

LAW ON THE PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM UNOFFICIAL CONSOLIDATED TEXT

CHAPTER I. GENERAL PROVISIONS

Article 1

This Law regulates the measures, actions and procedures that entities and competent authorities and bodies undertake to detect and prevent money laundering, related criminal offences and terrorist financing (hereinafter: money laundering and terrorist financing), as well as the operations and competencies of the Financial Intelligence Unit (hereinafter: the Unit).

Definitions

Article 2

The expressions used in this law have the following meaning:

- 1) **"Money laundering"** means the actions provided for by the Criminal Code as a criminal offense of laundering money and other proceeds of crime;
- 2) **"Financing of terrorism"** are the actions provided for by the Criminal Code as a criminal offense of financing of terrorism;
- 3) **"Terrorist act"** is a criminal offense defined in Article 2 of the International Convention for the Suppression of the Financing of Terrorism ratified in accordance with the Law on Ratification of the International Convention for the Suppression of the Financing of Terrorism, ("Official Gazette of the Republic of Macedonia" No. 30/2004), as a criminal offense of terrorism and other criminal offenses related to terrorism provided for in the Criminal Code;
- 4) **"Terrorist"** is a natural person who:
 - a) commits or attempts to commit a terrorist act in any way, directly or indirectly, unlawfully and knowingly;
 - b) participates as an accomplice in a terrorist act;
 - c) organizes or orders others to commit a terrorist act or
 - d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose, with the intention of carrying out the terrorist act and/or with knowledge of the group's intention to commit a terrorist act;
- 5) **"Terrorist organization"** is a group of terrorists that:
 - a) commits or attempts to commit a terrorist act in any way, directly or indirectly, unlawfully and knowingly;
 - b) participates as an accomplice in a terrorist act;
 - c) organizes or orders others to commit a terrorist act or
 - d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose, with the intention of carrying out the terrorist act and/or with knowledge of the group's intention to commit a terrorist act;
- 6) **"Proceeds of crime"** means proceeds of crime in accordance with the Criminal Code;
- 7) **"Related crime"** is a crime that generates income that may be the object of the action of the crime of money laundering;
- 8) **"Property"** means money or other means of payment, securities, deposits, other property of any form, whether tangible or intangible, including virtual assets in accordance with law, movable or immovable, other rights over objects, claims, as well as public documents and legal documents of

ownership and assets in written or electronic form or instruments that are evidence of property rights or legal interests;

9) "**Financial institutions**" are:

a) banks and savings banks established with a license from the Governor of the National Bank of the Republic of North Macedonia whose main activity is collecting deposits and other repayable sources of funds from the public and approving loans in their own name and for their own account;

b) legal entities that are not banks or savings banks that perform one or more of the following activities:

- lending, including factoring and financing of commercial transactions,
- issuing and administering means of payment (cheques, traveler's checks, bills of exchange),
- issuing electronic money,
- financial leasing,
- exchange operations,
- payment services in the country and abroad, including depositing and withdrawing cash on a payment account, activities related to opening, running/maintaining and closing the account, executing payment transactions, issuing payment instruments and/or accepting payment transactions, money remittances (including fast money transfers, as a type of money remittance) and payment initiation services,
- issuing payment guarantees, avals and other forms of collateral,
- trading in money market instruments,
- trading in foreign exchange, which also includes trading in precious metals,
- trading in securities,
- trading in financial derivatives,
- asset and portfolio management securities for clients and/or investment advice to clients,
- providing services for the safekeeping of investment and pension funds' assets,
- buying and selling, guaranteeing or placing an issue of securities,
- safekeeping of securities for clients,
- advising legal entities on the capital structure, business strategy or other related issues or providing services related to the merger or acquisition of legal entities,
- mediation in concluding credit and loan agreements and
- processing and analysis of information on the creditworthiness of legal entities;

c) legal and natural persons carrying out insurance activities, representation and/or mediation in life insurance with a savings and/or investment component and other related insurance with a savings and/or investment component;

d) private investment fund management companies and private funds;

e) open-end investment fund management companies and closed-end investment fund management companies;

f) mandatory and voluntary pension fund management companies;

g) branches of foreign financial institutions from subparagraphs a), b), c), d), e) and f) of this point in the Republic of North Macedonia;

h) AD Post of North Macedonia in the part of its operations related to postal money orders;

h) other legal or natural persons who, in accordance with the law, perform one or more activities related to granting loans, financial leasing, factoring, forfeiting, providing investment advisory services, keeping or administering/distributing cash and other financial activities determined by law;

10) "**Business relationship**" is a business, professional or commercial relationship, which is related to the professional and business activities of the entity referred to in Article 5 of this Law and which is expected at the time of its establishment to have an element of duration;

- 11) "**Occasional transaction**" is a transaction that is not carried out within the framework of an established business relationship;
- 12) "**Client**" is a natural person, legal entity, foreign trust and similar legal arrangement that establishes, has established a business relationship with the entity or carries out an occasional transaction;
- 13) "**Transaction**" means the payment and/or disbursement of cash, the payment (reception) and disbursement of a deposit, the exchange of currencies, the transfer of funds, the purchase, sale, exchange, receipt and transfer of virtual assets, the conclusion of contracts, the purchase and sale of goods and services, the sale or assignment of founding investments, the purchase or assignment of shares or units, the registration of securities or the transfer of securities or other property and other activities carried out by entities in accordance with the legal authorizations. In the insurance business, it means the payment of a premium and the payment of an insured amount upon occurrence or payment in the event of a harmful event, an advance/loan or the redemption of a life insurance policy;
- 14) "**Linked cash transactions**" are two or more cash transactions carried out within one business day of the execution of the first transaction by the same client or between the same clients or beneficial owners or carried out by multiple persons for the benefit of the same client;
- 15) "Money (cash)" means money in accordance with Article 2 paragraph (1) item 79 of the Law on Payment Services and Payment Systems (*);
- 16) "**Cash**" means paper and coin money that, based on law, is in circulation in the Republic of North Macedonia or in a foreign country;
- 17) "**Electronic money**" means electronic money in accordance with law;
- 18) "**Prepaid payment card**" is a type of payment instrument on which electronic money is stored;
- 19) "**Virtual assets**" are digital records of value or rights that can be stored, traded or transferred electronically using distributed ledger technology or any similar technology and can be used for exchange or investment purposes. Virtual assets do not include digital records of fiat currencies or money within the meaning of law that constitute legal tender, securities and other financial assets in accordance with law;
- 20) "**Virtual asset service provider**" means any natural or legal person whose business and professional activity consists of performing one or more activities or providing one or more services related to virtual assets for or on behalf of another natural or legal person;
- 21) "**Virtual asset services or activities**" are activities and services related to any virtual assets and include:
- a) custody and administration of virtual assets or instruments that enable control over virtual assets;
 - b) organization of a platform for trading virtual assets;
 - c) exchange of virtual assets for fiat currency, electronic money or other assets that are legal tender;
 - d) exchange of virtual assets for other virtual assets;
 - e) execution of orders for virtual assets for third parties;
 - f) participation in and provision of services related to the issuer's offer and/or sale of virtual assets;
 - f) management of a portfolio of virtual assets;
 - h) reception and transmission of orders for virtual assets and
 - h) provision of advice on virtual assets.
- 22) "**Custody and administration of virtual assets or instruments that enable control over virtual assets**" means custody or control of virtual assets for third parties or means through which virtual assets are accessed, where applicable in the form of private cryptographic keys;
- 23) "**Organization of a virtual asset trading platform**" means the organization and management of one or more virtual asset trading platforms within which the bringing together of buying and selling interests in virtual assets from third parties is enabled and facilitated and which can

communicate in a manner that results in a contract, whether for the exchange of one virtual asset for another or a virtual asset for a legal tender;

24) "**Execution of orders for virtual assets on behalf of third parties**" means the activity of buying or selling one or more virtual assets or ordering one or more virtual assets on behalf of third parties;

25) "**Participation in and provision of services related to the issuer's offering and/or sale of virtual assets**" means the placement of newly issued virtual assets or virtual assets that have already been issued but have not been accepted for trading on a virtual asset trading platform, to a specific group of buyers and which does not involve a public offering or an offer to existing holders of virtual assets of the issuer;

26) "**Virtual asset portfolio management**" means the management of individual virtual asset portfolios, based on a previously concluded agreement with the individual client;

27) "**Reception and transfer of orders for virtual assets**" means a service related to virtual assets provided to legal or natural persons participating in trade in accordance with the law, which enables the acceptance of a certain value in virtual assets corresponding to the price of the goods or services sold to the end consumer and through the exchange of virtual assets into fiat currency, i.e. money within the meaning of the law, the transfer of funds to legal and natural persons participating in trade is carried out;³

28) "**Virtual Asset Issuer**" means a natural or legal person who offers any type of virtual assets or seeks admission of such virtual assets to a virtual asset trading platform;

29) "**Public offering of virtual assets**" is an offer to third parties to acquire virtual assets in exchange for fiat currency or money within the meaning of law or other virtual assets;

30) "**Providing advice on virtual assets**" means offering, giving or providing personalized or specific recommendations to a third party, either at the request of a third party or at the initiative of the virtual asset service provider providing the advice, in relation to the acquisition or sale of one or more virtual assets, or the use of virtual asset services;

31) "**Crypto-machine**" is an automatic machine, i.e. an electromechanical device through which the provider of a service related to virtual assets trades, exchanges or transfers virtual assets for legal tender or for other virtual assets or provides other services depending on the type of crypto-machine;

32) "**Hosted electronic wallet for virtual assets**" means any facility provided by a virtual asset service provider for the storage and/or administration of virtual assets on behalf and for the account of the customer or user;

33) "**Non-hosted electronic wallet for virtual assets**" means any other means of storing and/or administering virtual assets, other than a hosted electronic wallet on which virtual assets are stored;

34) "**Physically transferable means of payment**" means traveler's checks, checks, bills of exchange, money orders and other physically transferable means of payment that are payable to bearer or are transferable without restriction;

35) "**Service providers to legal entities or trusts**" are natural or legal persons who, within the framework of their activity, provide the following services to third parties:

a) establish legal entities;

b) act as or engage another person to act as a management body or a member of the management body of the legal entity;

c) provide a registered office, business address, correspondence address or other related services to a legal entity or foreign trust;

d) act as or engage another person to act as a manager of a foreign trust or similar legal arrangement established by an express declaration;

e) act as or engage another person to act as a partner or act as a shareholder for another person (except for a listed company);

36) "**Trust**" is a legal relationship established in accordance with the regulations of another country between a person-founder, during life (inter vivos) or after death, when the property is entrusted to the management of a trustee for the benefit of a beneficiary/group of beneficiaries or for a specific purpose;

37) "**Beneficial owner**" means any natural person(s) who is the ultimate owner of the client or controls the client and/or the natural person(s) in whose name and for whose account a transaction is being carried out. The term also includes a natural person(s) who exercises ultimate and effective control over a legal person or foreign legal arrangement;

38) "**Register of beneficial owners**" is an information system that enables the receipt, recording, processing, storage and exchange of data and/or documents on beneficial owners in electronic form;

39) "**Public office holders**" are:

a) natural persons who are or have been entrusted with a public function in the Republic of North Macedonia or in another state, such as:

- presidents of states and governments, ministers and deputy or assistant ministers,
- elected representatives in the legislative branch,
- judges of supreme or constitutional courts or other holders of high judicial functions against whose decisions, except in exceptional cases, no legal remedies may be used,
- members of the management bodies of supervisory and regulatory bodies and agencies, the state audit institution and members of the board of a central bank,
- ambassadors,
- high-ranking officers in the armed forces (ranks higher than colonel),
- elected and appointed persons in accordance with law and members of the management and supervisory bodies of legal entities established by the state,
- persons holding functions in political parties (members of the executive bodies of political parties),
- persons who are or have been entrusted with a prominent function in an international organization, such as directors, deputy directors, members of management and supervisory boards or other equivalent functions and
- mayors and presidents of municipal councils.

b) Holders of public office from subparagraph a) of this point are considered persons at least two years after the termination of the performance of public office, and on the basis of a previously conducted risk assessment by the entities.

c) The term "holders of public office" also includes:

- family members of the holder of public office, namely: spouse or person with whom the holder of public office is in an extramarital relationship, children and their spouses or persons with whom the children of the holder of public office are in an extramarital relationship or parents of the holder of public office,
- a person who is considered a close associate of the holder of public office is a natural person who is known to have joint legal or actual ownership of a legal entity, has concluded contracts or established other close business relationships with the holder of public office or who is the sole beneficial owner of a legal entity or legal arrangement known to be established for the benefit of the holder of public office;

40) "**Temporary measures**" are temporary prohibitions on the use or disposal of money, securities, funds or other property, temporary storage and security based on a decision issued by a court or other competent authority in a procedure established by law;

41) **"Correspondent relationship"** is:

- a) when a bank as a "correspondent" provides banking services to another bank as a "respondent", including account maintenance and provision of account maintenance services such as cash management, international funds transfers, check settlement, payment used directly by third parties to perform work on their own behalf and foreign exchange services and/or
- b) a relationship between and within banks and other financial institutions when similar services are provided through a financial institution correspondent to the respondent financial institution, as well as relationships established for securities transactions or transfers of funds;
- c) a relationship between and within financial institutions and virtual asset service providers when similar services are provided through a virtual asset service provider correspondent to the respondent financial institution, as well as relationships established for virtual asset transactions or transfers of virtual assets;
- d) when a virtual asset service provider acts as a "correspondent" and provides services to another virtual asset service provider as a "respondent", including the management of instruments that enable control over virtual assets and services related to the management of instruments that enable control over virtual assets, international transfers of virtual assets as well as other relationships established for transactions with virtual assets or the transfer of virtual assets;

42) **"Transfer of funds"** means any transaction, including money remittances, which is at least partly executed electronically on behalf of the payer through a payment service provider with the aim of making funds available to the payee through a payment service provider, regardless of whether the payer and the payee are the same person and regardless of whether the payment service provider of the payer and the payee is the same;

43) **"Transfer of virtual assets"** means any transaction with virtual assets that is carried out electronically on behalf of the orderer through a virtual asset service provider with the aim of making the virtual assets available to the recipient, regardless of whether the orderer and the recipient are the same person and regardless of whether the virtual asset service provider of the orderer and the recipient is the same;

44) **"Program"** is an act of the entity that determines rules, procedures and instructions for the application of measures and actions for the prevention of money laundering and terrorist financing for the efficient reduction and management of the identified risk of money laundering and terrorist financing;

45) **"Authorized person"** is a person employed in the entity and appointed by the entity's management body, who is responsible for implementing measures and actions to prevent money laundering and terrorist financing and for cooperating with the Administration;

46) **"Senior management of the entity"** is a person who is authorized by law and internal acts to manage and is responsible for the operations of the entity and who has appropriate authorizations and functions to make decisions that may affect the exposure of the entity to the risk of money laundering and terrorist financing;

47) **"Responsible person in a legal entity"** is a responsible person in accordance with the Law on Misdemeanors;

48) **"Shell bank"** is a financial institution that does not have business premises, employees or management bodies in the country where it is registered and is not a member of a banking or other type of group that is subject to supervision on a consolidated basis;

49) **"Games of Chance"** are games of chance in accordance with the Law on Games of Chance and Entertainment Games;

50) **"Group"** is a group of legally independent companies in which a certain company (parent company) has control over one or more companies (subsidiaries) and consists of the parent company, its subsidiaries, companies with which the parent company or its subsidiaries are related through participation in the capital, as well as companies that are related to companies in the group

through control or are controlled by the same company included in the group.

