution (Article 11 paragraph 1 item 3);

2) fails to establish or maintain the technical conditions for using the internet application of the Financial Intelligence Unit or fails to submit the public keys of qualified certificates in line with the act referred to in Article 66 paragraph 15 of this Law (Article 11 paragraph 1 item 10a);

3) within 60 days from the date of establishment or commencement of business, fails to prepare an internal act on risk analysis identifying and assessing risks, taking into account risk factors relating to an individual customer, a group of customers, a country or geographical area, a business relationship, a transaction, a product, a service or distribution channel which may be misused for money laundering or terrorist financing,

and fails to update and retain it regularly and at least once a year in line with this Law (Article 12 paragraph 1 indent 1);

4) fails to assess the money laundering and terrorist financing risk relating to a new product, service or distribution channel provided in the course of its business, a new business practice or the manner of providing a new product, service or distribution channel before its introduction (Article 16 paragraph 1);

5) fails to take additional measures to mitigate and manage the money laundering and terrorist financing risks referred to in Article 16 paragraphs 1 and 2 of this Law on the basis of an updated risk analysis (Article 16 paragraph 3);

6) fails to verify whether a person acting on behalf of a customer has the right to represent the customer or is authorised by the customer and fails to identify that person in line with this Law (Article 17 paragraph 2);

7) prior to establishing a business relationship or carrying out an occasional transaction, fails to establish the purpose and intended nature of the business relationship or transaction or fails to obtain the information prescribed by Article 17 paragraph 4 of this Law (Article 17 paragraph 4);

8) fails to apply customer due diligence and monitoring measures where there is doubt as to the accuracy or reliability of data obtained on the identity of the customer or the beneficial owner of the customer (Article 18 paragraph 1 item 5);

9) fails to apply customer due diligence and monitoring measures where, in relation to a transaction, customer, funds or property, there are reasons for suspicion or grounds for suspicion that the property originates from criminal activity or is connected with money laundering or terrorist financing, regardless of the amount of the transaction (Article 18 paragraph 1 item 6);

10) fails to apply customer due diligence and monitoring measures to natural and legal persons trading in goods when carrying out occasional transactions in the amount of EUR 10,000 or more, regardless of whether the transaction is carried out as one transaction or several linked transactions (Article 18 paragraph 1 item 7);

11) fails to apply customer due diligence and monitoring measures when accepting stakes in the amount of EUR 20 or more in one or more linked transactions where the obliged entity is a gambling operator (Article 18 paragraph 1 item 8);

12) fails to apply customer due diligence and monitoring measures for each occasional transaction involving a transfer of crypto-assets valued at EUR 1,000 or more, regardless of whether it is one transaction or several linked transactions (Article 18 paragraph 1 item 9);

13) fails to verify the currency of existing data and obtain only the data and documentation which are missing, have changed in the meantime or have expired (Article 18 paragraph 3);

14) fails to apply the measures referred to in Article 17 paragraph 1 items 1 to 3 of this Law, including identification of the persons referred to in Articles 27 and 28 of this Law, prior to establishing a business relationship with a customer (Article 19 paragraph 1);

15) carries out a transaction referred to in Article 18 paragraph 1 items 2, 3, 4, 7, 8 and 9 of this Law without first applying the prescribed measures referred to in Article 17 paragraph 1 items 1 to 3 of this Law (Article 20);

16) fails to verify the identity of the beneficiary or beneficial owner of a life insurance policy (Article 21 paragraph 2);

17) when rights under a life insurance policy are transferred, in whole or in part, to a third party, fails to identify the new beneficiary or beneficial owner at the time of the transfer of rights (Article 21 paragraph 4);

18) fails to identify the legal representative or authorised person of the customer in line

with Article 22 paragraphs 1 to 5 of this Law and fails to obtain data on that person referred to in Article 117 paragraph 1 item 3 of this Law (Article 22 paragraph 6 indent 1);

19) fails to obtain and verify from the original written power of attorney or a certified photocopy of that power of attorney data on the customer referred to in Article 117 paragraph 1 item 3 of this Law (Article 22 paragraph 6 indents 2 and 3);

20) where it has doubts as to the accuracy of data obtained or the authenticity of documents or other documentation, fails to carry out additional checks from independent, credible and reliable sources and fails to obtain a written statement on the accuracy of the data obtained during identification of the customer, their legal representative or authorised person (Article 22 paragraph 7);

21) establishes a business relationship or carries out a transaction after establishing that the data in the identity document differ from the data in the CPR (Article 22 paragraph 9);

22) verifies the data on the customer referred to in Article 22 paragraph 1 of this Law, their legal representative or authorised person through the Financial Intelligence Unit by accessing the CPR without having the original identity document of the customer, legal representative or authorised person available at the time of verification (Article 22 paragraph 12);

23) identifies a customer contrary to Article 23 of this Law;

24) carries out video-electronic identification contrary to Article 24 of this Law;

25) fails to identify a customer who is a legal person or business organisation in line with Articles 19 and 20 of this Law (Article 26 paragraph 1);

26) acts contrary to Article 26 paragraph 7 of this Law;

27) fails to obtain data on all directors of a legal person or business organisation referred to in Article 117 paragraph 1 item 3 of this Law (Article 27 paragraph 2);

28) in the procedure for establishing and verifying the power of attorney for representation of a representative and all directors referred to in Article 27 paragraph 2 of this Law, fails to obtain the power of attorney and retain it in its documentation (Article 27 paragraph 3);

29) in the procedure for identifying an authorised person of a legal person or business organisation, fails to obtain data on the representative and all directors on whose behalf the authorised person acts in line with Article 28 paragraph 2 of this Law;

30) fails to obtain powers of attorney for representation of the persons referred to in Article 28 paragraph 1 of this Law and retain them in its documentation (Article 28 paragraph 3);

31) fails to identify the trustee or obtain data on the trustee (Article 29 paragraph 1 items 1 and 2);

32) fails to identify the representative or authorised person of the trustee in line with Articles 27 and 28 of this Law (Article 29 paragraph 1 item 3);

33) fails to obtain data on settlors, trust protectors, beneficiaries or classes of beneficiaries, including named beneficiaries, discretionary beneficiaries, future beneficiaries who are already designated or ascertainable and other natural persons exercising ultimate direct or indirect control over the trust, in line with Article 117 of this Law (Article 29 paragraph 1 item 4);

34) fails to carry out additional checks from independent, credible and reliable sources or fails to obtain from the trustee, where the trustee is a natural person, or from the representative or authorised person of the trustee, a written statement on the accuracy of that data (Article 29 paragraph 3);

35) the trustee fails to keep accurate and up-to-date records containing the data

prescribed by Article 117 paragraphs 1 and 3 of this Law concerning settlors, trust protectors, beneficiaries or classes of beneficiaries, including named beneficiaries, discretionary beneficiaries, future beneficiaries who are already designated or ascertainable and other natural persons exercising ultimate direct or indirect control over the trust, as well as, where applicable, data on representatives, authorised persons, investment advisers or managers, accountants and tax advisers (Article 29 paragraph 5);

36) the trustee fails to retain the records referred to in Article 29 paragraph 5 of this Law for five years after the end of their engagement in the trust (Article 29 paragraph 6);

37) the trustee fails to ensure that the data referred to in Article 29 paragraph 5 of this Law are accurate (Article 29 paragraph 7);

38) the trustee fails to enable direct electronic access to the data referred to in paragraph 5 of this Article to the Financial Intelligence Unit and the state administration authority responsible for tax collection where, on behalf of a trust, another person or a foreign-law entity equivalent to it, they enter into any form of business relationship or acquire immovable property in Montenegro (Article 29 paragraph 8);

39) fails to identify a customer in line with this Law when the customer enters premises where special games of chance are organised in a casino (Article 30 paragraph 1 item 1);

40) fails to identify a customer in line with this Law each time the lessee of a safe-deposit box or their representative or authorised person accesses the safe-deposit box (Article 30 paragraph 1 item 2);

41) in the procedure for identifying a customer referred to in Article 30 paragraph 1 item 1 of this Law, fails to obtain a photocopy of that person's identity document in line with Article 22 paragraph 3 of this Law and a written statement by which the customer declares under civil and criminal liability that they participate in games of chance in the casino for their own account and in their own name (Article 30 paragraph 2);

42) prior to entrusting implementation of the measures referred to in Article 31 paragraph 1 of this Law to a third party, fails to establish that the operations of that party are subject to regular supervision concerning compliance with anti-money laundering and counter-terrorist financing requirements in the manner established by this Law or the relevant regulations of another country, that it has mechanisms in place to fulfil the obligation to apply customer due diligence and monitoring measures at least equivalent to or more stringent than those prescribed by this Law and that it keeps records of the measures undertaken in the manner prescribed by this Law (Article 31 paragraph 3);

43) entrusts implementation of customer due diligence and monitoring measures to a third party which is a shell bank or anonymous company or is from a high-risk third country (Article 32);

44) the third party fails to implement customer due diligence and monitoring measures properly (Article 31 paragraph 5);

45) having assessed that there is doubt as to the reliability of customer due diligence and monitoring measures implemented by a third party or the accuracy of data and documentation obtained on the customer, fails to implement those measures directly (Article 34 paragraph 1);

46) fails to collect data on the payer and payee and enter it in the payment order form or electronic message accompanying the transfer of funds from the payer to the payee (Article 35 paragraph 1);

47) fails to verify the accuracy of data collected on the payer in line with Articles 22, 23, 24, 26, 27 and 28 of this Law before the transfer of funds (Article 35 paragraph 7);

48) fails to verify whether the data on the payer and payee have been entered in the payment order form or electronic message accompanying the transfer of funds in line with

Article 35 of this Law (Article 36 paragraph 1);

49) fails to refuse future transfers of funds or limit or terminate business cooperation with the payment service provider of the payer where that provider repeatedly fails to submit accurate and complete data in line with Article 35 of this Law (Article 37 paragraph 4);

50) fails to notify the Central Bank of Montenegro of the payment service provider of the payer which repeatedly fails to submit accurate and complete data in line with Article 35 of this Law and of the measures taken against that provider in line with Article 37 paragraphs 3 and 4 of this Law (Article 37 paragraph 5);

51) fails to establish whether the absence of accurate and complete data referred to in Article 35 of this Law constitutes grounds for suspicion of money laundering or terrorist financing and, where it establishes that the deficiency constitutes grounds for suspicion, fails to notify the Financial Intelligence Unit in line with Article 66 paragraphs 6, 8 and 10 of this Law (Article 37 paragraph 6);

52) fails to act in line with Article 37 paragraphs 2 to 7 of this Law where the payment order form or 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);

53) fails to provide data on the originator and beneficiary of crypto-assets when transferring crypto-assets (Article 40f paragraph 1);

54) where a transfer of crypto-assets is not recorded on a network using distributed ledger technology (DLT) or similar technology and is not made to or from a crypto-asset account of the originator, fails to ensure that a unique transaction identifier is attached to the transfer of crypto-assets (Article 40f paragraph 4);

55) fails to submit the data referred to in Article 40f paragraphs 2 and 3 of this Law to another crypto-asset service provider of the originator prior to, simultaneously with or in parallel with the execution of the crypto-asset transaction and in a manner ensuring the protection of those data in line with the law governing personal data protection (Article 40f paragraph 6);

56) fails to obtain and retain the data referred to in Article 40f paragraphs 2 and 3 of this Law and fails to ensure that a transfer of crypto-assets can be individually identified where crypto-assets are transferred to a self-hosted address (Article 40f paragraph 7);

57) prior to transferring crypto-assets, fails to verify the accuracy of data on the originator and beneficiary of the crypto-assets referred to in Article 40f paragraphs 2 and 3 of this Law on the basis of documents, data or information from a reliable and independent source (Article 40f paragraph 9);

58) allows the initiation or carries out a transfer of crypto-assets without the conditions prescribed by Article 40f paragraphs 1 to 10 of this Law being fulfilled (Article 40f paragraph 11);

59) fails to implement effective procedures, including, where appropriate, monitoring during or after the transfer of crypto-assets, to establish whether the data on the originator and beneficiary of crypto-assets referred to in Article 40f paragraphs 2, 3 and 4 of this Law are included in the transfer or in batch files for transfers, or are subsequently submitted (Article 40h paragraph 1);

60) fails to obtain and retain the data referred to in Article 40f paragraphs 2, 3 and 4 of this Law and fails to ensure that a transfer of crypto-assets can be individually identified where crypto-assets are transferred from a self-hosted address (Article 40h paragraph 2);

61) in addition to the measures referred to in Article 53c of this Law, fails to take appropriate measures to assess whether a self-hosted address is owned or controlled by the beneficiary of the crypto-assets where a transfer exceeding EUR 1,000 is made from

a self-hosted address (Article 40h paragraph 3);

62) fails to verify the accuracy of data on the beneficiary of crypto-assets referred to in Article 40f paragraph 3 of this Law on the basis of documents, data or information from a reliable and independent source before making the crypto-assets available to the beneficiary (Article 40h paragraph 4);

63) fails to implement effective risk-based procedures, including the measures referred to in Article 17 of this Law, to establish whether to execute, refuse, return or suspend a transfer of crypto-assets for which the required or complete data on the originator and beneficiary of crypto-assets are missing and fails to take appropriate further measures (Article 40i paragraph 1);

64) fails to refuse a transfer, return the transferred crypto-assets to the originator's account or request the required data on the originator and beneficiary before the crypto-assets become available to the beneficiary where it establishes that the data referred to in Article 40f paragraphs 2, 3 and 4 or Article 40g of this Law are missing or incomplete (Article 40i paragraph 2);

65) fails to act in line with Article 40i paragraph 3 items 1 and 2 of this Law where the crypto-asset service provider of the originator repeatedly fails to submit the required data on the originator or beneficiary of crypto-assets;

66) fails to notify the competent supervisory authority of a crypto-asset service provider of the originator which repeatedly fails to submit accurate and complete data in line with Article 40i of this Law and of the measures taken against that service provider in line with Article 40i paragraphs 1, 2 and 3 of this Law (Article 40i paragraph 4);

67) fails to establish whether the absence of accurate and complete data referred to in Article 40i of this Law constitutes grounds for suspicion of money laundering or terrorist financing and, where it establishes that the deficiency constitutes grounds for suspicion, fails to notify the Financial Intelligence Unit in line with this Law (Article 40j);

68) fails to ensure that all data received on the originator and beneficiary of crypto-assets which must accompany the transfer of crypto-assets are delivered with the transfer (Article 40k paragraph 1);

69) fails to keep and retain records of the data referred to in Article 40k paragraph 1 of this Law and, at their request, fails to allow the competent authorities to inspect those records (Article 40k paragraph 2);

70) fails to implement effective procedures, including, where appropriate, monitoring after or during a transfer of crypto-assets, to establish whether the data on the originator or 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 were submitted prior to, simultaneously with or in parallel with the transfer of crypto-assets or the transfer of crypto-assets through batch files, including where the transfer is carried out from or to a self-hosted address (Article 40l paragraph 1);