50-a) "**Financial group**" is a group whose parent company is a financial institution with its registered office in the Republic of North Macedonia.⁴

51) "**National Risk Assessment**" is a comprehensive process of identification and analysis of the risks of money laundering, terrorist financing and financing of the spread of weapons of mass destruction (proliferation financing) and other relevant risks in a particular country, for the purpose of developing appropriate measures to prevent money laundering and terrorist financing and efficient allocation of available resources in order to control, reduce or eliminate the identified risks and improve the system for preventing money laundering and terrorist financing;

52) "**Financial Intelligence Unit**" is a central national authority responsible for receiving and analyzing reports of suspicious transactions and other information of significance for money laundering and terrorist financing and submitting the results of the analysis and other additional relevant information to the competent authorities when there are grounds for suspicion of money laundering and terrorist financing;

53) "**Legal entity**" is a local self-government unit, political party, public enterprise, trade company, law firm, institution, association, foundation, union and organizational form of a foreign organization, sports association and other legal entity in the field of sports, financial organization and other organization specified by law registered as a legal entity and other organizational form recognized as a legal entity;

54) "**Legal arrangement**" means a trust and other similar legal form established in accordance with the regulations of a foreign country;

55) "**High-risk countries**" are countries that have not implemented or have insufficiently implemented international standards for the prevention of money laundering and terrorist financing, as well as countries identified by the FATF, the European Union, as well as countries for which competent international bodies require the taking of appropriate countermeasures or countries identified in accordance with the national risk assessment;

56) "**FATF - Financial Action Task Force**" is an intergovernmental body established by the G7 countries in 1989 with the aim of setting standards and promoting the effective implementation and advancement of standards as well as monitoring the effective implementation of legal, regulatory and operational measures to prevent money laundering, terrorist financing and the financing of the spread of weapons of mass destruction (proliferation financing) at the international level;

57) "**FATF Recommendations**" are international standards for the prevention of money laundering, terrorist financing and the financing of weapons of mass destruction (proliferation financing) issued by the FATF;

58) "**Non-profit organizations**" are legal entities, legal arrangements or organizations that are primarily involved in raising or redistributing funds for charitable, religious, cultural, educational or social purposes or other types of charitable activities;

59) "**Financing of proliferation of weapons of mass destruction**" means the provision of funds or financial services used, in whole or in part, for the production, acquisition, possession, development, export, transnational carriage, brokering, transportation, transfer, storage or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for illegitimate purposes), in violation of a law or a legal act of an international organization;

60) The terms interoperability, electronic document, electronic identification means, issuer of an electronic identification means and electronic identification scheme have the same meaning in accordance with the Law on Electronic Governance and Electronic Services and the Law on Electronic Documents, Electronic Identification and Trust Services;

- 61) "**Payment service provider**" means a bank or payment institution or electronic money institution with a license to provide payment services, i.e. a license to issue electronic money in accordance with the Law on Payment Services and Payment Systems (*);
- 62) "**Intermediary institution in the transfer of funds**" means a payment service provider that is not a payment service provider of the payer or a payment service provider of the payee, and that receives and transfers funds on behalf of the payer's payment service provider, on behalf of the payee's payment service provider or on behalf of another intermediary payment service provider;
- 63) "**Payer**" means a natural person or legal entity that has a payment account and agrees to execute a payment order from that account, or in the case where there is no payment account, a natural person or legal entity that issues a payment order;
- 64) "**Recipient**" means a natural person or legal entity for whom the funds that are the subject of the payment transaction are intended;
- 65) "**Virtual Asset Address**" is an alphanumeric identifier that identifies a network address of a distributed storage technology for encrypted data and records or any similar technology through which virtual assets are received and transferred;
- 66) "**Supranational Risk Assessment**" is an assessment of the risk of money laundering and terrorist financing carried out by the European Commission;
- 67) "**Batch file transfer**" is a collective transfer of multiple individual transfers or transfers of virtual assets that are combined together for the purposes of transfer;
- 68) "**Sender**" is a natural person or legal entity that has an account, i.e. a hosted electronic wallet for virtual assets with a virtual asset service provider or a device that allows the storage of virtual assets and allows the transfer of virtual assets from the account, hosted electronic wallet, or device, or the person who initiates or gives an order for the transfer of virtual assets when there is no account, hosted electronic wallet, or device;
- 69) "**Beneficiary**" is a natural person or legal entity to whom the transfer of virtual assets is intended;
- 70) "**Transfer of virtual assets between persons**" is the transfer of virtual assets without the involvement of service providers related to virtual assets and
- 71) "**Entity identifier**" is a unique alphanumeric reference identifier assigned to a legal entity in accordance with the international standard ISO 17442 or higher for the assignment of identifiers.

CHAPTER II.

NATIONAL RISK ASSESSMENT

National risk assessment of money laundering, terrorist financing, financing of weapons of mass destruction and other related risks

Article 3

- (1) The Republic of North Macedonia shall conduct a national risk assessment to identify, assess, understand and mitigate the risk associated with money laundering, terrorist financing, weapons of mass destruction financing and other related risks, and shall update it at least every four years.
- (2) When conducting the national risk assessment referred to in paragraph (1) of this Article, the findings of the Supranational Risk Assessment shall also be taken into account.
- (3) The Council for Combating Money Laundering and Terrorism Financing under this Law is responsible for coordinating the activities for implementing the national risk assessment in the Republic of North Macedonia and preparing a report on the national risk assessment.
- (4) The Council for Combating Money Laundering and Terrorism Financing shall submit the national risk assessment report referred to in this Law to the Government of the Republic of North Macedonia for adoption.

(5) The national risk assessment report, as well as all amendments and supplements to the report, shall be published on the website of the Authority. The published report shall not contain confidential data in accordance with the law.

Objectives of the national risk assessment

Article 4

(1) The findings of the national risk assessment report are used for:

- defining and implementing measures and actions to prevent money laundering, terrorist financing, financing of proliferation of weapons of mass destruction and other related risks in accordance with the identified risk,
- identifying shortcomings in the system for preventing money laundering and terrorist financing and measures to overcome them,
- improving the national regulation and system for preventing money laundering and terrorist financing,
- identifying sectors or activities with a lower or higher risk of money laundering and terrorist financing,
- identifying sectors or activities in relation to which entities are obliged to undertake enhanced analysis measures and, if necessary, determining other measures that entities are obliged to undertake,
- defining priorities and allocating resources in order to prevent money laundering, terrorist financing and financing of proliferation of weapons of mass destruction,
- preparing and adopting relevant regulations for individual sectors or activities and implementing measures in accordance with the identified risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction,
- informing and assisting entities in conducting their assessment of the risk of money laundering, financing of terrorism, financing of proliferation of weapons of mass destruction and other related risks,
- informing about the institutional structure and actions of the competent institutions in the system for preventing money laundering, financing of terrorism, financing of proliferation of weapons of mass destruction and other related risks as well as the allocated resources to the extent to which this information is available and
- informing about national measures and resources intended for combating money laundering, financing of terrorism, financing of proliferation of weapons of mass destruction and other related risks.

(2) The Council for Combating Money Laundering and Terrorism Financing under this Law, based on the findings of the national risk assessment report, shall prepare a draft National Strategy for Combating Money Laundering and Terrorism Financing with an action plan of measures and activities for reducing and managing the identified risks and consequences of money laundering and terrorism financing, financing of the proliferation of weapons of mass destruction and other related risks, and shall monitor its implementation as well as the fulfilment of the action plan.

(3) The Government of the Republic of North Macedonia shall adopt the National Strategy for Combating Money Laundering and Financing of Terrorism with the action plan of measures and activities referred to in paragraph (2) of this Article, for a period of four years.

CHAPTER III.
MEASURES AND ACTIONS TAKEN BY ENTITIES FOR THE PURPOSE OF DETECTING AND
PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING

1. GENERAL PROVISIONS

Subjects

Article 5

Entities are persons who are obliged to take the measures and actions for the detection and prevention of money laundering and terrorist financing provided for in this Law (hereinafter referred to as: entities), namely:

- 1) Financial institutions and subsidiaries, branches and business units of foreign financial institutions that, in accordance with the law, carry out activities in the Republic of North Macedonia;
- 2) Legal and natural persons who, as a business or professional activity, perform the following services:
 - a) mediation in real estate transactions, including and/or mediation in concluding real estate lease agreements only when the value of the monthly lease is 10,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia;
 - b) auditing and accounting services;
 - c) providing advice in the field of taxes or any form of assistance, support or advice, directly or through another person in the field of taxes;
 - d) providing services as an investment advisor and
 - e) providing services for organizing and conducting auctions;
- 3) Notaries, lawyers and law firms that exercise public authorization in accordance with the law;
- 4) Organizers of games of chance that organize games of chance in the Republic of North Macedonia in accordance with the law;
- 5) Service providers to trusts or legal entities;
- 6) Central Securities Depository;
- 7) Legal entities that perform the activity of accepting movable objects and real estate as collateral (pawnshops);
- 8) Persons who trade or act as intermediaries in the trade of works of art, including when the activity is performed by art galleries or auction houses, and where the value of the individual transaction or several related transactions amounts to 10,000 euros in denar equivalent or more according to the middle exchange rate of the National Bank of the Republic of North Macedonia;
- 9) Persons who store, trade or act as intermediaries in the trade of works of art, when the activity takes place in free zones and where the value of the individual transaction or several related transactions amounts to 10,000 euros in denar equivalent or more according to the middle exchange rate of the National Bank of the Republic of North Macedonia and
- 10) Providers of services related to virtual assets.

**Exceptions regarding legal and natural persons carrying out financial activities on an
occasional or limited basis**

Article 6

(1) Entities referred to in Article 5 of this Law that carry out financial activities on an occasional or limited basis and for which the national risk assessment has determined a low risk of money laundering and terrorist financing, are not obliged to apply the measures and actions for the prevention of money laundering and terrorist financing provided for in this Law, if the following conditions are met:

- the financial activity is secondary and directly related to the main business activity,
 - the annual net turnover from the financial activity does not exceed 100,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia or 5% of the total annual turnover of the entity,
 - the main activity is not the provision of auditing services, organizing and holding games of chance, accounting services, tax advisory services, real estate brokerage activities, providing services to trusts or legal entities or notary and lawyer services,
 - the highest transaction amount per client and per individual transaction, regardless of whether it is carried out as one or several transactions that appear to be interconnected must not exceed 500 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia and
 - the financial activity is carried out only for persons who are clients from the perspective of the main business activity and is not generally available to the public.
- (2) The provisions of paragraph (1) of this Article shall not apply to legal entities, sole proprietors or natural persons who independently carry out an activity if they make money transfers in accordance with the law.
- (3) The entity referred to in paragraph (1) of this Article shall submit a request to the Administration not to apply the provisions of this Law. The request shall be accompanied by documentation from which it can be determined that the conditions referred to in paragraph (1) of this Article have been met and documentation for a conducted assessment of the risk of money laundering and terrorist financing for each financial activity.
- (4) For the request referred to in paragraph (3) of this Article, the Administration shall adopt a decision in accordance with the provisions of the Law on General Administrative Procedure.
- (5) The decision referred to in paragraph (4) of this Article shall be valid for two years from the date of its adoption. After the expiry of the decision, the entity shall submit a new request for exemption from the application of the provisions of this Law in accordance with paragraph (3) of this Article.
- (6) If the circumstances on the basis of which the decision is issued change before the expiry of the validity of the decision, the entity referred to in paragraph (1) of this Article shall be obliged to notify the Administration of these changes within 15 days from the day of their occurrence. Based on this notification or on the basis of other information, the Administration shall ex officio adopt a new decision with a validity of two years, annulling the previous decision and deciding on the application of the provisions of this Law.

Article 7

- (1) Notaries, lawyers and law firms exercising public powers in accordance with the law are obliged to apply the measures and actions for the prevention of money laundering and terrorist financing in cases where they provide legal services to their clients that relate to the following activities:
- a) purchase and sale of real estate and movable property or leasing of property;
 - b) management of money, securities or other property or assets of the client;
 - c) opening and management of bank accounts, savings deposits, safes or securities accounts;
 - d) organizing the collection of funds for the establishment, operation or management of legal entities;
 - e) establishment, operation or management of legal entities or legal arrangements, purchase and sale of legal entities or legal arrangements as well as any form of assistance, support or advice, directly or through another person for the purposes of the sale or purchase of legal entities or legal arrangements.

(2) The obligations arising from this Law shall not apply to the entities referred to in Article 5, item 2), sub-items b) and c) and item 3) of this Law when they perform the function of defense, representation or other activities for which they are authorized by law on behalf of the client in a court procedure. In this case, upon request of the Administration, the entity referred to in this paragraph shall, within seven days, submit a written explanation of the reasons for not acting in accordance with the provisions of this Law.

Virtual asset service providers

Article 8

(1) The Authority shall maintain and keep a Register of Service Providers Related to Virtual Assets in electronic form, which shall be published on its website.

(2) The register of virtual asset service providers shall contain:

1) name of the legal entity, registered office, electronic address, unique identification number (EMBS) and unique tax number (EDB), date of establishment and activity code;

2) data on the members of the management body (name and surname, unique identification number or other identification number, address of residence, i.e. place of residence, date of birth and citizenship and capacity in the management body); 3)

description of the type of services and activities performed within the meaning of this Law, including if they are performed using cryptomat/s;

4) data on the domain through which the virtual asset service provider performs its professional and business activity if it is performed via an electronic communication network (Internet) and

5) data and information on established business relationships with legal entities necessary for the performance of activities of a virtual asset service provider.

(3) Providers of services related to virtual assets are obliged to notify the Administration that they are carrying out activities prescribed by this Law within 30 days from the date of registration in the Central Registry of the Republic of North Macedonia, i.e. 30 days from the date of commencement of the provision of services related to virtual assets on the territory of the Republic of North Macedonia for service providers who are not registered in the Central Registry of the Republic of North Macedonia and to submit data, information and documents from reliable and independent sources in accordance with paragraph (2) of this Article.

(4) If there are doubts about the accuracy of the data submitted under paragraph (2) of this Article, the Administration may at any time request additional documents, data and information about the activities and services of the service provider related to virtual assets.

(5) Service providers are obliged to submit additional documents, data and information on the activities and services related to virtual assets referred to in paragraph (4) of this Article within ten working days from the date of receipt of the request referred to in paragraph (4) of this Article.

(6) The Minister of Finance shall prescribe the manner of keeping, the form and the content of the register referred to in paragraph (1) of this Article.