71) fails to establish effective risk-based procedures, including the measures referred to in Article 17 of this Law, to determine whether to execute, refuse, return or suspend a transfer of crypto-assets for which the required and complete data on the originator and beneficiary of crypto-assets are missing and fails to take appropriate measures (Article 40m paragraph 1);

72) fails, on the basis of a risk assessment and without undue delay, to act in line with Article 40m paragraph 2 items 1 and 2 of this Law where, on receiving a transfer of crypto-assets, it establishes that the data referred to in Article 40f paragraph 2 items 1, 3 and 4 and paragraph 3 items 1, 2 and 3 or Article 40g paragraph 1 of this Law are missing or incomplete;

73) fails to act in line with Article 40m paragraph 3 items 1 and 2 of this Law where a

crypto-asset service provider repeatedly fails to submit the required data on the originator or beneficiary of crypto-assets;

74) fails to notify the competent supervisory authority of a crypto-asset service provider which repeatedly fails to submit accurate and complete data and of the measures taken in line with Article 40m paragraphs 1, 2 and 3 of this Law (Article 40m paragraph 4);

75) fails to establish whether the absence of accurate and complete data referred to in Article 40m of this Law during a transfer of crypto-assets or a related transaction constitutes grounds for suspicion of money laundering or terrorist financing and, where it establishes that the deficiency constitutes grounds for suspicion, fails to notify the Financial Intelligence Unit in line with this Law (Article 40n);

76) fails to submit, fully and without delay, including through the single point of contact referred to in Article 62 paragraph 8 of this Law, data collected in line with this Law at the request of competent authorities and competent supervisory authorities (Article 40p paragraph 1);

77) fails to establish the beneficial owner of a legal person, business organisation, trust, other person or foreign-law entity equivalent to it by obtaining the data referred to in Article 44 of this Law (Article 42 paragraph 1);

78) in the procedure for establishing the beneficial owner, fails to obtain documentation on the basis of which the ownership structure and controlling member of the customer and the data on the beneficial owner can be established (Article 42 paragraph 6);

79) fails to obtain a photocopy of the beneficial owner's identity document in line with Article 22 paragraph 3 of this Law (Article 42 paragraph 8);

80) fails to obtain a written statement on the accuracy of the data from the representative or authorised person of the customer where, when collecting data referred to in Article 42 paragraphs 2, 3, 5, 6 and 7 of this Law, it has doubts as to the accuracy of the data obtained or the authenticity of the documents and other documentation from which the data were obtained (Article 42 paragraph 9);

81) fails to keep records of the measures undertaken to establish the beneficial owner referred to in Article 42 paragraph 1 of this Law (Article 42 paragraph 11);

82) fails to enter the prescribed data on beneficial owners and changes to beneficial owners in the Register of Beneficial Owners within eight days from the date of entry in the CRPS or the register of taxpayers or within eight days from the date of a change in data on the beneficial owner (Article 43 paragraph 3);

83) fails to verify and confirm the accuracy of its data in the Register of Beneficial Owners once a year and no later than 31 March of the current year (Article 43 paragraph 5);

84) fails to designate at least one natural person employed by the obliged entity who has a permanent or temporary residence in Montenegro or a business organisation which is an obliged entity under Article 4 paragraph 2 item 13 indent 2 and paragraph 3 of this Law and is registered in Montenegro (Article 43 paragraph 9);

85) where a trustee fails to submit to 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, at their request, without delay and no later than three days from receipt of the request, all information on the trust, its beneficial ownership and the trust assets which it holds or manages (Article 43 paragraph 10);

86) fails to enter a trust in the Register of Trusts within five days from the date on which it entered into a business relationship with the trustee (Article 43a paragraph 5);

87) the trustee fails to enter the trust in the Register of Beneficial Owners within 25 days from the date of conclusion of the business relationship or acquisition of immovable property (Article 43a paragraph 7);

88) fails to submit to the state administration authority responsible for tax collection documentation on the basis of which the ownership structure and controlling member of the customer can be established and fails to collect data on the beneficial owner (Article 48 paragraph 3);

89) fails to comply with the order referred to in Article 48 paragraph 4 of this Law within three days from receipt of that order (Article 48 paragraph 5);

90) fails to apply measures for monitoring the business relationship of the customer, including control of transactions and monitoring the source of funds used by the customer in conducting business (Article 49 paragraph 1);

91) fails to apply the measures referred to in Article 49 paragraph 2 of this Law;

92) fails to ensure and adapt the scope and frequency of applying the measures referred to in Article 49 paragraph 1 of this Law to the money laundering and terrorist financing risk to which the obliged entity is exposed when carrying out an individual transaction or conducting business with a customer (Article 49 paragraph 3);

93) verifies data in the CPR for a natural person who is not its customer (Article 49 paragraph 5);

94) fails to ensure that the frequency of monitoring a higher-risk customer's business relationship is not longer than one year and that of a lower-risk customer is not longer than five years (Article 49 paragraph 7);

95) fails to check a customer at least once a year and no later than one year after the previous check where the customer is a foreign legal person or a legal person with its registered office in Montenegro in which foreign capital participation is at least 25% and which carries out transactions referred to in Article 18 paragraph 1 items 2, 3, 4, 6, 7 and/or 9 of this Law with the obliged entity (Article 50 paragraph 1);

96) fails to contact the customer to verify all relevant information when it establishes a discrepancy in the data (Article 50 paragraph 6);

97) fails to apply enhanced customer due diligence and monitoring measures where a higher money laundering and terrorist financing risk has been established in the risk-analysis guidelines referred to in Article 12 paragraph 5 of this Law (Article 52 paragraph 1 item 7);

98) fails to apply enhanced customer due diligence and monitoring measures where a higher money laundering and terrorist financing risk has been established in line with the National Risk Assessment (Article 52 paragraph 1 item 8);

99) fails to apply enhanced customer due diligence and monitoring measures in other cases where it assesses that a higher money laundering and terrorist financing risk exists or may exist in relation to a customer, group of customers, country or geographical area, business relationship, transaction, product, service or distribution channel (Article 52 paragraph 2);

100) when establishing a correspondent relationship involving payment execution with a credit institution or other financial institution having its registered office outside Montenegro and acting as respondent, fails, in addition to the measures referred to in Article 17 of this Law, to take the additional measures referred to in Article 53 paragraph 1 items 1 to 9 of this Law;

101) prior to establishing a correspondent relationship with a respondent, fails to obtain the written consent of a senior manager to establish that business relationship (Article 53 paragraph 2);

102) fails to regulate its responsibility and the responsibility of the respondent by contract when concluding a correspondent relationship (Article 53 paragraph 3);

103) fails to review and amend or, where necessary, terminate a correspondent relationship with a credit institution or other financial institution acting as respondent in a

high-risk third country (Article 53 paragraph 6);

104) establishes or continues a correspondent relationship with a credit institution or other financial institution having its registered office outside Montenegro without first taking the measures or any of the measures referred to in Article 53 paragraphs 1 to 4 of this Law (Article 53 paragraph 7 item 1);

105) establishes or continues a correspondent relationship with a credit institution or other financial institution having its registered office outside Montenegro where that credit institution or financial institution has not established anti-money laundering and terrorist financing controls or does not apply laws and other regulations on preventing and detecting money laundering and terrorist financing (Article 53 paragraph 7 item 2);

106) establishes or continues a correspondent relationship with a credit institution or other financial institution having its registered office outside Montenegro where that credit institution or financial institution operates as a shell bank or establishes or maintains correspondent or other business relationships and carries out transactions with shell banks (Article 53 paragraph 7 item 3);

107) fails to establish and assess the money laundering and terrorist financing risk associated with transfers of crypto-assets directed to or originating from a self-hosted address and fails to establish internal policies, procedures and controls for those purposes (Article 53b paragraph 1);

108) fails to apply any of the risk-mitigation measures corresponding to the risks established (Article 53b paragraphs 2 and 3);

109) fails to establish whether a respondent is licensed or registered (Article 53c paragraph 1 item 1);

110) fails to collect sufficient information on the respondent to fully understand the nature of its business and fails to assess the respondent's reputation and the quality of supervision of its business on the basis of publicly available information (Article 53c paragraph 1 item 2);

111) fails to assess the respondent's controls relating to preventing money laundering and terrorist financing (Article 53c paragraph 1 item 3);

112) fails to obtain the written consent of a senior manager before establishing a new correspondent relationship (Article 53c paragraph 1 item 4);

113) fails to document the responsibilities of each party to the correspondent relationship (Article 53c paragraph 1 item 5);

114) in relation to crypto-asset payable-through accounts, fails to ensure that the respondent has verified the identity and applied enhanced customer due diligence and monitoring measures to customers with direct access to the correspondent's accounts and that it can provide relevant data on those measures to the correspondent on request (Article 53c paragraph 1 item 6);

115) fails to document the decision to terminate a correspondent relationship for reasons related to the anti-money laundering and counter-terrorist financing policy (Article 53c paragraph 2);

116) fails regularly to update information on the application of enhanced customer due diligence and monitoring measures in relation to a correspondent relationship or when new risks relating to the respondent arise (Article 53c paragraph 3);

117) prior to establishing a business relationship with a customer, fails to check in the Register referred to in Article 55 of this Law whether the customer, their legal representative, authorised person or beneficial owner is a politically exposed person (Article 54 paragraph 1);

118) when applying enhanced customer due diligence and monitoring measures to a customer or beneficial owner who is a politically exposed person, fails, in addition to the

measures referred to in Article 17 of this Law, to take appropriate measures and establish the source of wealth and funds involved in the business relationship or transaction with that customer (Article 56 paragraph 1 item 1);

119) when applying enhanced customer due diligence and monitoring measures to a customer or beneficial owner who is a politically exposed person, fails, in addition to the measures referred to in Article 17 of this Law, to establish whether the customer who is a politically exposed person is the beneficial owner of a legal person, business organisation, trust, other person or foreign-law entity equivalent to it or a natural person with its registered office in another country on whose behalf a business relationship is established, a transaction is carried out or another activity of the customer is performed (Article 56 paragraph 1 item 3);

120) when applying enhanced customer due diligence and monitoring measures to a customer or beneficial owner who is a politically exposed person, fails, after establishing the business relationship, to pay special attention to monitoring transactions and other business activities carried out by the politically exposed person or by the customer whose beneficial owner is a politically exposed person (Article 56 paragraph 1 item 4);

121) when providing custody services to a customer, fails, in addition to the measures referred to in Article 17 of this Law, to take appropriate measures and establish the source of wealth and funds involved in the business relationship or transaction with that customer (Article 57 paragraph 1 item 1);

122) when providing custody services to a customer, fails, in addition to the measures referred to in Article 17 of this Law, to obtain the written consent of a senior manager before establishing the business relationship or, where it has already been established, to continue it (Article 57 paragraph 1 item 2);

123) when providing custody services to a customer, fails, in addition to the measures referred to in Article 17 of this Law, to establish whether the customer concludes a contract on the provision of custody services in their own name and on their own account or whether it is a sub-custody arrangement (Article 57 paragraph 1 item 3);

124) when providing custody services to a customer, fails, in addition to the measures referred to in Article 17 of this Law, to establish, for each transaction, on whose account the sub-custodian carried out the transaction (Article 57 paragraph 1 item 4);

125) where it is unable to apply the measures referred to in Article 57 paragraph 1 of this Law, establishes a business relationship or fails to terminate an existing relationship (Article 57 paragraph 2);

126) in the case of complex and unusually large transactions, transactions carried out in an unusual manner, transactions without an obvious economic justification or legal purpose or transactions deviating from the usual or expected business of the customer, for which it was not possible to assess whether they were suspicious transactions, fails, in addition to the measures referred to in Article 17 of this Law, to take the measures referred to in Article 58 paragraph 1 of this Law;

127) when establishing a business relationship or carrying out transactions with a person from a high-risk third country or where a high-risk third country is involved in a transaction, fails, in addition to the measures referred to in Article 17 of this Law, to take the additional measures referred to in Article 58 paragraph 1 of this Law (Article 59 paragraph 1 item 1);

128) after establishing a business relationship with a customer from a high-risk third country, fails to apply enhanced monitoring of that business relationship and the transactions carried out by that customer (Article 59 paragraph 2);

129) fails regularly to monitor and verify whether the conditions for applying simplified measures continue to exist (Article 61 paragraph 2);

130) opens or maintains for a customer an anonymous account, anonymous crypto-asset account, anonymous safe-deposit box, savings book or securities account under a code, in the name of the bearer or otherwise, or provides another service or product which directly or indirectly enables concealment of the customer's identity (Article 63);

131) operates as a shell bank (Article 64 paragraph 1);

132) establishes or maintains a correspondent relationship with a credit institution which operates or may operate as a shell bank or with another credit institution known to allow shell banks to use its accounts (Article 64 paragraph 2);

133) receives a payment or makes a cash payment or pays out winnings in the amount of EUR 10,000 or more, or where the payment is made in two or more linked transactions in a total amount of EUR 10,000 or more (Article 65 paragraphs 1 and 2);

134) fails to implement the restriction on the use of cash referred to in Article 66 of this Law (Article 65 paragraph 6);

135) fails to submit to the Financial Intelligence Unit, without delay and no later than three working days from the date of execution of the transaction or the date on which it becomes aware that the transaction was executed, accurate and complete data on the customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law for each non-cash transaction in the amount of EUR 100,000 or more, each cash transaction carried out as an occasional transaction in the amount of EUR 3,000 or more but less than EUR 10,000 where the obliged entity is referred to in Article 4 paragraph 2 items 12 and 13 indents 3, 4 and 8 of this Law, each cash transaction in the amount of EUR 15,000 or more where the obliged entity is a credit institution or other payment service provider, or each transaction in the amount of EUR 2,000 or more where the obliged entity is referred to in Article 4 paragraph 2 item 10 of this Law (Article 66 paragraph 1);

136) fails to submit to the Financial Intelligence Unit, without delay and no later than three working days from the date of execution of the transaction, accurate and complete data on the customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law for each non-cash transaction in the amount of EUR 20,000 or more (Article 66 paragraph 2);

137) fails to submit to the Financial Intelligence Unit, without delay and no later than three days from the date of execution of the transaction or the date on which it becomes aware that the transaction was executed, accurate and complete data on the customer due diligence and monitoring 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 carried out to accounts of legal or natural persons in high-risk third countries or involving high-risk third countries (Article 66 paragraph 3);

138) fails to refrain from executing a suspicious transaction, regardless of its amount, until the order referred to in Article 93 of this Law is issued and fails, without delay, to notify the Financial Intelligence Unit and submit to it data on the customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law (Article 66 paragraph 6);

139) fails to submit to the Financial Intelligence Unit the data referred to in Article 66 paragraph 6 of this Law before execution of the transaction and fails to specify the deadline within which the transaction is to be executed (Article 66 paragraph 7);