2. MEASURES AND ACTIONS FOR DETECTION AND PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Article 9

Measures and actions for the detection and prevention of money laundering and terrorist financing (hereinafter: measures and actions), which are undertaken by the entities, are:

- preparation of an assessment of the risk of money laundering and terrorist financing and its regular updating,

- introduction and implementation of programs for efficient reduction and management of the

identified risk of money laundering and terrorist financing,

- analysis of clients,
- reporting and submission of data, information and documentation to the Administration in accordance with the provisions of this Law and the by-laws adopted on its basis,
- storage, protection and keeping records of data,
- appointment of an authorized person and his/her deputy and/or establishment of a department for the prevention of money laundering and terrorist financing,
- implementation of internal control and
- other measures arising from the provisions of this Law.

Article 10

(1) The obligation to take the measures and actions provided for by this Law also exists in cases where the entities are in bankruptcy and liquidation proceedings.

(2) The obligation referred to in paragraph (1) of this Article shall be performed by the bankruptcy trustee until the completion or conclusion of the bankruptcy procedure, or by the liquidator until the completion of the liquidation procedure.

Preparing a money laundering and terrorist financing risk assessment

Article 11

(1) Entities are obliged to prepare a money laundering and terrorist financing risk assessment in order to identify, assess, understand and mitigate the risks of money laundering and terrorist financing, taking into account the risk factors relating to:

- a) the client;
- b) countries or geographical areas;
- c) products, services or transactions and
- d) distribution channels.

(2) The risk assessment referred to in paragraph (1) of this Article must be documented and appropriate to the size of the entity, the type, scope and complexity of its business activity.

(3) The entity shall be obliged to regularly update the risk assessment referred to in paragraph (1) of this Article.

(4) The entity is obliged to submit the risk assessment referred to in paragraph (1) of this Article upon request to the competent supervisory authorities referred to in Article 151 of this Law.

(5) The entity is obliged to align the risk assessment referred to in paragraph (1) of this Article with the national risk assessment, the risk factors that may indicate a potentially low or high risk, determined by the European Union, as well as with other acts, documents and information published by the competent supervisory authorities referred to in Article 151 of this Law.⁶

(6) The entity is obliged, before making significant changes in its business activities and processes that may affect the measures taken to prevent money laundering and terrorist financing, as well as when introducing a new product, service, activity or distribution channel, as well as when introducing new technologies, to conduct a risk assessment in order to determine and assess how the changes affect the exposure to the risk of money laundering and terrorist financing and is obliged to take appropriate measures to reduce and effectively manage the risk.

(7) The supervisory authorities referred to in Article 151 of this Law shall prepare guidelines for conducting a risk assessment for the entities they supervise, which shall include, but not be limited to, the risk factors that may indicate a potentially low or high risk, as determined by the European Union.

Introduction and implementation of Programs for effective reduction and management of the identified risk of money laundering and terrorist financing

Article 12

- (1) Entities are obliged to prepare and implement a Program for efficient reduction and management of the identified risk of money laundering and terrorist financing, which contains:
- objectives, scope and method of operation of the system for preventing money laundering and terrorist financing of the entity,
 - organizational structure of the entity, position of the authorized person and his deputy in the organizational structure,
 - data on the authorized person and his deputy,
 - authorizations and responsibilities of the authorized person and his deputy,
 - authorizations and responsibilities of all employees of the entity who participate in the implementation of the provisions of this Law and the by-laws adopted on its basis,
 - conclusions from the conducted risk assessment and method of managing the risk of money laundering and terrorist financing,
 - measures of client analysis and client acceptability,
 - method of recognizing unusual transactions and transactions suspected of money laundering and terrorist financing,
 - method of establishing an internal mechanism for timely and appropriate reporting,
 - method of storing data and documents,
 - method of submitting reports to the Administration,
 - a plan for continuous training of the entity's employees in the field of preventing money laundering and terrorist financing, which ensures the implementation of at least two training sessions during the year,
 - a procedure and plan for performing internal control of the implementation of measures and actions for preventing money laundering and terrorist financing appropriate to the size and type of the entity,
 - screening procedures during employment and for employees in order to ensure high standards for preventing money laundering and terrorist financing and
 - policies, procedures and internal controls for the application of restrictive measures in accordance with the law⁸
- (2) For entities under this Law that are obliged to establish a separate department in accordance with this Law, in addition to the elements referred to in paragraph (1) of this Article, the program should also contain elements for an independent audit function for testing the entire internal system for preventing money laundering and terrorist financing, depending on the size and nature of the entity's activity.
- (3) The senior management of the entity shall be obliged to adopt the program referred to in paragraph (1) of this Article, to regularly monitor and evaluate its adequacy, compliance and efficiency and, if necessary, to strengthen the measures taken by the entity.

Customer analysis

Article 13

Entities are obliged to conduct customer due diligence in the following cases:

- a) when a business relationship is established with the customer;
- b) when an occasional transaction is carried out in the amount of EUR 15,000 or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North

Macedonia, regardless of whether the transaction is carried out as a single operation or several operations that are clearly interconnected;

- c) when an occasional transaction is carried out that represents a transfer of funds, including virtual funds, in the amount of EUR 1,000 or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia;
- d) in games of chance in the case of payment and payment of winnings, as well as when purchasing or paying out chips or credits in the amount of 1,000 euros or more in denar equivalent according to the average exchange rate of the National Bank of the Republic of North Macedonia, regardless of whether the transaction is carried out as a single transaction or several transactions that are clearly interconnected and which in total reach a value of 1,000 euros or more in denar equivalent according to the average exchange rate of the National Bank of the Republic of North Macedonia;
- e) when there is doubt about the truthfulness or adequacy of previously obtained data on the identity of the client or the beneficial owner and
- f) when there is suspicion of money laundering or terrorist financing, regardless of any exception or amount of funds.

Cases when client analysis is not conducted

Article 14

(1) Entities are not obliged to implement the measures referred to in Article 15 of this Law in relation to electronic money, if the National Risk Assessment has determined a low risk of money laundering and terrorist financing and if the following conditions are met:

- 1) the payment instrument is not topped up or the total amount of transactions on a monthly basis is limited to the amount of 150 euros in denar equivalent, according to the middle exchange rate of the National Bank of the Republic of North Macedonia and can only be used in the Republic of North Macedonia;
- 2) the maximum amount of the payment instrument does not exceed 150 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia;
- 3) the payment instrument is used exclusively for the purchase of goods or services;
- 4) the payment instrument is not issued anonymously and
- 5) the issuer of the payment instrument monitors and controls the transactions or business relationships, in order to detect complex or unusual transactions or suspicious transactions.

(2) The exception from paragraph (1) of this Article shall not apply in cases of redemption of electronic money in cash or withdrawal of cash in the equivalent value of electronic money exceeding 50 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia.

(3) The provisions of paragraph (1) of this Article shall not apply in cases where there are reasons to suspect money laundering or terrorist financing.

Customer analysis measures

Article 15

(1) The analysis of the client referred to in Article 13 of this Law includes:

- a) identification of the client and confirmation of his identity using documents, data and information from reliable and independent sources, including by using electronic identification means issued within the framework of a registered scheme for electronic identification at a high level of security in accordance with the law if possible;
- b) identification of the person acting on behalf of and for the account of the client and confirming that he is authorized to do so, as well as confirming his identity using documents, data and

information from reliable and independent sources, including by using electronic identification means issued within the framework of a registered scheme for electronic identification at a high level of security in accordance with the law if possible;

c) identification of the beneficial owner of the client and taking appropriate measures to confirm his identity, using documents, data and information from reliable and independent sources in order for the entity to be confident that it knows who the beneficial owner is;

d) understanding and appropriately providing information about the purpose and intent of the business relationship and

e) ongoing monitoring of the business relationship, which consists of:

- ongoing monitoring of transactions carried out within the established business relationship in order to ensure that these transactions are consistent with the client's risk profile and business, and where necessary, determining the sources of funds, and

- ensuring that the documents and data provided within the framework of the client analysis are valid, up-to-date and relevant through regular verification thereof, especially for higher-risk clients.

(2) Where the client is a legal entity or legal arrangement, the entity shall be obliged to take measures to determine the ownership and control structure.

(3) The entity shall be obliged to provide sufficient information to ensure that it can determine the identity of the beneficiary or group of beneficiaries of the trust or other legal arrangement, at the time of payment or at the time when the beneficiary or group of beneficiaries of the property decides to exercise the granted rights.

(4) Entities are obliged to perform a risk assessment for each client and to apply each measure from the client analysis, in accordance with the client's risk profile.

(5) Entities shall be obliged to make available to the competent supervisory authorities referred to in Article 151 of this Law the documents for assessing the client's risk, in order to confirm that the determined risk of money laundering and terrorist financing is appropriate and that the scope of the measures taken is in accordance with the client's risk.

(6) Entities are obliged to apply customer and existing customer due diligence measures based on relevance, significance, risk and to implement them within an appropriate time period and taking into account previous activities undertaken within the framework of customer due diligence and the adequacy of the data obtained.

Identification and verification of identity

Article 16

(1) Entities are obliged to carry out the identification and verification of the identity of the client, the person acting on behalf of and for the account of the client, the agent and the beneficial owner before establishing a business relationship or before carrying out an occasional transaction.

(2) By way of exception to paragraph (1) of this Article, entities may verify the identity of the client, the person acting on behalf of and for the account of the client, the agent or the beneficial owner during the establishment of the business relationship, in order not to disrupt the conduct of the business relationship and when there is a low risk of money laundering and terrorist financing.

(3) In matters related to life insurance, it is permissible to verify the identity of the client, the person acting in the name and on behalf of the client, the agent or the beneficial owner of the policy, after the business relationship has been established. In this case, the identity verification should be carried out before or during the payment of the policy or before or when the beneficiary intends to exercise the rights arising from the policy.

(4) The entity has an obligation to identify the beneficiary of the life insurance policy where the name of the beneficiary is known and stated, but also where the name of the beneficiary in the life insurance policy is not stated, but his relationship with the insured is defined.

(5) The entity has an obligation to identify the beneficiary of the life insurance policy as a relevant risk factor when conducting the risk assessment, i.e. it is necessary to introduce enhanced monitoring by identifying and verifying the identity of the beneficial owner of the insurance beneficiary at the time of payment of the damage in cases where the entity determines that the beneficiary who is a legal entity or legal arrangement is high risk.

Identifying and verifying the client's identity

Article 17

(1) When the client is a natural person, his identity shall be identified and confirmed by submitting an original and valid identification document issued by a competent authority, and if possible, by using electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security in accordance with the law.

(2) From the document referred to in paragraph (1) of this Article, and if possible also from the identification data of persons using electronic identification means, the name, surname, date and place of birth, place and address of residence or place of stay, unique personal identification number or identification number and number of the valid identification document or serial number of the electronic identification means, the authority that issued the document and the date of validity, i.e. the name of the issuer of the electronic identification means and the period of validity of the electronic identification means shall be determined.

(3) When the client is a legal entity, its identity is confirmed by a registration document in original or a copy certified by a notary, issued by a competent authority of the country in which the legal entity is registered, which must not be older than six months, including by using electronic identification means issued within the framework of a registered electronic identification scheme with a high level of security in accordance with the law, if possible. The registration or establishment document is submitted in paper and/or electronic form. Registration documents issued by a competent authority of a foreign country should be translated into Macedonian by an authorized court translator.

(4) The document referred to in paragraph (3) of this Article, and if possible also from the identification data of legal entities using electronic identification means, shall determine the name, legal form, registered office, tax number or other registration number of the legal entity, the legal representative, the management body or the persons authorized to establish a business relationship, i.e. perform a transaction on behalf of the client, and in accordance with the risk of the legal entity, a history document issued by a competent authority may also be used in the event of changes to this data.⁹

(5) When the client is a legal arrangement, it is identified and its identity is confirmed by an act establishing the legal arrangement in original or a copy certified by a notary, which determines the form, seat, tax number or other registration number of the legal arrangement, the founder(s), the trustee(s), the beneficiary or group of beneficiaries of the legal arrangement, the legal representative, the management body and the persons authorized to establish a business relationship, i.e. perform a transaction on behalf of the client.

(6) Entities shall mandatorily retain a copy in paper and/or electronic form of the documents referred to in paragraphs (1), (3) and (5) of this Article, as well as electronic records of the data referred to in paragraphs (1), (3) and (5) of this Article for the identification of persons who have used electronic identification means provided through the use of electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security, while applying technical and organizational measures in accordance with the regulations on the protection of personal data in accordance with the law.

(7) Entities may also request other data, information and documents from the client and/or reliable and independent sources to confirm the client's identity.

(8) Identification and verification of the identity of the client using electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security in accordance with this Law is not permitted:

- 1) for products, services, transactions or distribution channels for which a high risk of money laundering and terrorist financing has been determined in accordance with the provisions of this Law;
- 2) if the client is a minor natural person;
- 3) if the client is a natural person or legal entity that is a citizen or has a place of residence or residence, i.e. a registered office in a high-risk country in accordance with the provisions of this Law;
- 4) if the entity determines that the electronic identification means is not valid, and the issuer of the registered electronic identification scheme has not yet suspended it;
- 5) if the electronic identification means does not contain the necessary data in accordance with this Article.

Identification and verification of the person acting on behalf of and for the account of the client

Article 18

(1) Entities are obliged to determine whether the person acts in the name and on behalf of the client.

(2) In the cases referred to in paragraph (1) of this Article, the entities are obliged to identify and confirm the identity of the person acting on behalf and for the account of the client, the client or the holder of the rights and the power of attorney, on the basis of documents, data and information from reliable and independent sources, and if possible, by using electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security in accordance with the law.

(3) Entities are obliged to provide the power of attorney referred to in paragraph (2) of this Article in original or a copy certified by a notary.

(4) Entities shall mandatorily retain a copy in paper and/or electronic form of the documents referred to in paragraphs (2) and (3) of this Article, as well as electronic records of the data referred to in paragraph (2) of this Article for the identification of persons who have used electronic identification means provided through the use of electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security, while applying technical and organizational measures in accordance with the regulations on the protection of personal data.

(5) The documents referred to in paragraphs (2) and (3) of this Article, issued or certified by a competent authority in a foreign country, should be translated into Macedonian by an authorized court translator.

Identifying and verifying the identity of the rightful owner

Article 19

(1) Entities are obliged to identify the beneficial owner of their client and to take appropriate measures to confirm the identity of the beneficial owner based on data and information from reliable and independent sources, with which they are convinced and know who the beneficial owner of the client is to an extent appropriate to the risk assessment performed.

- (2) Entities shall provide data on the beneficial owner from the original or certified documentation from a commercial, court or other public register, which must not be older than six months.
- (3) Subjects, in addition to the measures referred to in paragraphs (1) and (2) of this Article, are obliged to check the data on the beneficial owner from the register of beneficial owners, and may not rely exclusively on the data entered in this register.
- (4) In the event that the trustee/manager of the trust, i.e. the person performing similar functions in the legal arrangement, acts in the name and on behalf of the trust or legal arrangement, when establishing a business relationship or when carrying out a transaction, the entity is obliged to provide information supported by documents establishing that the person acts in that capacity, to provide information on the identity of the persons specified in Article 22 of this Law, as well as to provide data on the name, address, legal form of the trust or other legal arrangement.¹⁰
- (5) In the event that the trustee/manager of the trust, i.e. the person performing similar functions in the legal arrangement acts in the name and on behalf of the trust or legal arrangement, establishes a business relationship or carries out a transaction with an entity referred to in Article 5 of this Law, he shall be obliged to provide information supported by documents informing him that he is acting in that capacity, as well as to provide information on the identity of the persons specified in Article 22 of this Law.
- (6) Entities shall mandatorily retain a copy in paper and/or electronic form of the documents and information referred to in paragraphs (1), (2), (3), (4) and (5) of this Article, while applying technical and organizational measures in accordance with the regulations on personal data protection.
- (7) If entities cannot obtain all data on the beneficial owner of the client from the commercial, court or other public register or the register of beneficial owners, they should provide the necessary data by checking the original or certified documents and business records submitted by the legal representative of the client or a person authorized by him.
- (8) If the client is not subject to registration in an appropriate register and the entities cannot obtain the necessary data on the beneficial owner in the manner described in paragraphs (2), (3), (4), (6) and (7) of this Article, the entities are obliged to provide the data directly with a written statement under full moral and material responsibility certified by a notary of the legal representative or a person authorized by him before establishing a business relationship or before carrying out a transaction.
- (9) If, after determining the beneficial owner, the entities have doubts regarding the reliability of the submitted data or the reliability of the documents or other business documentation, they are obliged to request a written statement from the legal representative under full moral and material responsibility, certified by a notary or a person authorized by him, before establishing a business relationship or before carrying out a transaction.
- (10) In the cases referred to in paragraphs (7), (8) and (9) of this Article, the entities shall be obliged to apply one or more measures for enhanced analysis in accordance with the provisions of this Law.
- (11) The Director of the Administration shall, by means of instructions, determine the manner of identifying the beneficial owner.

Beneficial owner of a legal entity

Article 20

- (1) The beneficial owner of a legal entity is:
- 1) The natural person(s) who ultimately owns or controls the legal entity through direct and/or indirect ownership of a sufficient percentage of the shares, i.e. shares or voting rights, as well as through other ownership interest in that legal entity, including through bearer shares or other form

of control.

2) The natural person(s) who has a high management position in the legal entity, i.e. who is authorized by law and internal acts to manage and is responsible for the operations of the legal entity.

(2) An indicator of direct ownership referred to in paragraph (1) item 1) of this Article is the ownership of over 25% of the shares, voting rights or other rights in the legal entity or the ownership of 25% plus one share.

(3) An indicator of indirect ownership referred to in paragraph (1) item 1) of this Article is the ownership or control of a natural person (persons) over one or more legal entities that individually or jointly hold over 25% of the shares or 25% plus one share.

(4) If, by applying paragraph (1) point 1) of this Article, no natural person(s) can be determined as the beneficial owner(s) or if the entity is not sure that the natural person(s) identified in accordance with paragraph (1) point 1) of this Article is/are the beneficial owner(s), in that case the person(s) identified by applying paragraph (1) point (2) of this Article shall be considered the beneficial owner(s).

(5) In the cases prescribed in paragraph (4) of this Article, the entity is obliged to keep the data, i.e. the records of all measures and activities undertaken in the process of identifying the true owner.

Beneficial owner of other legal entities **Article 21**

The beneficial owner of domestic and foreign associations and their unions, institutions, chambers, trade unions, political parties, cooperatives, religious communities, communities of owners or other organizations in which participation in management based on ownership share in the capital cannot be determined is considered any natural person who is authorized to represent them or the natural person who has a controlling position in the management of the organization's property.

Beneficial owner of a trust or other legal arrangement **Article 22**

(1) The beneficial owner of a trust is any natural person who is:

- 1) the settlor;
- 2) the trustee;
- 3) the protector (if any);
- 4) a beneficiary or group of beneficiaries, provided that the future beneficiaries are identified or can be identified;
- 5) another natural person who, through direct or indirect ownership or otherwise, exercises control over the trust.

(2) The beneficial owner of a legal arrangement is a person(s) who performs the same or similar function(s) as those referred to in paragraph (1) of this Article.

(3) The beneficial owner of a foundation is a person(s) who performs the same or similar functions as those referred to in paragraph (1) of this Article.

Beneficial owner of a sole proprietorship or independent business entity **Article 23**

The beneficial owner of a sole proprietorship or independent business operator is the natural person registered to perform the activity and at the same time is the sole authorized representative.

Beneficial owner of budget users

Article 24

The beneficial owner of a budget user is the head of the budget user.

Beneficial owner of a state-owned legal entity Article 25

The beneficial owner of a state-owned legal entity is the person who manages or directs the management body of the state-owned legal entity.

Beneficial owner of a legal entity that is in bankruptcy or liquidation proceedings Article 26

The actual owner of a legal entity that is in bankruptcy or liquidation proceedings is the bankruptcy trustee, i.e. the liquidator, until the completion of the bankruptcy or liquidation proceedings.

Exceptions regarding identification of the beneficial owner Article 27

The entity does not have to identify and confirm the identity of the beneficial owner if the client is a legal entity whose securities are listed on a domestic or foreign stock exchange from countries that meet international standards for the prevention of money laundering and terrorist financing and the data on the beneficial owners is transparent and publicly available.

Obligation to provide and store data on the beneficial owner Article 28

(1) The obligation to provide and store data and documents on the beneficial owner shall be imposed on the entities registered in the registers maintained by the Central Registry of the Republic of North Macedonia and trusts and other legal arrangements established in accordance with the law of a foreign country (hereinafter referred to as: legal entities), namely:

- 1) trade companies, sole proprietors, independent business operators, subsidiaries and branches of foreign trade companies and foreign sole proprietors;
- 2) associations, unions, foundations, chambers, trade unions, political parties, cooperatives, religious communities, communities of owners, representative offices of foreign trade companies or other organizations;
- 3) notaries, lawyers and other persons exercising public authorizations;
- 4) budget users;
- 5) state-owned legal entities;
- 6) legal entities in bankruptcy or liquidation proceedings and
- 7) Trusts and legal arrangements if:
 - a) the trustee or a person who performs activities equal or similar to those referred to in Article 22 of this Law and has a registered office or residence in the Republic of North Macedonia or 11
 - b) the trustee or a person who performs activities equal to or similar to those referred to in Article 22 of this Law and does not have a registered office or residence in the Republic of North Macedonia, and on behalf of the trust or legal arrangement acquires property or establishes

business relations with the entities prescribed by this Law or 12

c) have received a unique tax number (UTC) in the Republic of North Macedonia in accordance with the law.

(2) The legal entities referred to in paragraph (1), points 1), 2), 3) and 7) of this Article shall be obliged to provide and keep appropriate, accurate and up-to-date data and documents on:

1) the beneficial owner(s), namely:

a) name and surname;

b) address of residence, i.e. place of stay;

c) day, month and year of birth;

d) unique identification number or other identification number and data on the type, number, issuer, country and date of issue of the identification document;

e) citizenship and

f) data on the type and scope of beneficial ownership.

2) the legal form and ownership structure, and for commercial companies and data on shares, deposits or other forms of participation in the ownership of the company.

(3) The legal entities referred to in paragraph (1) items 4), 5) and 6) of this Article are obliged to possess and keep appropriate, accurate and up-to-date data referred to in paragraph (2) item 1) of this Article.

(4) The persons who are the beneficial owners are obliged to submit all data and documents referred to in paragraph (2) of this Article to the legal entities and to the trustee/manager or to a person who performs similar activities in the legal arrangement.

(5) The legal entities referred to in paragraph (1) shall be obliged to provide information and documents about their owner and the beneficial owner of the entities referred to in Article 5 of this Law for the purpose of conducting customer due diligence in accordance with this Law.

(6) The legal entities referred to in paragraph (1) shall be obliged to keep the data on the beneficial owner referred to in this Article within ten years from the date of establishment of the legal entity, i.e. from the date of change of the beneficial owner of the legal entity.

(7) A manager/trustee of a trust or similar legal arrangement, i.e. a person acting in the name and on behalf of a trust or similar legal arrangement prescribed by this Law, is obliged to keep data and information on the beneficial owner referred to in Article 22 of this Law, within 10 years from the moment when he ceases to carry out activities in the name and on behalf of the trust or legal arrangement.

Register of beneficial owners Article 29

(1) In order to ensure transparency of the ownership structure of legal entities, a register of beneficial owners shall be established, which shall contain information and data on the beneficial owners in accordance with this Law (hereinafter referred to as: register).

(2) The Central Registry of the Republic of North Macedonia (hereinafter referred to as: Registry Administrator) shall establish, maintain, and manage the registry in electronic form.

Applicants Article 30

(1) The authorized person for representation and advocacy of the legal entity referred to in Article 28 paragraph (1) of this Law is obliged to enter the data in the register.

(2) Legal entities may, through the registry administrator's system, authorize another person to enter data on their beneficial owners, as well as data on changes in beneficial owners, in the registry on their behalf.

(3) The legal entities referred to in Article 28 paragraph (1) of this Law are responsible for the accuracy, adequacy and up-to-dateness of the data entered in the register.

(4) The registration agent or the registry administrator in the registration procedure is obliged to inform the legal entity about the obligation for mandatory registration of the data on the beneficial owner.

Entering data into the register

Article 31

(1) Trade companies, subsidiaries and branches of foreign trade companies and foreign sole proprietors, associations, unions, foundations, chambers, trade unions, political parties, cooperatives, religious communities, communities of owners, representative offices of foreign trade companies or other organizations shall enter the data on their beneficial owners in the register within 15 days of the entry of the business entity in the trade register and in the register of other legal entities within 15 days of the change in the data on the beneficial owner.

(2) Trusts and legal arrangements shall enter the data on their beneficial owner(s) in the register within 15 days from the date on which the trustee/manager or a person performing activities equal or similar to those described in Article 22 of this Law acquired a registered office or residence in the Republic of North Macedonia, i.e. on behalf of the trust or legal arrangement acquired property or established business relations with the entities prescribed by this Law or from the date on which he received a unique tax number (UTN) in the Republic of North Macedonia in accordance with the law. Trusts and legal arrangements shall be obliged to enter the data on their beneficial owner(s) in the register within 15 days from the date of change in the data on the beneficial owner in accordance with Article 22 of this Law.¹³

(3) The following data shall be recorded in the register:

1) data on the legal entity, with the exception of legal arrangements: name, registered office, EMBS and tax number, date of establishment and deletion of the business entity, which shall be taken over and recorded ex officio and automatically from the single trade register and the register of other legal entities;

2) data on legal arrangement: name, date and place of establishment, tax number or other identification number and country under whose law it is established;

3) data on the beneficial owner: name and surname (personal name), unique identification number or other identification number, address of residence, i.e. place of stay, date of birth and citizenship, which are taken ex officio and using electronic means from the Central Population Register, by entering the citizen's unique identification number, for citizens of the Republic of North Macedonia living in the country or abroad, as well as foreigners with regular residence in the Republic of North Macedonia for more than one year or are entered by the applicant for a foreigner in Latin script, as recorded in the valid identification document;

4) data on the ownership of the beneficial owner and

5) data on the day on which the person acquired the status of beneficial owner in accordance with this Law.

(4) Foreign citizens with regular residence in the Republic of North Macedonia for more than one year, in addition to the data referred to in paragraph (3) item 3) of this Article, shall also enter data on a foreign identification number, foreign address (address of permanent residence-residence) and country of permanent residence in accordance with the valid identification document.

(5) The registry administrator shall maintain and manage the registry in such a way that:

- in addition to the latest status of the beneficial owner data, all previous entries, data changes and deletions are also kept according to the time and type of event, and
- the data in the registry are available for ten years after the deletion of the legal entity from the competent registry.

(6) Data entry shall be carried out electronically, through the web portal of the registry administrator, free of charge, within the legally prescribed deadlines, by applying technical and organizational measures in accordance with the regulations on personal data protection.

(7) If the applicant has filed an application with the register of beneficial owners that contains obvious technical errors, he or she may correct it within three days from the date of filing the application.

(8) In case of unavailability of the Central Population Register system, as well as in the case when the specific EMBG is not recorded within it, the data on: personal name (first name and last name), unique identification number or other identification number, address of residence, i.e. place of residence, date of birth, citizenship for citizens of the Republic of North Macedonia living in the country or abroad, as well as foreign citizens with regular residence in the Republic of North Macedonia for longer than one year, shall be entered manually by the applicant.

(9) The Minister of Finance shall prescribe the manner of entering, reporting, correcting and deleting data from the register, the manner of expressing the amount of the share (indicator for determining ownership), the manner of searching and using it, the manner of maintenance and administration and the technical requirements (needs) for establishing the register.

Article 32

(1) In the event that the entity, through a direct check in the electronic system of the Registry, determines that the data and information about the beneficial owner of the legal entity referred to in Article 28 of this Law has not been recorded or updated in the register of beneficial owners in accordance with this Law, the entity is obliged to postpone the establishment of the business relationship, to postpone the transaction within the framework of an established business relationship or to postpone the execution of a transaction until the data and information are entered into the register.

(2) In the cases referred to in paragraph (1) of this Article and if the entity establishes discrepancies between the information on the beneficial owner(s) recorded, i.e. updated in the register and the information on the beneficial owner available to them on the basis of the analysis conducted on the client in accordance with this Law, the entity shall immediately notify the Administration electronically. If such method of submission is impossible for technical reasons, the entities shall inform the Administration in writing.

(3) The Director of the Administration shall determine by instruction the manner of submitting the information referred to in paragraph (2) of this Article.

Access to beneficial ownership data

Article 33

(1) The data recorded in the register shall be directly and electronically accessible to:

- 1) the Administration;
- 2) the Courts;
- 3) the authorities in accordance with Articles 130 paragraph (1) and 151 paragraph (1) of this Law;
- 4) the entities referred to in Article 5 of this Law;
- 5) other legal and natural persons.

(2) The competent authorities referred to in paragraph (1) items 1), 2) and 3) of this Article may provide all data contained in the register free of charge, in a timely manner, in accordance with the

Law on the Central Register, as well as forward them to the competent authorities and financial intelligence units of other countries in accordance with their competencies determined by law.

(3) The entities referred to in paragraph (1) item 4) of this Article shall have timely access to all data contained in the register in accordance with the Law on the Central Register and shall use them for the exercise of their powers in accordance with this Law.

(4) The data from the register on name and surname, month and year of birth, citizenship, country of residence, ownership interest or other form and type of ownership or control, in the form of information, and in accordance with the Tariff of the registry administrator, are publicly available to the legal and natural persons referred to in paragraph (1) item 5) of this Article.

Issuance of data on beneficial owners

Article 34

(1) The information on the beneficial owner for the entities subject to registration in the register in accordance with this Law shall be issued in accordance with the latest data entered in the Central Population Register and the register of beneficial owners on the day of its issuance. In case of unavailability of the Central Population Register system at the time of issuance of the information, the data on the beneficial owner for the entities subject to registration in the register in accordance with this Law shall be issued in accordance with the latest data entered in the register of beneficial owners.