140) where, due to the nature of the transactions or other justified reasons, it cannot act in line with Article 66 paragraph 6 of this Law, fails to submit data on the customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law without delay and no later than the next working day from the date of execution of the transaction or the date on which it becomes aware that the transaction was executed (Article 66 paragraph 8);

141) when submitting data in the manner referred to in Article 66 paragraph 8 of this Law, fails to provide an explanation containing the reasons why it did not act in line with Article 66 paragraph 6 of this Law (Article 66 paragraph 9);

142) fails, without delay, to submit to the Financial Intelligence Unit accurate and complete data on the customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 and paragraph 8 of this Law in all cases of suspicious business or in relation to funds or other property which it knows or has reasons for suspicion constitute proceeds of crime or are connected with money laundering or terrorist financing (Article 66 paragraph 10);

143) fails, without delay, to notify the Financial Intelligence Unit that a customer has sought advice relating to money laundering or terrorist financing (Article 66 paragraph 11);

144) fails to notify the Financial Intelligence Unit, no later than three working days from the date of inspection, of every inspection of data, information and documentation carried out by a supervisory authority referred to in Article 131 paragraph 1 of this Law (Article 66 paragraph 12);

145) fails to submit to the Financial Intelligence Unit data, an explanation and notifications in the manner prescribed by Article 66 paragraph 13 of this Law;

146) fails to provide the compliance officer for the prevention of money laundering and terrorist financing with the prescribed conditions (Article 77 paragraph 1);

147) fails to submit to the Financial Intelligence Unit, at its request, without delay and no later than five days from receipt of the request, accurate and complete data, information and documentation at its disposal (Article 90 paragraph 4);

148) fails to submit data, information and documentation requested with the designation ‘URGENT’ without delay and no later than 24 hours from receipt of the request (Article 90 paragraph 5);

149) fails to submit the data, information and documentation referred to in Article 90 paragraph 1 of this Law to the Financial Intelligence Unit in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law (Article 90 paragraph 7);

150) fails, without delay, to take the measures referred to in Article 93 paragraphs 1 and 4 of this Law (Article 93 paragraph 5);

151) fails to comply with the request referred to in Article 95 paragraph 1 of this Law (Article 95 paragraph 1);

152) informs the customer or compromises information that the Financial Intelligence Unit has requested continuous monitoring of the customer’s financial operations (Article 95 paragraph 2);

153) fails to submit data to the Financial Intelligence Unit before execution of a transaction or conclusion of a business for transactions exceeding EUR 1,000 for a natural person or EUR 3,000 for a legal person (Article 95 paragraph 3);

154) where, due to the nature of the transaction or business or other justified reasons, it cannot act in line with Article 95 paragraph 3 of this Law, fails to submit the data without delay and no later than the next working day from the date of execution of the transaction or conclusion of the business and fails to explain in detail the reasons why it did not act in line with Article 95 paragraph 3 of this Law (Article 95 paragraphs 4 and 5);

155) fails, without delay, to notify the Financial Intelligence Unit where, in carrying out activities, it discovers facts indicating a possible connection with money laundering and related predicate offences or terrorist financing (Article 114 paragraph 1);

156) fails, at the request of the Financial Intelligence Unit, to submit data, information or documentation indicating a possible connection with money laundering and related predicate offences or terrorist financing, in line with the Law (Article 114 paragraph 2);

157) fails to keep the records referred to in Article 116 paragraph 1 of this Law;

158) fails to keep the records referred to in Article 116 paragraph 1 of this Law in a manner ensuring the reconstruction of individual transactions, including amounts and currency, which could be used in proceedings for detecting the criminal activities of customers (Article 116 paragraph 2);

159) the records kept in line with the Law do not contain the data prescribed by Article 117 of this Law;

160) discloses to a customer or third party the data referred to in Article 123 paragraph 1 items 1 to 4 of this Law (Article 123 paragraph 1);

161) fails to take the necessary measures to protect the compliance officer for the prevention of money laundering and terrorist financing and other employees implementing the provisions of this Law from threats and other unfavourable or discriminatory acts directed at their physical or psychological integrity (Article 125 paragraph 1);

162) fails to take the necessary measures to ensure that decisions of the compliance officer for the prevention of money laundering and terrorist financing or the deputy compliance officer are not compromised by the commercial interests of the obliged entity and that those interests do not unjustifiably influence the compliance officer or deputy compliance officer (Article 125 paragraph 2);

163) fails to establish appropriate procedures, following the prior opinion of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, regulating the manner in which employees report breaches of the provisions of this Law through a dedicated and anonymous channel, in line with the nature and size of the obliged entity (Article 125 paragraph 3);

164) uses personal data obtained in line with this Law for a purpose for which those data are not processed or processes them for commercial purposes (Article 126 paragraph 1);

165) fails to retain data, information and documentation obtained in line with this Law, data on the identification number of each customer account, data and documentation on electronic transfers of money, documentation on business correspondence and reports for five years after termination of the customer's business relationship, execution of an occasional transaction, refusal to establish a business relationship, refusal to execute an occasional transaction, entry of the customer into a casino or premises where other games of chance are organised or access to a safe-deposit box, unless a longer retention period is prescribed by a special law or retention is extended at the request of the Financial Intelligence Unit, the competent authority referred to in Article 96 paragraph 1 of this Law or the supervisory authority referred to in Article 131 paragraph 1 of this Law (Article 127 paragraphs 1, 2 and 3);

166) fails to retain 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 field of preventing and detecting money laundering and terrorist financing and implementation of internal control and audit measures for four years from expiry of the licence or completion of professional training and development or internal control and audit (Article 127 paragraph 4);

167) fails, where it ceases to exist, to submit the data, information and documentation referred to in Article 127 paragraphs 1 and 2 of this Law to the supervisory authority referred to in Article 131 paragraph 1 of this Law, which is required to retain them for five years from the date of receipt (Article 127 paragraph 5);

168) fails to submit, no later than eight days from the date of service of the request, accurate and complete data, information and documentation necessary for carrying out

supervision at the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law (Article 132b paragraph 3).

Exceptionally, for the misdemeanour referred to in paragraph 1 of this Article, an obliged entity referred to in Article 4 paragraph 2 items 1, 2 and 3 of this Law shall be fined EUR 10,000 to EUR 80,000.

For the misdemeanour referred to in paragraph 1 of this Article, a member of the management body or other responsible person in a legal person, a natural person, a natural person carrying out a business activity and a notary shall be fined EUR 1,000 to EUR 8,000.

Exceptionally, for the misdemeanour referred to in paragraph 1 of this Article, a member of a collegiate management body responsible for implementing this Law shall, where a fine is imposed on the obliged entity under Article 131a paragraph 2 of this Law, be fined an amount equal to six gross monthly salaries or remuneration up to 12 gross monthly salaries or remuneration received by that person in the month preceding the month in which the fine referred to in Article 131a paragraph 2 of this Law was imposed.

For the misdemeanour referred to in paragraph 1 of this Article, a sole proprietor shall be fined EUR 1,000 to EUR 20,000.

For the misdemeanour referred to in paragraph 1 of this Article, a legal person, a sole proprietor, a responsible person in a legal person and a natural person may be prohibited from performing their profession, activity or duty for a period of up to six months.

For the misdemeanours referred to in paragraph 1 items 2 and 157 of this Article, the request for initiation of misdemeanour proceedings shall also be submitted by an authorised police officer of the Financial Intelligence Unit.