(2) The information on the beneficial owner of the sole proprietor, independent business operators and persons exercising public authorizations, as well as budget users, legal entities in full state ownership and legal entities in bankruptcy and liquidation proceedings shall be issued in accordance with the latest data entered in the single trade register and the register of other legal entities and the register of budget users under the jurisdiction of the Ministry of Finance.

Checking the data in the registry

Article 35

(1) The registry administrator shall check the data in the registry and determine whether the legal entities referred to in Article 28 paragraph (1) of this Law have entered the data referred to in Article 31 of this Law, the change of such data within the deadline and in a manner prescribed in accordance with the regulation referred to in Article 31 of this Law.

(2) The registry administrator shall immediately inform the Administration electronically about the legal entities referred to in Article 28 paragraph (1) of this Law that have not entered the data referred to in Article 31 of this Law and have not entered the change to such data in the manner and within the deadline prescribed in accordance with the regulation referred to in Article 31 of this Law.

Processing of data in the registry

Article 36

(1) The Administration shall continuously process the data entered in the register under Article 31 of this Law by the legal entities under Article 28 paragraph (1) of this Law.

(2) For the purposes of processing the data referred to in paragraph (1) of this Article, the Administration shall also use software solutions, which shall comply with the regulations on personal data protection.

(3) The information from the processing of data on the ownership structure, through the register of beneficial owners, is available to the entities under this law for use for the purposes of implementing measures and actions to prevent money laundering and terrorist financing.

Continuous monitoring of a business relationship

Article 37

- (1) The entity is obliged to carefully monitor the business activities and transactions carried out within the framework of the business relationship with the client, in order to confirm that they are in accordance with the purpose and intent of the business relationship, the client's risk profile, his financial situation and his sources of financing.
- (2) The entity is obliged to regularly check and update the documents and data on the clients, the beneficial owners and the risk profile of the clients with whom it has established a business relationship.
- (3) The entity shall ensure that the scope and frequency of the implementation of the measures referred to in paragraph (2) of this Article are in accordance with the analysis and assessment of the risk referred to in Article 11 of this Law and that they are aligned with the risk of money laundering and terrorist financing to which the entity is exposed in the course of carrying out a specific business activity or transaction, i.e. within the framework of the business relationship with the client.

Simplified customer analysis

Article 38

- (1) Entities may apply simplified customer due diligence measures when, in accordance with the provisions of Article 11 of this Law, they have determined that there is a low risk of money laundering and/or terrorist financing.
- (2) When deciding on the application of simplified customer due diligence measures, entities shall also take into account the results of the national risk assessment.
- (3) Simplified customer due diligence measures may include:
 - verifying the identity of the customer or beneficial owner upon establishment of the business relationship,
 - reducing the frequency of updating customer documents and data, and/or
 - reducing the level of monitoring of the customer's business relationship and transactions.
- (4) Entities shall be obliged to provide appropriate documentation on the basis of which it will be possible to confirm that the application of simplified customer due diligence is permitted and that the simplified customer due diligence measures are appropriate to the risk, as well as to make that documentation available to the supervisory authorities referred to in Article 151 of this Law.
- (5) Simplified customer due diligence is not permitted when there is a suspicion of money laundering or terrorist financing in relation to the customer, transaction, business relationship or property, specific scenarios of high risk of money laundering or terrorist financing apply or in cases of complex and unusual transactions.
- (6) Entities shall be obliged to implement the measures referred to in paragraph (3) line 3 of this Article to a extent that will enable them to detect complex and unusual or suspicious transactions.

Enhanced customer analysis

Article 39

- (1) In cases where there is a high risk and medium-high risk of money laundering or terrorist financing, determined in accordance with Article 11 of this Law or based on a national risk assessment of this Law or in case of suspicion of money laundering and/or terrorist financing, except in cases prescribed by Articles 40, 41, 42, 43, 44 and 45 of this Law, the entity is obliged to

undertake all measures for enhanced customer due diligence for appropriate risk management, including:

- providing additional data on the customer and the beneficial owner(s),
- frequent updating of documents and data on the customer,
- providing additional data on the nature of the customer's business relationships and transactions,
- providing additional data on the source of funds and the source of the customer's wealth,
- providing information on the reason for the planned or executed transactions,
- providing approval from senior management for the establishment of new or continuation of business relationships and
- enhanced monitoring of business relationships.

(2) The entity is obliged to document the implementation of the enhanced analysis measures referred to in paragraph (1) of this Article and to make that documentation available to the supervisory authorities referred to in Article 151 of this Law.

Correspondent relationship Article 40

(1) When establishing cross-border correspondent relationships, the financial institution shall undertake the following enhanced due diligence measures:

- a) to collect sufficient data on the correspondent financial institution to fully determine its business and, from publicly available information, to determine its reputation, as well as the quality of supervision, including whether it has been the subject of an investigation for money laundering or terrorist financing or other supervisory measures;
- b) to assess the procedures and control mechanisms for preventing money laundering and terrorist financing of the correspondent financial institution;
- c) to obtain approval from senior management before establishing a new correspondent relationship;
- d) to determine and precisely prescribe the mutual responsibilities arising from the correspondent relationship and
- e) to determine whether the correspondent financial institution performs the client analysis referred to in this Law on persons who have direct access to its correspondent accounts with financial institutions in the Republic of North Macedonia, at least to the extent and in the manner specified in this Law, as well as to determine whether the correspondent financial institution is willing to provide the data for identifying and confirming the identity of the client of the foreign bank or other financial institution and its beneficial owner and to submit them to the bank or other financial institution upon its request.

(2) The measures referred to in paragraph (1) of this Article shall also apply in situations where financial institutions establish correspondent relationships with service providers related to virtual assets, as well as in situations where service providers with virtual assets establish correspondent relationships with each other.

A customer who is not physically present Article 41

When the client, as well as the person acting on behalf of and for the account of the client, is not physically present for identification purposes and if their identity cannot be established using electronic identification means issued within the framework of a registered electronic identification scheme at a high level of security in accordance with the law, the entity should take one or more of the following enhanced due diligence measures:

- a) to establish the identity of the client with additional documents, data or information;
- b) to take additional measures to confirm the provided documents or to request that the documents be confirmed by a financial institution from the Republic of North Macedonia, from a Member State of the European Union or from a country in which the regulations provide for approximately the same criteria and standards for the prevention of money laundering and the financing of terrorism as the requirements provided for in this Law and
- c) to make the first payment through the account in the name of the client opened in a financial institution in a country that meets international standards for the prevention of money laundering and the financing of terrorism and that implements at least the same customer due diligence measures as prescribed in this Law.

Client - public office holder

Article 42

(1) When the entity carries out transactions or establishes a business relationship with a client - a public office holder, the entity is obliged, in addition to the measures set out in Article 15 of this Law, to take the following enhanced due diligence measures:

- a) establish risk management systems to determine whether the client or the beneficial owner is a public office holder, including to provide his/her declaration;
- b) obtain approval from senior management before establishing a business relationship with a client - a public office holder and/or the beneficial owner, as well as to provide consent for the continuation of the business relationship with an existing client - a public office holder and/or the beneficial owner who has in the meantime become a public office holder;
- c) take appropriate measures to determine the source of wealth and the source of funds of the client and the beneficial owner(s) identified as public office holders and
- d) conduct continuous enhanced monitoring of the business relationship.

(2) The entity shall be obliged to take measures to determine whether the beneficiary and/or the beneficial owner of the life insurance and other investment-related insurance is a public office holder.

(3) In the cases referred to in paragraph (2) of this Article, the entity shall be obliged to notify senior management prior to the payment of the insurance policy premium and to review and determine in detail the entire business relationship with the client, as well as to determine the need to submit a report in accordance with Article 65 of this Law.

(4) International organizations accredited in the Republic of North Macedonia shall publish on their official websites data on directors, deputy directors, board members and other equivalent positions in the international organization.

(5) The Administration shall maintain an updated list of positions in the Republic of North Macedonia that are considered public positions in accordance with this Law and publish it on its website.

High-risk countries

Article 43

(1) When a business relationship or transaction involves a high-risk country, the entity is obliged to take the following measures when establishing a business relationship or executing a transaction:

- 1) providing additional data on the client and the beneficial owner(s);
- 2) providing additional data on the purpose and nature of the business relationship;
- 3) providing additional data on the source of funds and the source of wealth of the client and the beneficial owner(s);

- 4) providing data on the reason for the planned or executed transaction;
 - 5) providing approval from senior management for establishing new business relationships or continuing existing business relationships and
 - 6) intensively monitoring the business relationship with increased and frequent controls, as well as with further analysis of certain transaction samples.
- (2) When a business relationship or transaction involves a high-risk country, the entity shall, where applicable, require that the first payment be made through an account in the name of the client opened in a financial institution in a country that meets international standards for the prevention of money laundering and terrorist financing and that implements at least the same customer due diligence measures as prescribed in this Law.¹⁴
- (3) In addition to the measures referred to in paragraphs (1) and (2) of this Article, the entity shall be obliged to take one or more measures to reduce the risk, namely:
- 1) to take additional measures of enhanced analysis;
 - 2) to introduce additional mechanisms for reporting on the client's transactions or
 - 3) to limit the establishment of business relations or the performance of transactions with natural or legal persons from high-risk countries.
- (4) The Administration shall regularly, and at least twice a year, publish a list of high-risk countries for the purpose of implementing the measures referred to in paragraphs (1) and (2) of this Article on its official website based on the public announcements on identified high-risk countries published by the FATF, the decisions adopted at the level of the European Union on identified high-risk countries with strategic deficiencies and high-risk countries identified in accordance with the national risk assessment.
- (5) Upon the proposal of the Council for Combating Money Laundering and Terrorism Financing, the Government shall adopt a decision to introduce measures towards high-risk countries, as follows:
- prohibition on establishing a subsidiary, branch or representative office of entities from a high-risk country,
 - prohibition on establishing a subsidiary, branch or representative office of entities in a high-risk country,
 - increase in supervisory controls or increase in requirements for independent audits of a subsidiary, branch or representative office of entities from a high-risk country,
 - increase in requirements for independent audits of financial groups of subsidiaries or branches in a high-risk country,
 - request from financial institutions to check and supplement or, if necessary, terminate the correspondent relationship with the correspondent financial institution in a high-risk country.
- (6) The proposal referred to in paragraph (5) of this Article shall be prepared by the Council at the request of the FATF or on the basis of assessment reports or other reports from international organizations involved in the fight against money laundering and terrorist financing and for the purposes of preventing money laundering and terrorist financing.

Non-profit organizations

Article 44

Entities are required to undertake enhanced due diligence measures in relation to business relationships and transactions with non-profit organisations that pose a higher risk identified according to the national risk assessment as well as non-profit organisations that pose a higher risk according to the risk assessment by the entity and which include:

- 1) providing additional data on the client and the beneficial owners;
- 2) frequently updating documents and data on the client;

- 3) providing additional data on the nature of the client's business relationships and transactions and the specific objectives of the non-profit organisations;
- 4) providing additional data on the source of funds and the source of the client's assets and additional data on the beneficiaries who receive the non-profit organisation's funds;
- 5) providing information on the reason for the planned or executed transactions and
- 6) enhanced monitoring of business relationships.

Complex and unusual transactions

Article 45

(1) The entity shall investigate, to the extent reasonably possible, the background and purpose of all transactions that meet at least one of the following criteria:

- 1) the transaction is complex;
- 2) the transaction is unusually large;
- 3) the transaction is carried out in an unusual manner;
- 4) the transaction has no apparent economic justification or legal purpose and/or
- 5) deviates from the usual or expected business operations of the customer.

(2) In the cases referred to in paragraph (1) of this Article, entities are obliged to increase the level and nature of monitoring of the business relationship with the client, in order to determine whether those transactions or activities have suspicious elements.

(3) In the cases referred to in paragraphs (1) and (2) of this Article, the entity is obliged to conduct an analysis in written or electronic form and to determine the need to submit a report to the Administration in accordance with Article 65 of this Law.

(4) In relation to the transactions referred to in paragraph (1) of this Article, the entity shall be obliged to keep the analysis referred to in paragraph (3) of this Article and make it available upon request to the supervisory authorities referred to in Article 151 of this Law.

Refusal of a business relationship and transaction

Article 46

(1) When it cannot implement the customer due diligence measures under this Law, the entity is obliged to:

- 1) refuse to establish a business relationship with the customer;
- 2) terminate the business relationship with the customer;
- 3) not carry out an occasional transaction and/or
- 4) not carry out a transaction within the framework of an established business relationship, until the moment of implementation of the customer due diligence measures.

(2) In the cases referred to in paragraph (1) items 1) and 2) of this Article, the entity shall be obliged to notify the Administration electronically. If this method of submission is impossible for technical reasons, the entities shall submit the notification in writing.

(3) In the cases referred to in paragraph (1) of this Article, the entity shall be obliged to conduct a written analysis and determine the need to submit a report to the Administration in accordance with Article 65 of this Law.

(4) The entity is obliged to keep the analysis referred to in paragraph (3) of this Article for ten years from its preparation and to make it available upon request to the supervisory authorities referred to in Article 151 of this Law.

Exception from the implementation of customer due diligence measures

Article 47

(1) In the event that the entity suspects money laundering or terrorist financing and has a reasonable belief that the implementation of customer due diligence measures will lead to the client being informed of the measures being taken, the entity may not conduct the entire customer due diligence process, but may immediately submit a report to the Authority in accordance with Article 65 of this Law and explain the reasons for which it acted in accordance with this Article.

(2) Entities are obliged to explain in writing the reasons for acting in accordance with paragraph (1) of this Article and to make the data available upon request to the supervisory authorities referred to in Article 151 of this Law.

Application of measures and actions to prevent money laundering and terrorist financing by subsidiaries and branches of the entity

Article 48

(1) An entity that has its subsidiaries or branches in another country should ensure the implementation of measures for the prevention of money laundering and terrorist financing in the subsidiaries or branches.

(2) In the event that the regulations of the country in which the subsidiary or branch referred to in paragraph (1) of this Article is established do not allow the application of the measures referred to in paragraph (1) of this Article, the entity shall immediately inform the relevant supervisory authority referred to in Article 151 of this Law.

(3) Entities that are part of a group, including a financial group, are obliged to implement a Program for effective reduction and management of the identified risk of money laundering and terrorist financing of the group, i.e. the financial group, in all subsidiaries and branches that are part of the group, i.e. the financial group.

(4) The program referred to in paragraph (3) of this Article shall contain:

- objectives, scope and method of operation of the system for preventing money laundering and terrorist financing of the entity at the level of a financial group,
- organizational structure of the entity, position of the authorized person and his deputy in the organizational structure,
- data on the authorized person and his deputy,
- authorizations and responsibilities of the authorized person and his deputy,
- authorizations and responsibilities of all employees of the entity who participate in the implementation of the provisions of this Law and the by-laws adopted on the basis thereof,
- conclusions from the conducted risk assessment and method of managing the risk of money laundering and terrorist financing,
- measures of client analysis and client acceptability,
- method of recognizing unusual transactions and transactions suspected of money laundering and terrorist financing,
- method of establishing an internal mechanism for timely and appropriate reporting,
- method of storing data and documents,
- method of submitting reports to the Administration,
- plan for continuous training of the employees of the entity in the field on the prevention of money laundering and terrorist financing which ensures the implementation of at least two trainings during the year,
- a procedure and plan for performing internal control of the implementation of measures and actions for the prevention of money laundering and terrorist financing appropriate to the size and type of the entity,
- screening procedures during employment and for employees in order to ensure high standards for

the prevention of money laundering and terrorist financing,

- policies, procedures and internal controls for the application of restrictive measures in accordance with the law,
- policies and procedures for the exchange of information for the purposes of customer analysis and the management of money laundering and terrorist financing risks,
- ensuring compliance at the group level in the application of measures for the prevention of money laundering and terrorist financing, in relation to information on customers, accounts and transactions by branches and subsidiaries, for the purposes of preventing money laundering and terrorist financing and
- application of appropriate confidentiality safeguards when using the exchanged data and information.

(5) An entity that has subsidiaries or branches in another country where the minimum requirements for preventing money laundering and terrorist financing are less stringent than the obligations prescribed by this Law, the entity shall implement the obligations for preventing money laundering and terrorist financing in the subsidiaries and branches in accordance with this Law, to the extent permitted by the regulations of the other country.

(6) If the regulations of the other country where the entity has subsidiaries or branches do not allow the implementation of the measures and actions for the prevention of money laundering or terrorist financing prescribed by this Law, the entity is obliged to apply additional measures for the effective management of the risk of money laundering or terrorist financing and to immediately notify the supervisory authority referred to in Article 151 of this Law.

(7) If the measures referred to in paragraph (6) of this Article are not sufficient, unless otherwise provided by another law, the competent supervisory authorities referred to in Article 151 of this Law may carry out additional supervisory actions in accordance with their competences determined by law, including requesting the entity not to establish or terminate business relationships and not to carry out transactions and, where necessary, requesting the entity to close its subsidiaries or branches in that country.

Entrusting client analysis responsibilities to third parties

Article 49

(1) In cases where the entities implement the measures referred to in Article 15 of this Law, they may, under the conditions set out in this Law, entrust the execution of the measures and actions referred to in Article 15 paragraph (1) items a), b), c) and d) of this Law to third parties.

(2) The responsibility for implementing the customer due diligence measures in the cases referred to in paragraph (1) of this Article shall remain with the entity that has entrusted the obligations for performing the measures and actions referred to in Article 15 paragraph (1) items a), b), c) and d) of this Law to third parties.

(3) Third parties referred to in paragraph (1) of this Article are the entities referred to in Article 5 of this Law, member organizations and federations of those entities or other institutions established in the Republic of North Macedonia, a Member State of the European Union or in another country in which it is mandatory:

- to apply measures for customer due diligence and data retention in accordance with and in a manner at least identical to the manner established by this Law and which are in accordance with international standards,
- to apply measures and actions for the prevention of money laundering and terrorist financing is subject to supervision by a competent authority in accordance with this Law or are in accordance with international standards.

(4) The entity is obliged to previously check whether the third party meets the conditions prescribed by this Law, and in the case where the third party is an entity from another country, it is obliged to take into account the level of risk of money laundering and terrorist financing of that country.

(5) The entity may not entrust the taking of the measures and actions referred to in Article 15 paragraph (1) items a), b), c) and d) to a third party originating or established in a high-risk country in accordance with this Law or to a shell bank.

(6) In the cases referred to in paragraph (1) of this Article, the entity shall immediately obtain from the third party:

a) the information necessary to carry out the customer due diligence in accordance with this Law;
b) upon its request, without delay, obtain data and information on the customer due diligence carried out, i.e. copies of the identification and identity verification documents, including, if possible, information and data obtained using electronic identification means issued within the framework of a registered high-security electronic identification scheme in accordance with the law or other reliable, electronic means of remote identification regulated, approved and accepted by the competent authorities of foreign countries.

(7) Entities may entrust the execution of the measures and actions referred to in Article 15 paragraph (1) items a), b), c) and d) of this Law to third parties, part of the same financial group, if the group:

- applies the requirements for customer analysis, data retention and procedures for preventing money laundering and terrorist financing in accordance with international standards,
- applies the requirements for customer analysis and data retention that are subject to supervision at the group level by a competent authority and
- appropriately manages the risks associated with high-risk countries.

(8) The provisions of this Article shall not apply to a third party in the event that the third party acts as an agent for the entity or when the entity has concluded a service agreement with the third party for the purposes of performing activities specified in this Law on behalf of the entity.

Transfer of funds Article 50

The payment service provider and the intermediary institution in the transfer of funds in any currency for the purposes of preventing money laundering and terrorist financing are obliged to apply the provisions of this law that regulate the transfer of funds.

Obligations of the payer's payment service provider Article 50-a

(1) The payer's payment service provider shall be obliged to provide accurate data on the payer and the recipient of the transfer of funds in any currency in the paper or electronic form of the payment order and to include them in the electronic message accompanying the transfer of funds from the payer to the recipient.

(2) The data on the payer referred to in paragraph (1) of this Article are:

- the name and surname, i.e. the name of the payer,
- the payment account number and
- the address, including the name of the country, the number of the personal identification

document, the unique identification number (unique citizen identification number) or the date and place of birth if the payer is a natural person, i.e. the registered office, including the name of the country, the unique identification number (unique entity identification number or entity identification code) if the payer is a legal entity.

(3) The data on the recipient referred to in paragraph (1) of this Article are:

- the name and surname, i.e. the name of the recipient,
- the payment account number and
- a unique identification number (unique registration number of the entity or identification mark of the entity) if the recipient is a legal entity.

(4) By way of derogation from paragraph (2) line 2 and paragraph (3) line 2 of this Article, in the case of a transfer of funds that is not made from or to a payment account, the payer's payment service provider shall be obliged to ensure that the transfer of funds is accompanied by a unique identification mark of the payment transaction.

(5) In the case of a cross-border batch file transfer by a single payer, the individual transfers of funds that are part of such a transfer do not have to contain the data referred to in paragraphs (2) and (3) of this Article, provided that the data referred to in paragraphs (2), (3) and (4) of this Article are included in the batch transfer and that each individual transfer of funds includes at least the payer's payment account number or the unique identifier of the payment transaction.

(6) When the amount of the transfer of funds, including the amount of the transactions related to that transfer, does not exceed 1,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of payment, the payment service provider of the payer is obliged to ensure that the transfer of funds includes at least the following data about the payer and the payee:

- the name and surname, i.e. the name of the payer and the payee, and
- the payment account number of the payer and the payee, whereby if it is missing or cannot be determined, then it is necessary to determine the unique identification code of the payment transaction.

(7) The payer's payment service provider shall verify the accuracy of the payer's data provided in accordance with Articles 15, 16, 17, 18 and 19 of this Law, before carrying out a transfer of funds.

(8) The payer's payment service provider shall be deemed to have confirmed the accuracy of the data received about the payer before executing the transfer of funds, if it has previously established a business relationship with the payer and has identified and confirmed his identity in accordance with Articles 15, 16, 17, 18 and 19 of this Law and if it has acted in accordance with Article 37 of this Law.

(9) By way of derogation from paragraph (7) of this Article, the payer's payment service provider shall not be obliged to verify the accuracy of the data provided about the payer if the amount of the transfer of funds, including the amount of the payment transactions related to that transfer, does not exceed EUR 1,000 in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of payment and if the following conditions are met:

- there are no grounds for suspicion of money laundering or terrorist financing and
- the payment service provider has not received the funds to be transferred in cash or as anonymous electronic money.

(10) The payer's payment service provider shall be obliged to establish and implement procedures for verifying the completeness of the data referred to in this Article.

(11) In accordance with the risk assessment, the payer's payment service provider may verify the accuracy of the data received regardless of the amount of funds transferred.

(12) The payer's payment service provider shall not transfer funds before ensuring full compliance with the conditions provided for in this Article.

Obligations of the payee's payment service provider Article 50-b

- (1) The payment service provider of the payee shall be obliged to confirm whether the data on the payer and the payee of the transfer of funds are provided and contained in the electronic message accompanying the transfer of funds, in accordance with Article 50-a of this Law.
- (2) The payment service provider shall be obliged to establish and implement procedures for checking the completeness of the data referred to in paragraph (1) of this Article.
- (3) If the transfer of funds exceeds EUR 1,000 in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day before the payment service provider of the recipient approves the payment transaction of the recipient or makes the funds available to the recipient, the payment service provider of the recipient shall be obliged to confirm the accuracy of the data obtained about the recipient, in accordance with Articles 15, 16, 17, 18 and 19 of this Law, unless the recipient has already been identified and his identity has been confirmed in accordance with Articles 15, 16, 17, 18 and 19 of this Law and the payment service provider acts in accordance with Article 37 of this Law, and there are no grounds for suspicion of money laundering or terrorist financing.
- (4) Where the amount of the transfer of funds, including the value of the payment transactions related to that transfer, does not exceed EUR 1,000 in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day before the payment service provider of the recipient approves the payment transaction of the recipient or makes the funds available to the recipient, the payment service provider of the recipient is not obliged to confirm the accuracy of the data received about the recipient, unless:
- the funds are made available to the recipient in cash or in anonymous electronic money and
 - there are reasons to suspect money laundering or terrorist financing.
- (5) In accordance with the risk assessment, the payment service provider shall be obliged to verify the identity of the recipient regardless of the amount of funds transferred in accordance with Articles 15, 16, 17, 18 and 19 of this Law.

Obligations when transferring funds in case of incomplete data Article 50-c

- (1) The payment service provider of the payee shall be obliged, by applying the risk-based approach, to establish and implement procedures for the transfer of funds that do not include the complete data specified in Article 50-a of this Law.
- (2) When the transfer of funds does not include complete data in accordance with Article 50-a of this Law, in accordance with the risk assessment, the payment service provider of the payee shall be obliged to determine in its procedures referred to in paragraph (1) of this Article in which cases:
- it will refuse to carry out the transfer of funds,
 - it will postpone the execution of the transfer of funds until it has provided the missing data, which it must request from the institution intermediary in that transfer or from the payer's payment service provider, or
 - it will carry out the transfer of funds and at the same time request the missing data from the institution intermediary in the transfer or the payer's payment service provider.
- (3) If the payer's payment service provider continuously fails to provide accurate and complete data as specified in Article 50-a of this Law, the payer's payment service provider in the transfer of funds shall be obliged to warn him thereof, informing him of the deadline within which he must implement the obligations prescribed by the provisions of this Law. If the payer's payment service

provider fails to comply with the obligations prescribed by the provisions of this Law after receiving such a warning and after the expiry of the specified deadline, the payer's payment service provider shall be obliged to refuse future transfers of funds or to limit or terminate business cooperation with the payer's payment service provider.

(4) In the cases referred to in paragraph (3) of this Article, the payment service provider of the recipient shall be obliged:

- to inform the National Bank of the Republic of North Macedonia about the payment service provider that does not provide accurate and complete data in accordance with Article 50-a of this Law and about all measures taken in relation to it in accordance with paragraph (3) of this Article and
- to determine whether the lack of accurate and complete data referred to in Article 50-a of this Law and the existence of other circumstances indicate suspicion of money laundering or terrorist financing, for which it shall submit a report to the Administration in accordance with Article 65 of this Law.

Obligations for the intermediary institution in the transfer of funds **Article 50-d**

(1) The intermediary institution in the transfer of funds is obliged to forward the received data on the payer and the payee from the payer's payment service provider to the payee's payment service provider.

(2) The institution intermediary in the transfer of funds is obliged to determine whether all data about the payer and the recipient are listed in the electronic message accompanying the transfer of funds.

(3) The intermediary institution in the transfer of funds shall be obliged, by applying the risk-based approach, to establish and implement procedures that it will apply in the event that the electronic message for the transfer of funds does not contain the data referred to in Article 50-a of this Law.

(4) When the transfer of funds does not include the complete data referred to in Article 50-a of this Law, in accordance with the risk assessment, the intermediary institution in the transfer of funds shall be obliged to determine in its procedures in which cases:

- it will refuse to carry out the transfer of funds,
- it will postpone the execution of the transfer of funds until it has provided the missing data, which it must request from the intermediary institution in that transfer or from the payment service provider of the payer, or
- it will carry out the transfer of funds and at the same time request the missing data from the intermediary institution in the transfer of funds or the payment service provider of the payer.

(5) If the payer's payment service provider or the payee's payment service provider fails to provide accurate and complete data as set out in Article 50-a of this Law, the intermediary institution in the transfer of funds shall be obliged to warn it thereof, informing it of the deadline within which it must implement the obligations prescribed by the provisions of this Law. If the payer's payment service provider or the payee's payment service provider fails to implement the obligations prescribed by the provisions of this Law after receiving such a warning and after the expiry of the specified deadline, the intermediary institution in the transfer of funds shall be obliged to refuse future transfers of funds received from the payer's payment service provider or the payee's payment service provider or to limit or terminate business cooperation with it.

(6) In the cases referred to in paragraph (4) of this Article, the intermediary institution in the transfer of funds shall be obliged to:

- inform the National Bank of the Republic of North Macedonia about the payment service provider that does not provide accurate and complete data in accordance with Article 50-a of this Law and

about all measures taken in relation to the same in accordance with paragraph (4) of this Article and

- determine whether the lack of accurate and complete data referred to in Article 50-a of this Law and the existence of other circumstances indicate suspicion of money laundering or terrorist financing, for which it shall submit a report to the Administration in accordance with Article 65 of this Law.

Exceptions when transferring funds Article 50-e

The provisions of Articles 50, 50-a, 50-b, 50-c and 50-d of this Law shall not apply in the following cases:

- a) when the transfer of funds is carried out in order to pay taxes, fines or other public charges in the Republic of North Macedonia;
- b) when the transfer of funds is carried out solely for the purpose of purchasing goods or services using a payment card, electronic money payment instrument, mobile phone or any other digital or information technology device, provided that the number of such card, instrument or device, or a unique identification mark, accompanies such transfer in a manner that allows the data on the payer to be obtained through such number or identification mark, whereby this exception shall not apply in the case where the payer and the recipient are natural persons and the transfer of funds does not arise from the performance of a business activity, as well as the transfer of funds or virtual assets that have the characteristics of electronic money tokens;
- c) when the transfer involves services and payment transactions referred to in Article 3 of the Law on Payment Services and Payment Systems (*);
- d) when the payer and the payee are payment service providers acting for themselves and on their own behalf;
- e) when the payer withdraws cash from his account;
- f) when the transfer of funds is made in order to pay the recipient for telecommunications services, services for the distribution of electricity, gas, heat, water, services for the collection, treatment and disposal of waste, services for the maintenance of residential buildings or other facilities, where the following conditions are met:
 - the amount of the transfer of funds does not exceed 1,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of receipt of the order for the transfer of funds,
 - the charges for the services should be made to the payment account of the recipient that is used only for such type of payments,
 - the payment service provider of the recipient can, through the recipient, on the basis of a unique identification mark of the payment transaction or other data accompanying the transfer of funds, obtain data on the transfer of funds from the person who has a contract with the recipient regarding the provision of the services referred to in this point,
 - the transfer of funds is within the Republic of North Macedonia and
 - when the conditions of the article are met 14 of this Law and
- g) the person does not perform any other activity than exchanging documents from paper to electronic form or providing other type of support in accordance with an agreement with the payment service provider.