Misdemeanour proceedings for misdemeanours referred to in paragraph 1 of this Article committed by credit institutions and other financial institutions may not be initiated after four years have elapsed from the date on which the misdemeanour was committed.

**Article 137a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 69)*

Legal person shall be fined EUR 5,000 to EUR 40,000 for a misdemeanour if:

1) has a collegiate management body but fails to appoint one member of that body responsible for implementing this Law (Article 11 paragraph 2);

2) fails to include in the risk analysis an assessment of the measures, actions and procedures undertaken by the obliged entity to prevent and detect money laundering or terrorist financing (Article 12 paragraph 2);

3) fails to include in the risk analysis at least an analysis of the money laundering and terrorist financing risks relating to the overall operations of the obliged entity and an analysis of those risks for each group or type of customer, business relationship, service provided by the obliged entity in the course of its business or transaction (Article 12 paragraph 3);

4) fails to prepare the risk analysis in written and electronic form and/or fails to make it proportionate to the size of the obliged entity and the nature and scope of its business (Article 12 paragraph 4);

5) fails to prepare the risk analysis on the basis of the guidelines for risk analysis established by the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, in line with the regulation referred to in Article 15 of this Law and the National Risk Assessment (Article 12 paragraph 5);

6) fails to submit the risk analysis within three days from the date of receipt of a request from the competent authority referred to in Article 131 paragraph 1 of this Law (Article 12 paragraph 8);

7) fails to establish a system for managing the risk of money laundering and terrorist financing in line with Article 14 paragraph 1 of this Law;

8) fails to make the policies, controls and procedures referred to in Article 14 paragraph 1 item 2 of this Law proportionate to the scope and nature of the obliged entity's business, the size and type of customer with whom it does business and the type of product or service it provides (Article 14 paragraph 2);

9) fails to establish internal policies, controls and procedures in line with Article 14 paragraph 4 of this Law;

10) fails to regulate by internal acts the procedures for implementing the measures referred to in Article 17 paragraphs 1 and 2 of this Law (Article 17 paragraph 5);

11) at the request of the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, fails to submit, or submits inadequate, analyses, documents and other information demonstrating that the measures have been implemented in line with the identified money laundering and terrorist financing risk (Article 17 paragraph 6);

12) fails to notify the Financial Intelligence Unit that it cannot implement one or more measures referred to in Article 17 paragraph 1 of this Law (Article 17 paragraph 7);

13) fails to obtain the data referred to in Article 17 paragraphs 1 and 2 of this Law (Article 18 paragraph 5);

14) establishes a business relationship with a customer or, where the business relationship has been established, fails to terminate it if it cannot implement the measures referred to in Article 19 paragraph 1 of this Law (Article 19 paragraph 2);

15) establishes a business relationship with a customer or, where the business relationship has been established, fails to terminate it if it assesses that it cannot effectively manage the money laundering and terrorist financing risk relating to that customer (Article 19 paragraph 4);

16) fails to adopt an internal act regulating procedures for refusing to establish a business relationship or terminating an existing business relationship referred to in Article 19 paragraphs 3 and 4 of this Law (Article 19 paragraph 6);

17) in the customer identification procedure referred to in Article 22 paragraph 1 of this Law, fails to obtain a photocopy of the identity document, record the date, time and name and surname of the person who inspected the photocopy, and retain that photocopy and the collected data in line with this Law (Article 22 paragraph 3);

18) after identification has been carried out, fails to enter in the records referred to in Article 117 paragraph 1 of this Law the data on the manner in which the customer was identified (Article 22 paragraph 10, Article 23 paragraph 9 and Article 24 paragraph 18);

19) within eight days from the date of service of the decision referred to in Article 25 paragraph 6 of this Law, fails to regulate by internal acts the detailed manner of carrying out video-electronic identification (Article 24 paragraph 19);

20) fails to retain the video recording made during the verification procedure referred to in Article 24a paragraph 1 of this Law in line with this Law (Article 24a paragraph 5);

21) fails to prepare an analysis of the risks of the system and solution used for electronic and video-electronic identification within eight days from the date of obtaining the authorisation referred to in Article 25 of this Law (Article 24b paragraphs 1 and 2);

22) fails to use secure communication channels for interaction with the customer during electronic and video-electronic identification, using secure protocols and cryptographic algorithms in line with best practice and industry standards for the purpose of protecting

confidentiality, integrity, availability and data protection and for the purpose of cyber security (Article 24b paragraph 3);

23) fails to continuously monitor the solution referred to in Article 24b paragraph 1 of this Law in order to ensure that its functionality remains in line with this Law and the acts referred to in Article 24 of this Law (Article 24b paragraph 4);

24) fails to manage the identified risks referred to in Article 24b paragraph 1 of this Law (Article 24b paragraph 5);

25) commences electronic or video-electronic identification before preparing the risk analysis referred to in Article 24b paragraph 1 of this Law (Article 24b paragraph 6);

26) carries out electronic or video-electronic identification of a customer who is a natural person, sole proprietor or natural person carrying out a business activity, or of their legal representative or authorised person, without holding authorisation to carry out electronic or video-electronic identification (Article 25 paragraph 1);

27) obtains the data referred to in Article 26 paragraph 1 of this Law by inspecting a document issued more than three months earlier (Article 26 paragraph 3);

28) fails to notify the obliged entity that it acts as a trustee or as a representative or authorised person of a trustee and fails to provide the information referred to in Article 29 paragraph 1 of this Law (Article 29 paragraph 4);

29) fails to regulate by internal act the procedures for accepting identification of the customer and the beneficial owner of the customer through a third party (Article 34 paragraph 2);

30) fails to regulate by internal act the procedures for checking the completeness of data collected in line with Article 35 paragraphs 2 to 8 of this Law (Article 35 paragraph 11);

31) fails to verify the accuracy of the data collected under Article 36 paragraphs 2 and 3 of this Law in line with Articles 22, 23, 24, 26, 27 and 28 of this Law (Article 36);

32) fails to introduce effective procedures for establishing whether, in the messages or payment and settlement systems used to execute transfers of funds, the fields relating to payer and payee data are completed using the letters, numbers and symbols permitted under the rules of that system (Article 36 paragraph 5);

33) fails to prepare an internal act on the procedure, including, where appropriate, ex-post monitoring or real-time monitoring, where the payment order form or electronic message accompanying a transfer of funds does not contain the accurate and complete data referred to in Article 35 of this Law (Article 37 paragraph 1);

34) fails to warn the payment service provider of the payer that it repeatedly fails to submit accurate and complete data in line with Article 35 of this Law and fails to set a deadline within which that provider must bring its conduct in line with this Law (Article 37 paragraph 3);

35) fails to ensure that all data on the payer and payee are retained in the payment order form or electronic message accompanying a transfer of funds (Article 38 paragraph 1);

36) fails to prepare an internal act on the procedure, including, where appropriate, ex-post monitoring or real-time monitoring, where the payment order form or electronic message accompanying a transfer of funds does not contain the accurate and complete data referred to in Article 35 of this Law (Article 38 paragraph 2);

37) fails to save electronically or print an extract from the register referred to in Article 42 paragraph 2 of this Law and fails to mark the date and time and the name and surname of the person who carried out the check;

38) fails to require the customer to correct data in the register within eight days, or,

where the customer fails to do so within the prescribed deadline, fails to notify without delay the Financial Intelligence Unit and the state administration authority responsible for tax collection of the data which differ and the data on persons whom the obliged entity considers to be the beneficial owners of the customer (Article 42 paragraph 4);

39) fails to verify beneficial-owner data in line with Article 42 paragraph 7 of this Law;

40) when examining a foreign legal person, fails to obtain the additional data referred to in Article 50 paragraph 3 items 1 and 2 of this Law;

41) when applying enhanced customer due diligence and monitoring measures to a customer or beneficial owner who is a politically exposed person, fails, in addition to the measures referred to in Article 17 of this Law, to obtain the written consent of a senior manager before establishing a business relationship with the customer, or written consent of a senior manager to continue the business relationship where it has already been established (Article 56 paragraph 1 item 2);

42) in line with the guidelines referred to in Article 12 paragraph 5 of this Law, fails to regulate by internal act risk-based procedures applied to the identification of a customer who is a politically exposed person or to the establishment of the beneficial owner of a customer who is a politically exposed person, and to the monitoring of the business of that customer and beneficial owner (Article 56 paragraph 2);

43) fails to take appropriate measures to establish whether beneficiaries of life insurance or investment-linked life insurance and the beneficial owners of beneficiaries are politically exposed persons no later than at the time of payment under the policy or the full or partial transfer of the policy (Article 56a paragraphs 1 and 2);

44) in a higher-risk case, fails, in addition to the measures referred to in Article 17 of this Law, to take additional measures (Article 56a paragraph 3);

45) fails to apply the additional measures referred to in Article 56a paragraph 3 of this Law to members of the close family and close associates of persons referred to in Article 54 paragraphs 2 and 3 of this Law (Article 56a paragraph 4);

46) at the request of the Financial Intelligence Unit or the competent supervisory authority referred to in Article 131 paragraph 1 of this Law, fails to make available the results of the analysis referred to in Article 58 paragraph 1 item 6 of this Law (Article 58 paragraph 2);

47) fails to establish by internal act the criteria for recognising transactions referred to in Article 58 paragraph 1 of this Law (Article 58 paragraph 3);

48) when establishing a business relationship or carrying out transactions with persons from high-risk third countries, or where a high-risk third country is involved in a transaction, fails, in addition to the measures referred to in Article 17 of this Law, to obtain the written consent of a senior manager before establishing the business relationship, or, where the business relationship has already been established, to obtain written consent of a senior manager to continue it (Article 59 paragraph 1 item 2);

49) fails to implement the measures referred to in Article 59 paragraphs 1 and 2 of this Law in line with the money laundering and terrorist financing risk established in the risk analysis (Article 59 paragraph 3);

50) in relation to a customer for whom a lower money laundering and terrorist financing risk has been established, fails to implement business-relationship monitoring and transaction-control measures to the extent determined in line with Article 61 paragraph 1 item 3 of this Law (Article 61 paragraph 4);

51) fails to prepare an internal act prescribing the conditions under which services may be provided or transactions carried out by applying simplified measures, including restrictions relating to the amount, number or type of transactions that may be carried out in order to ensure that they comply with the expected standards for the particular business

relationship (Article 61 paragraph 5);

52) fails to ensure that the measures for preventing and detecting money laundering and terrorist financing established by this Law are implemented to the same extent in branches or majority-owned companies of the obliged entity having their registered office in another country which is a Member State of the European Union or a country applying the same standards for implementing measures for preventing and detecting money laundering and terrorist financing as those established by this Law or European Union law (Article 62 paragraph 1);

53) fails to designate a single point of contact in Montenegro to ensure, on its behalf, compliance with anti-money laundering and counter-terrorist financing rules and to facilitate supervision by the competent supervisory authority, in particular by providing documents and information at the request of that authority (Article 62 paragraph 8);

54) within 60 days from the date of establishment or commencement of business, fails to designate a compliance officer for the prevention of money laundering and terrorist financing and at least one deputy (Article 69 paragraph 1);

55) fails to submit to the Financial Intelligence Unit the notifications referred to in Article 69 paragraphs 1, 2 and 6 of this Law (Article 69 paragraph 9);

56) fails to submit the report referred to in Article 76 paragraph 1 item 12 of this Law to the competent supervisory authority referred to in Article 131 paragraph 1 of this Law at its request, within three days from the date of receipt of that request (Article 76 paragraph 2);

57) fails to provide regular professional training and development in the field of preventing and detecting money laundering and terrorist financing for all employees participating in those activities at the obliged entity (Article 78 paragraph 1);

58) fails to prepare the professional training and development programme referred to in Article 78 paragraph 1 of this Law by the end of the first quarter of the current year for that year (Article 78 paragraph 3);

59) fails to order and supervise the application of the rules referred to in Article 79 paragraphs 1 and 2 of this Law in branches and majority-owned companies of the obliged entity having their registered office in other countries (Article 79 paragraph 3);

60) fails to ensure regular internal control and audit of the implementation of policies, controls and procedures for preventing and detecting money laundering and terrorist financing, or the performance of activities for preventing and detecting money laundering and terrorist financing, in line with the money laundering and terrorist financing risk established in the risk analysis (Article 80 paragraph 1);

61) fails to organise an independent internal audit whose remit includes regular assessment of the adequacy, reliability and efficiency of the system for managing the risk of money laundering and terrorist financing where the law governing the obliged entity's business requires an independent internal audit (Article 80 paragraph 2);

62) fails to use the indicator lists referred to in Articles 82 and 83 of this Law when establishing reasons for suspicion that property derives from criminal activity or is connected with money laundering or terrorist financing, and other circumstances relating to that suspicion (Article 81);

63) fails to prepare its own list of indicators for recognising suspicious customers and transactions (Article 83 paragraph 1);

64) fails to submit to the Financial Intelligence Unit, in the manner prescribed by the act referred to in Article 66 paragraph 15 of this Law, the requested data, information and documentation (Article 91 paragraph 2);

65) fails to submit quarterly, by electronic means, to the Financial Intelligence Unit data on each collective custody account, the credit institution or other financial institution at

which that custody account is opened, and the number of transactions and total turnover on that collective custody account (Article 114 paragraph 3);

66) at the request of the competent supervisory authority, fails to submit, within eight days from the date of receipt of the request and in electronic form, accurate and complete data on the basis of which the sectoral money laundering and terrorist financing risk assessment is carried out (Article 131 paragraph 14).

Exceptionally, for the misdemeanour referred to in paragraph 1 of this Article, an obliged entity referred to in Article 4 paragraph 2 items 1, 2 and 3 of this Law shall be fined EUR 10,000 to EUR 80,000.

For the misdemeanour referred to in paragraph 1 of this Article, a member of the management body or other responsible person in a legal person, a natural person, a natural person carrying out a business activity and a notary shall be fined EUR 500 to EUR 4,000.

For the misdemeanour referred to in paragraph 1 of this Article, a sole proprietor shall be fined EUR 500 to EUR 12,000.

For the misdemeanour referred to in paragraph 1 of this Article, a legal person, a sole proprietor, a responsible person in a legal person and a natural person may be prohibited from performing their profession, activity or duty for a period of up to six months.

For the misdemeanour referred to in paragraph 1 item 56 of this Article, the request for initiation of misdemeanour proceedings shall also be submitted by an authorised police officer of the Financial Intelligence Unit.

Misdemeanour proceedings for misdemeanours referred to in paragraph 1 of this Article committed by credit institutions and other financial institutions may not be initiated after four years have elapsed from the date on which the misdemeanour was committed.