Obligations for the service provider related to the sender's virtual assets Article 51

(1) The virtual asset service provider of the sender shall ensure that the transfer of virtual assets is accompanied by the following data and information about the sender:

- the name and surname, i.e. the name of the sender,
- the address of the hosted or non-hosted electronic wallet for virtual assets and the account number, if any and used for the purposes of the transfer, and if the address, i.e. the account is missing or cannot be determined, then it is necessary to determine the unique identification mark of the virtual asset transfer, which allows its tracking, and
- the address, including the name of the country, the number of the personal identification document, a unique identification number (unique citizen identification number) or date and place of birth if the sender is a natural person, i.e. a unique identification number (unique entity identification number or entity identification mark) if the sender is a legal entity.

(2) The provider of services related to virtual assets referred to in paragraph (1) of this Article shall be obliged to ensure that the transfer of virtual assets is accompanied by the following data and information about the user:

- the name and surname, i.e. the name of the user,
- the address of the hosted or non-hosted electronic wallet for virtual assets and the account number, if it exists and is used for the purposes of the transfer, and if the address, i.e. the account is missing or cannot be determined, then it is necessary to determine the unique identification mark of the transfer of virtual assets, which allows its tracking, and
- a unique identification number (unique registration number of the entity or identification mark of the entity) if the user is a legal entity.

(3) Providers of services related to virtual assets shall be obliged to transmit the data referred to in paragraphs (1) and (2) of this Article before or during the transfer of virtual assets and in a manner that ensures the reliability of such data, as well as protection against unauthorized access, without limiting them to being an integral part of the transfer.

(4) By way of exception to paragraphs (1) and (2) of this Article, in the case of a transfer of virtual funds made from or to a non-hosted electronic wallet, the provider of services related to virtual funds of the sender shall be obliged to ensure that the transfer is accompanied by a unique identification mark.

(5) Service providers related to virtual assets are obliged, within the framework of internal procedures and risk assessment, in the transfer of virtual assets exceeding 1,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of transfer, to a non-hosted electronic wallet for virtual assets, to assess whether the addresses of the payer and the recipient are controlled by the same person.

(6) The provider of services related to virtual assets shall verify the accuracy of the sender data provided in accordance with Articles 15, 16, 17, 18 and 19 of this Law, before transferring the virtual assets.

(7) The provider of services related to virtual assets shall be deemed to have confirmed the accuracy of the data received about the sender before carrying out the transfer of virtual assets, if it has previously established a business relationship with the payer and has identified and confirmed his identity in accordance with Articles 15, 16, 17, 18 and 19 of this Law and if it has acted in accordance with Article 37 of this Law.

(8) The virtual asset service provider shall not transfer virtual assets to the sender before ensuring that there is full compliance with the conditions provided for in this Article.

(9) In the case of a batch file transfer by a single sender, the individual transfers of virtual assets that are part of such transfer do not have to contain the data referred to in paragraphs (2) and (3) of this Article, provided that the data referred to in paragraphs (6) and (7) of this Article are included in the batch transfer and that each individual transfer of assets includes at least a unique

transaction identifier.

Obligations of the service provider related to the user's virtual assets

Article 51-a

(1) The provider of services related to the user's virtual assets shall be obliged to establish and implement procedures for checking the completeness of the data referred to in Article 51, paragraphs (1), (2), (3) and (4) of this Law during or after the execution of the transfer in order to verify whether the data on the sender and the user or the data referred to in Article 51, paragraph (9) of this Law have been provided.

(2) In the case of a transfer of virtual funds that is made from a non-hosted electronic wallet, the provider of services related to virtual funds of the user is obliged to provide and store the data referred to in Article 51, paragraphs (1) and (2) of this Law and to ensure that the transfer of virtual funds can be identified.

(3) The provider of services related to the user's virtual assets is obliged, within the framework of internal procedures and risk assessment in the transfer of virtual assets exceeding 1,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of transfer, from a non-hosted electronic wallet for virtual assets, to assess whether the addresses of the sender and the user are controlled by the same person.

(4) The provider of services related to virtual assets, before making virtual assets available to the user, shall be obliged to confirm the accuracy of the information about the user referred to in Article 51, paragraph (2) of this Law on the basis of data and information from reliable and independent sources.

(5) The verification of the data referred to in paragraph (4) of this Article shall be deemed to have been carried out when the provider of services related to virtual assets referred to in this Article has appropriately applied the provisions of this Law relating to the analysis of customers, the continuous monitoring of the business relationship and the storage of data and information provided for by this Law.

Obligations when transferring virtual assets in case of incomplete data

Article 51-b

(1) The provider of services related to virtual assets of the user is obliged, by applying the approach based on risk assessment, to establish and implement procedures for the transfer of virtual assets that do not include complete data specified in Article 51 of this Law.

(2) When the transfer of virtual assets does not include complete data in accordance with Article 51 of this Law, in accordance with the risk assessment, the provider of services related to virtual assets of the user shall be obliged to determine in its procedures referred to in paragraph (1) of this Article in which cases:

- it will refuse to transfer virtual assets,
- it will return the virtual assets to the sender or
- it will request the missing data from the provider of services related to virtual assets before making them available to the user.

(3) If the provider of services related to virtual assets continuously fails to provide accurate and complete data as specified in Article 51 of this Law, the provider of services related to virtual assets shall be obliged to warn the user of the transfer of virtual assets thereof, informing him of the deadline within which he should implement the obligations prescribed by the provisions of this Law. If the provider of services related to virtual assets fails to implement the obligations prescribed by the provisions of this Law, upon receipt of such warning and after the expiry of the

specified deadline, the provider of services related to virtual assets shall be obliged to refuse future transfers of virtual assets to the user or to limit or terminate business cooperation with the provider of services related to virtual assets.

(4) In the cases referred to in paragraph (3) of this Article, the provider of services related to virtual assets of the user shall be obliged:

- to inform the competent authority in accordance with the law about the provider of services related to virtual assets that does not provide accurate and complete data in accordance with Article 51 of this Law and about all measures taken in relation to it in accordance with paragraph (3) of this Article and
- to determine whether the lack of accurate and complete data in accordance with Article 51 of this Law and the existence of other circumstances indicate suspicion of money laundering or terrorist financing, for which it shall submit a report to the Administration in accordance with Article 65 of this Law.

Obligations for the virtual asset service provider acting as an intermediary Article of the 51-c

(1) The virtual asset service provider acting as an intermediary in the execution of a transfer of virtual assets between the virtual asset service provider of the sender and the user shall ensure that the data and information referred to in Article 51 of this Law for the sender and the user accompanying the transfer of virtual assets are transmitted together with the transfer of virtual assets or the aggregate transfer of virtual assets, including a transfer of virtual assets made from or to a non-hosted electronic wallet for virtual assets.

(2) The provider of services related to virtual assets acting as an intermediary referred to in paragraph (1) of this Article shall be obliged to store the data and information on the sender and the user within the period specified in Article 62 of this Law and, if necessary, to make them available to the supervisory authorities referred to in Article 151 of this Law upon their request.

(3) The provider of services related to virtual assets acting as an intermediary referred to in paragraph (1) of this Law shall be obliged, by applying the risk-based approach, to establish and implement procedures that it will apply when the electronic message for the transfer of virtual assets does not contain the data referred to in Article 51 of this Law.

(4) When the transfer of virtual assets does not include the complete data referred to in Article 51 of this Law, in accordance with the risk assessment, the virtual asset service provider acting as an intermediary referred to in paragraph (1) of this Article in the transfer of virtual assets shall be obliged to determine in its procedures in which cases:

- it will refuse to transfer virtual assets,
- it will return the virtual assets to the sender, or
- it will request the missing data from the virtual asset service provider before executing the transfer.

(5) If the virtual asset service provider does not provide the sender with accurate and complete data as specified in Article 51 of this Law, the virtual asset service provider acting as an intermediary in the transfer of virtual assets shall be obliged to warn him thereof, informing him of the deadline within which he should implement the obligations prescribed by the provisions of this Law. If the virtual asset service provider of the sender fails to implement the obligations prescribed by the provisions of this Law, upon receipt of such warning and after the expiry of the specified deadline, the virtual asset service provider acting as an intermediary in the transfer of virtual assets shall be obliged to refuse future transfers of virtual assets received from the virtual asset service provider or to limit or terminate business cooperation with him.

(6) In the cases referred to in paragraph (5) of this Article, the virtual asset service provider acting as an intermediary referred to in paragraph (1) of this Article in the transfer of virtual assets shall be obliged to:

- inform the competent authority in accordance with the law about the virtual asset service provider that does not provide accurate and complete data in accordance with Article 51 of this Law and about all measures taken in relation to it in accordance with paragraph (5) of this Article and
- determine whether the lack of accurate and complete data in accordance with Article 51 of this Law and the existence of other circumstances indicate suspicion of money laundering or terrorist financing, for which it shall submit a report to the Administration in accordance with Article 65 of this Law.

Exceptions when transferring virtual assets **Article 51-d**

The provisions of Articles 51, 51-a, 51-b and 51-c of this Law shall not apply in the following cases:

- a) when transferring virtual assets between virtual asset service providers who perform this transfer on their own behalf and for their own account and
- b) when transferring virtual assets between non-hosted electronic wallets for virtual assets that are performed as a transfer of virtual assets that does not involve a virtual asset service provider.

Virtual asset service providers **Article 52**

(1) When performing a transaction related to virtual assets within the meaning of this Law, providers of services related to virtual assets shall, in addition to the measures set out in Article 15 of this Law, be obliged to establish the identity of the client in accordance with Article 17 of this Law, prior to each occasional transaction with virtual assets.

(2) The provider of services related to virtual assets, within the framework of the implementation of the measures and actions for the prevention of money laundering and terrorist financing under this Law, in addition to the measures under Article 15 of this Law, is obliged to provide and store data on the hosted or non-hosted electronic wallet, i.e. virtual asset addresses used or used by the client to execute a transaction related to virtual assets, as well as to take measures to determine whether the client uses multiple wallets, i.e. virtual asset addresses.

(3) The entities referred to in paragraph (1) of this Article are obliged to record the client data in chronological order in a numbered register signed by the authorized person or another person with the authorization to sign the register given by a manager in accordance with the internal acts of the entities.

Money Exchanges **Article 53**

(1) Entities that have a license for currency exchange operations, in addition to the measures set out in Article 15 of this Law, are obliged to determine the identity of the client in accordance with Article 17 of this Law, before each transaction involving an amount exceeding 500 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia.

(2) The entities referred to in paragraph (1) of this Article are obliged to record the client data in chronological order in a numbered register signed by the authorized person or another person with

the authorization to sign the register given by a manager in accordance with the internal acts of the entities.

(3) The numbered register referred to in paragraph (2) of this Article shall contain the following data:

- "Ordinal number" shall record the transactions in chronological order starting from the numerical unit "one" and continuing until the closing of the register with the last page for the current month,
- "Date" shall record the date on which the transaction was carried out,
- "Name and surname of a natural person" shall record in the original as in the valid identification document, the name and surname of the client who carried out the transaction exceeding 500 euros in denar equivalent,
- "Date and place of birth" shall record in the original as in the valid identification document, the date and place of birth of the client who carried out the transaction exceeding 500 euros in denar equivalent,
- "Address and place of residence or residence" shall record in the original as in the valid identification document, the address and place of residence or residence of the client who carried out the transaction exceeding 500 euros in denar equivalent,
- "EMBG or identification number" is recorded in the original as from the valid identification document, the unique personal identification number of the citizen - resident or the identification number of the natural person - non-resident, for the client who performed the transaction exceeding 500 euros in denar equivalent,
- "Number of the identification document" is recorded the number of the valid identification document (ID card number or passport number) of the client who performed the transaction exceeding 500 euros in denar equivalent,
- "Authority that issued the identification document" is recorded the authority that issued the identification document (ID card number or passport number) of the client who performed the transaction exceeding 500 euros in denar equivalent,
- "Purchase/sale" is recorded whether the transaction buys or sells foreign currency over 500 euros in denar equivalent,
- "Type of currency" shall be recorded the code of the currency of the transaction exceeding 500 euros in denar equivalent, in accordance with the Instructions on the manner of performing international payment operations of the National Bank of the Republic of North Macedonia,
- "Transaction amount" shall be recorded the amount of the transaction exceeding 500 euros in denar equivalent,
- "Name and surname" shall be recorded the name and surname of the authorized person or other person authorized to sign the register and
- Signature of the authorized person or other person authorized to sign the register.

Organizers of games of chance

Article 54

(1) The organizers of games of chance in a gaming house (casino), in addition to the measures set out in Article 15 of this Law, are obliged to establish the identity of the client in accordance with Article 17 of this Law immediately upon entering the casino and upon purchase or payment of chips or credits in an amount exceeding 1,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of purchase, i.e. payment, regardless of whether the transaction is carried out as an individual transaction or through several transactions that are obviously connected.

(2) Organizers of games of chance, with the exception of organizers of games of chance in a gaming house (casino), in addition to the measures set out in Article 15 of this Law, are obliged to

determine the identity of the client in accordance with Article 17 of this Law before paying out winnings, paying a deposit, or in both cases when the transaction is worth 1,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia, regardless of whether the transaction is carried out as an individual transaction or through several transactions that are obviously connected.

Brokerage houses and banks with a license to work with securities

Article 55

(1) Brokerage houses and banks with a license to operate with securities are obliged to keep a numbered register for trading in securities whose total amount exceeds 15,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia, signed by the authorized person or another person with the authorization to sign the register given by a manager in accordance with the acts of the brokerage houses and banks with a license to operate with securities.