**Article 138**

**(***Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 39)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 70)*

Notary shall be fined EUR 3,000 to EUR 8,000 for a misdemeanour if:

1) the notary fails to enter a trust in the Register of Trusts within five days from the date on which the notarial deed relating to the acquisition of immovable property on behalf of the trust was drawn up (Article 43a paragraph 5);

2) the notary draws up and certifies a notarial record enabling avoidance of the national payment system of Montenegro in connection with Article 65a paragraph 1 of this Law (Article 65a paragraph 2);

3) the notary fails to obtain proof that the payment transaction under a contract or preliminary contract for the sale and purchase of immovable property, or another legal transaction whereby ownership or another real right in immovable property is acquired or transferred, was executed before certification of the legal transaction (Article 65a paragraph 3);

4) the notary fails to submit to the Financial Intelligence Unit, without delay and no later than three days from the date of conclusion of the legal transaction, accurate and complete data on customer due diligence and monitoring measures referred to in Article 117 paragraphs 1 to 6 of this Law for each transaction or acquisition of rights under a preliminary contract or contract relating to immovable property with a value of EUR 15,000 or more, and under a contract, statement or any instrument relating to a loan with a value of EUR 10,000 or more (Article 66 paragraph 4);

5) the notary fails to submit to the Financial Intelligence Unit, without delay and no later than three days from the date of conclusion of the legal transaction, an electronic copy of the contract or a copy of the statement of the natural person who is the buyer on the source of money for contracts executed using cash, together with the proof referred to in Article 65a paragraph 3 of this Law (Article 66 paragraph 5).

Notary may be prohibited from performing the profession, activity or duty for a period of up to six months for the misdemeanour referred to in paragraph 1 of this Article.

**Article 138a**

**(***Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 49)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 71)*

Natural person who is the beneficial owner of an entity shall be fined EUR 3,000 to EUR 8,000 for a misdemeanour if that person fails to provide the entity referred to in Article 43 paragraph 3 of this Law with the data referred to in Article 44 paragraph 1 item 2 indents 1, 2 and 4 of this Law for entry in the Register of Beneficial Owners (Article 43 paragraph 6).

Politically exposed person referred to in Article 54 paragraphs 1 and 2 of this Law shall be fined EUR 500 to EUR 1,000 for a misdemeanour if that person fails, without delay and no later than eight days from the date of appointment, to enter accurate and complete data on themselves and the persons referred to in Article 54 paragraph 4 of this Law in the Register of Politically Exposed Persons (Article 55 paragraph 5).

Natural person shall be fined EUR 1,000 to EUR 8,000 for a misdemeanour if that person receives a payment or makes a cash payment in the amount of EUR 10,000 or more, or where the payment is made in two or more linked transactions in a total amount of EUR 10,000 or more (Article 65 paragraphs 1 and 2).

## XI. TRANSITIONAL AND FINAL PROVISIONS

### Deadline for Adoption of Secondary Legislation

**Article 139**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 72)*

Secondary legislation for implementation of this Law shall be adopted within three months from the date of entry into force of this Law.

Pending the adoption of the secondary legislation referred to in paragraph 1 of this Article, secondary legislation adopted pursuant to the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro" 33/14, 44/18, 73/19 and 70/21) shall apply, provided that it is not contrary to this Law.

Secondary legislation referred to in Article 111a paragraph 6 of this Law shall be adopted within six months from the date of entry into force of this Law.

### Implementation of measures for already established business relationships

**Article 140**

Obliged entity shall implement the measures referred to in Article 17 of this Law in

relation to customers referred to in Article 18 paragraph 2 of this Law with whom it has already established business relationships when carrying out the first transaction after the entry into force of this Law.

**Entering and updating data in the Register of beneficial owners**

**Article 141**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 50)*

Legal person, business organisation, association, institution, political party, religious community, artistic organisation, chamber, trade union, employers' association, foundation or other business entity, a legal person that receives, manages or distributes funds for specific purposes, a trust, other person or foreign-law entity equivalent to it under foreign law that receives, manages or distributes assets for specific purposes, registered in the CRPS or the register of taxpayers before the entry into force of this Law and that has not entered or updated the data in the Register of Beneficial Owners, shall enter or update such data within 30 days from the date of entry into force of the act referred to in Article 45 paragraph 4 of this Law.

**Establishing records**

**Article 142**

Obliged entities, state and other authorities and institutions shall establish the records which they are required to keep in line with this Law within three months from the date of entry into force of this Law.

**Harmonizing business activities**

**Article 143**

Obliged entities shall, for the purpose of preventing money laundering and terrorist financing, bring their operations in line with this Law within six months from the date of entry into force of the by-laws referred to in Article 139 paragraph 1 of this Law.

**Obtaining licences**

**Article 144**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 40)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 73)*

Compliance officers for the prevention of money laundering and terrorist financing and their deputies who were designated before the date of entry into force of this Law shall obtain a licence in line with this Law within 24 months from the date of entry into force of the acts referred to in Articles 71 and 72 of this Law.

Until obtaining a licence in line with paragraph 1 of this Article, compliance officers for the prevention of money laundering and terrorist financing and their deputies shall continue to perform their duties in line with this Law.

Should compliance officers for the prevention of money laundering and terrorist financing and their deputies fail to obtain a licence in line with this Law within the period referred to in paragraph 1 of this Article, their status as compliance officers for the prevention of money laundering and terrorist financing or deputy compliance officers shall cease.

**Deadline for establishing a register of accounts and safe-deposit boxes**

**Article 145**

Central Bank of Montenegro shall establish the registers referred to in Article 112 of this Law within 12 months from the date of entry into force of this Law.

**Deadline for Establishing Risk Analysis Guidelines and the System for Managing Money Laundering and Terrorist Financing Risk**

**Article 145a**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 51)*

Supervisory authority referred to in Article 131 paragraph 1 item 3 of this Law shall establish guidelines for risk analysis and for establishing the system for managing money laundering and terrorist financing risk in line 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**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 51)*

Administrative authority 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 the Register of Crypto-Asset Service Providers**

**Article 145c**

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 024/25 of 12 March 2025, Article 51)*

Supervisory authority referred to in Article 131 paragraph 1 item 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.

## Establishing obliged entities' internal acts and organisation

### Article 146

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 74)*

Obliged entities shall bring their internal acts and internal organisation in line with this Law within six months from the date of entry into force of this Law.

Until the adoption of internal acts referred to in Articles 77, 78 and 80 of this Law, the Rulebook on the manner of work of an authorised person, the manner of conducting internal control, the storage and protection of data, the manner of keeping records and the training of employees ("Official Gazette of Montenegro", no. 71/20) shall be applied.

Obliged entities shall adopt the internal act referred to in Article 61 paragraph 5 of this Law within six months from the date of entry into force of this Law.

## Deferred Application

### Article 146a

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 065/24 of 5 July 2024, Article 41)*

*(Law Amending the Law on the Prevention of Money Laundering and Terrorist Financing, Official Gazette of Montenegro 059/26 of 4 May 2026, Article 75)*

Provisions of Article 48a, Article 108 paragraph 2 and Article 134 paragraphs 8 and 9 of this Law shall apply from the date of accession of Montenegro to the European Union.

## Initiated Procedures

### Article 147

Proceedings initiated before the date of entry into force of this Law that have not been finally concluded shall be concluded under the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro" 33/14, 44/18, 73/19 and 70/21).

## Repealing

### Article 148

On the date of entry into force of this Law, the Law on the Prevention of Money Laundering and Terrorist Financing ("Official Gazette of Montenegro" 33/14, 44/18, 73/19 and 70/21) shall cease to have effect.

## Entry into force

### Article 149

This Law shall enter into force on the eighth day following its publication in the "Official Gazette of Montenegro".

---

* Provisions of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 have been transposed into this Law.

* Provisions of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU and Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 have been transposed into this Law.

* Provisions of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU and 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 have been transposed into this Law.