(2) The numbered register referred to in paragraph (1) of this Article shall contain the following data:

- "Ordinal number" records transactions in chronological order, starting from the numerical unit "one" and onwards, until the register is closed with the last page for the current month,
- "Date" records the date when the transaction was carried out,
- "Name and surname of the client - natural person/Name of the client - legal entity" is recorded in the original from the valid identification document, name and surname when the client is a natural person or the name of the legal entity is recorded when the client is a legal entity,
- "Date and place of birth of the client - natural person" is recorded in the original from the valid identification document, date and place of birth of the client when he is a natural person,
- "Address and place of residence or place of stay of the client - natural person/Head office of the client - legal entity" is recorded in the original from the identification document, address and place of residence or place of stay when the client is a natural person or the head office is recorded when the client is a legal entity,
- "EMBG or identification number of the client - natural person/EDB or identification number of the client - legal entity" is recorded in the original of the identification document EMBG (unique citizen identification number) when the client is a natural person - resident or identification number when the client is a natural person - non-resident, or EDB (unique tax number) is recorded when the client is a legal person - resident or identification number when the client is a legal person - non-resident,
- "Number of the identification document of the client - natural person/legal representative of the client - legal entity" is recorded the number of the valid identification document (ID card number or passport number),
- "Authority that issued the identification document of the client - natural person/legal representative of the client - legal entity" is recorded the authority that issued the identification document,
- "Name, surname and EMBG or identification number of the authorized person" shall be recorded in the original of the identification document the name, surname and EMBG when the authorized natural person is a resident or the identification number when the authorized natural person is a non-resident,
- "Name, surname and EMBG or identification number of the beneficial owner" shall be recorded in the original of the identification document the name, surname and EMBG when the beneficial owner is a resident or the name, surname and identification number when the beneficial owner is a non-resident,

- "Purchase or sale" shall be recorded the word "purchase" or the word "sale" depending on the specific case,
- "Client account - natural or legal entity or agent" shall be recorded in numbers, the transaction account number of the client or agent when it is a natural or legal entity, through which the transaction was carried out,
- "Number of shares" shall be recorded in numbers, how many shares were purchased or sold,
- "Total amount of the transaction in denars" shall be recorded in numbers, the total amount of the transaction carried out,
- "Issuer of shares" shall be recorded in numbers, the name of the legal entity issuing the shares that are the subject of the transaction,
- "Name and surname" shall be recorded in numbers, the name and surname of the authorized person or other person authorized to sign the register, and
- signature of the authorized person or other person authorized to sign the register.

Persons who trade or act as intermediaries in the trade of works of art

Article 56

(1) Entities that are persons trading or acting as intermediaries in the trade of works of art in accordance with Article 5 paragraph (1) item 8) of this Law, in addition to the measures set out in Article 15 of this Law, are obliged to establish the identity of the client in accordance with Article 17 of this Law before each transaction involving an amount exceeding 10,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia, regardless of whether the transaction is carried out as an individual transaction or through several transactions that are obviously linked.

(2) The entities referred to in paragraph (1) of this Article are obliged to record the client data in chronological order in a numbered register signed by the authorized person or another person with the authorization to sign the register given by a managing person in accordance with the acts of the entities.

(3) The numbered register referred to in paragraph (2) of this Article shall contain the following data:

- "Ordinal number" shall record the transactions in chronological order, starting from the numerical unit "one" and onwards, until the register is closed with the last page for the current month,
- "Date" shall record the date on which the transaction was carried out,
- "Name and surname of the client - natural person/Name of the client - legal entity" shall be recorded in the original from the identification document, name and surname when the client is a natural person or the name of the legal entity shall be recorded when the client is a legal entity,
- "Date and place of birth of the client - natural person" shall be recorded in the original from the valid identification document, date and place of birth of the client when he is a natural person,
- "Address and place of residence or place of stay of the client - natural person/Head office of the client - legal entity" shall be recorded in the original from the valid identification document, address and place of residence or residence when the client is a natural person or the registered office is recorded when the client is a legal entity,
- "EMBG or identification number of the client - natural person/ EDB or identification number of the client - legal entity" is recorded in the original of the identification document EMBG (unique citizen identification number) when the client is a natural person - resident or identification number when the client is a natural person - non-resident, or EDB (unique tax number) is recorded when the client is a legal person - resident or identification number when the client is a legal person - non-resident,
- "Number of the identification document of the client - natural person/legal representative of the

- client - legal entity" is recorded the number of the identification document (ID card number or passport number),
- "Authority that issued the identification document of the client - natural person/legal representative of the client - legal entity" is recorded the authority that issued the document for identification,
 - "Name, surname and EMBG or identification number of the authorized person" is recorded in the original of the identification document, the name, surname and EMBG when the authorized natural person is a resident or the identification number when the authorized natural person is a non-resident,
 - "Name, surname and EMBG or identification number of the beneficial owner" is recorded in the original of the identification document, the name, surname and EMBG when the beneficial owner is a resident or the name, surname and identification number when the beneficial owner is a non-resident,
 - "Purchase or sale" is recorded in the word "purchase" or the word "sale" depending on the specific case,
 - "Total amount of the transaction in denars" is recorded in figures, the total amount of the transaction performed,
 - "Name and surname" shall include the name and surname of the authorized person or other person authorized to sign the register and
 - signature of the authorized person or other person authorized to sign the register.

Persons who store, trade or act as intermediaries in the trade of works of art when the activity takes place in free zones¹⁵

Article 57

(1) Entities that are persons trading or acting as intermediaries in the trade of works of art in accordance with Article 5 paragraph (1) item 9) of this Law, in addition to the measures set out in Article 15 of this Law, are obliged to establish the identity of the client in accordance with Article 17 of this Law before each transaction involving an amount exceeding 10,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia, regardless of whether the transaction is carried out as an individual transaction or through several transactions that are obviously connected.

(2) The entities referred to in paragraph (1) of this Article are obliged to record the client data in chronological order in a numbered register signed by the authorized person or another person with the authorization to sign the register given by a manager in accordance with the internal acts of the entities.

(3) The numbered register referred to in paragraph (2) of this Article shall contain the following data:

- "Ordinal number" shall record the transactions in chronological order, starting from the numerical unit "one" and onwards, until the register is closed with the last page for the current month,
- "Date" shall record the date on which the transaction was carried out,
- "Name and surname of the client - natural person/Name of the client - legal entity" shall be recorded in the original from the identification document, name and surname when the client is a natural person or the name of the legal entity shall be recorded when the client is a legal entity,
- "Date and place of birth of the client - natural person" shall be recorded in the original from the valid identification document, date and place of birth of the client when he is a natural person,
- "Address and place of residence or place of stay of the client - natural person/Head office of the client - legal entity" shall be recorded in the original from the identification document, address and place of residence or place of stay when the client is a natural person or the registered office is

recorded when the client is a legal entity,

- "EMBG or client identification number - natural person/ EDB or client identification number - legal entity" is recorded in the original of the identification document EMBG (unique citizen identification number) when the client is a natural person - resident or identification number when the client is a natural person - non-resident or EDB (unique tax number) is recorded when the client is a legal entity - resident or identification number when the client is a legal entity - non-resident,

- "Number of the identification document of the client - natural person/legal representative of the client - legal entity" is recorded the number of the identification document (ID card number or passport number),

- "Authority that issued the identification document of the client - natural person/legal representative of the client - legal entity" is recorded the authority that issued the identification document,

- "Name, surname and EMBG or identification number of the authorized person" shall be recorded in the original of the identification document, the name, surname and EMBG when the authorized natural person is a resident or the identification number when the authorized natural person is a non-resident,

- "Name, surname and EMBG or identification number of the beneficial owner" shall be recorded in the original of the identification document, the name, surname and EMBG when the beneficial owner is a resident or the name, surname and identification number when the beneficial owner is a non-resident,

- "Purchase or sale" shall be recorded with the word "purchase" or the word "sale" depending on the specific case,

- "Total amount of the transaction in denars" shall be recorded in figures, the total amount of the transaction carried out,

- "Name and surname" shall be recorded with the name and surname of the authorized person or other person authorized to sign the register and

- signature of the authorized person or other person authorized to sign the register.

(4) The Minister of Finance, upon proposal of the Director of the Administration, shall prescribe the format of the numbered register referred to in Articles 52, 53, 55, 56 and 57 of this Law.

Ban Article 58

(1) Cash payment for goods and services in the amount of 3,000 euros or more in denar equivalent in the form of one or more obviously related transactions, which is not carried out through a bank, savings bank or through an account in another institution providing payment services, is prohibited.

(2) Entities authorized by law to register securities, other property or legal matters or to report or perform transfers of money, securities or other property may perform such registration or transfer only if the client submits evidence that the transfer of money exceeding the amount referred to in paragraph (1) of this Article was carried out through a bank, savings bank or through an account in another institution providing payment services.

(3) The prohibition referred to in paragraph (1) of this Article shall not apply to organizers of games of chance.

(4) It is prohibited to carry out transactions related to the exchange of virtual assets for money within the meaning of the law that are carried out with cash in an amount exceeding 500 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of carrying out the transaction, in the form of one or more obviously

related transactions, which is not carried out through a bank, savings bank or through an account in another institution that provides payment services.

Article 59

(1) Financial institutions and service providers related to virtual assets are prohibited from establishing or continuing a business relationship with Shell Bank (the shell banks) and from starting or continuing a correspondent business relationship with a bank that they know allows the opening and operation of Shell Bank (the shell banks) accounts.

(2) Shell banks are prohibited from carrying out financial activities in any way in the Republic of North Macedonia.

(3) Financial institutions and service providers related to virtual assets referred to in paragraph (1) of this Article shall be obliged to ensure that the financial institution with which it has correspondent business cooperation prohibits its accounts from being used by shell banks.

Article 60

(1) Financial institutions are prohibited from opening and maintaining accounts, savings books and safe deposit boxes in anonymous form, encrypted form or under fictitious names, or from performing other services that directly or indirectly enable concealment of the client's identity, or anonymity.

(2) It is prohibited to provide services related to virtual assets that directly or indirectly enable concealment of the client's identity, as well as to conduct transactions with such virtual assets.

(3) The issuer of virtual assets as well as the provider of services related to virtual assets may not use resources or means through an information system that enables or facilitates concealment of the identity of the client or that disables or makes difficult the monitoring of transactions related to virtual assets.

Article 61

Acceptance of payments made using an anonymous prepaid payment card is prohibited when:

- 1) the payment instrument is topped up or the total amount of transactions on a monthly basis is not limited to 150 euros in denar equivalent, according to the middle exchange rate of the National Bank of the Republic of North Macedonia and can only be used in the Republic of North Macedonia;
- 2) the maximum amount of the payment instrument exceeds 150 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia;
- 3) the payment instrument is not used exclusively for the purchase of goods or services;
- 4) the payment instrument is issued anonymously and
- 5) the issuer of the payment instrument does not monitor and control the transactions or business relationships in order to detect complex or unusual transactions or suspicious transactions.

Data storage

Article 62

(1) Entities shall be obliged to keep documents or electronic records provided by customer due diligence measures, customer files and business correspondence, the results of any analysis carried out on the customer or the beneficial owner, in electronic or written form, for ten years from the termination of the business relationship with the customer or from the date of execution of the occasional transaction.

(2) Entities are obliged to keep documents or electronic records of all transactions for ten years after their execution, including supporting evidence and records of transactions consisting of

original documents or copies that may serve as evidence in court proceedings, which are necessary to identify and enable the reconstruction of individual transactions.

(3) The entities are obliged to keep the data, in the manner in which they submitted it to the Administration, for ten years from the date of submission. After the expiry of this period, the entities are obliged to delete the client's personal data.

(4) Financial institutions and service providers related to virtual assets are obliged to keep the data on the payer, i.e. the orderer and the recipient of the non-cash transfer of funds or transfer of virtual assets from Articles 50, 50-a, 50-b, 50-c, 50-d, 51, 51-a, 51-b and 51-c of this Law, for ten years from the transfer.

(5) The register referred to in Articles 52, 53, 54, 55, 56 and 57 of this Law shall be kept for ten years from the last recorded data.

(6) Entities are obliged to keep copies of the documentation referred to in Article 69 of this Law for ten years from the date of the internal control.

(7) In the event of the termination of the entity's existence, the obligation to store the data within the period specified in paragraph (1) of this Article shall be transferred to the legal successors of the entity.

(8) If there are no legal successors of the legal entity, the obligation to keep the data referred to in paragraph (1) of this Article shall be transferred to its founders.

(9) Entities are obliged to make the documents referred to in paragraphs (1) and (2) of this Article available upon request to the supervisory authorities referred to in Article 151 of this Law.

(10) Upon request of the Administration, the entities are obliged to keep the data referred to in paragraph (1) of this Article for longer than ten years.

Submission of data to the Administration

Article 63

(1) Entities are obliged to submit the collected data, information and documents to the Administration in the case of a cash transaction in the amount of 15,000 euros in denar equivalent according to the average exchange rate of the National Bank of the Republic of North Macedonia or more, regardless of whether it is a single transaction or several obviously related transactions.

(2) The entities shall be obliged to submit the collected data, information and documents on the executed transactions referred to in paragraph (1) of this Article to the Administration no later than three working days from the executed transaction in the form of a report.

(3) The Minister of Finance, upon proposal of the Director of the Administration, shall prescribe the form and content of the report referred to in paragraph (2) of this Article.

Article 64

(1) Notaries shall submit the collected data on drawn up notarial documents and notarial certifications of signatures on contracts by which the right to ownership of property is acquired in the value of 15,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of drawing up, i.e. certification, specified in the contract, as well as the drawn up notarial documents and notarial certifications of signatures on contracts referred to in this paragraph to the Administration in the form of a report in electronic form no later than three working days from the day of drawing up, i.e. certification.

(2) Banks shall submit the collected data on disbursed loans to their clients in the value of 15,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day the loan is disbursed to the Administration by the tenth day of the current month for the previous month in the form of a report in electronic form.

(3) Banks shall submit the collected data on loans granted and/or received between clients in the value of 5,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia to the Administration by the tenth day of the current month for the previous month in the form of a report in electronic form.

(4) Providers of money remittance services (fast money transfer) shall submit data on transactions in the amount of 1,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of execution of the transaction to the Administration in the form of a report in electronic form no later than three working days from the day of execution of the transaction.

(5) Insurance companies that carry out life insurance activities shall submit the collected data on concluded policies as well as the concluded life insurance policy to the Administration in the form of a report in electronic form no later than three working days from the day of conclusion in the following cases:

- for concluded life insurance policies with a premium payment for life insurance policies in an amount equal to or greater than 15,000 euros and a payment based on redemption, loan or experience equal to or greater than 15,000 euros in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day the insurance policy is concluded, i.e. on the day the payment is made, except for life insurance contracts without a savings component, i.e. without an investment component and

- for life insurance policies concluded by a public office holder, regardless of the value of the insured amount, except for life insurance contracts without a savings component, i.e. without an investment component.

(6) Legal entities whose activity is the purchase and sale of vehicles shall submit the collected data on the concluded contracts for the purchase and sale of new vehicles worth 15,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day the contract was concluded to the Administration in the form of a report in electronic form no later than three working days from the day the contract was concluded.

(7) The organizers of games of chance in a gaming house (casino) shall submit the collected data on the purchase or payment of chips or credits in the amount of 1,000 euros in denar equivalent or more according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of purchase or payment, regardless of whether the transaction is carried out as an individual transaction or through several transactions that are obviously connected, to the Administration in the form of a report in electronic form no later than three working days from the day of purchase or payment.

(8) Other organizers of games of chance, except organizers of games of chance in a gaming house (casino), shall submit the collected data on the payment of winnings, payment of a deposit or in both cases when the transaction is worth 1,000 euros in denar equivalent or more according to the middle exchange rate of the National Bank of the Republic of North Macedonia, regardless of whether the transaction is carried out individually or through several transactions that are obviously connected, to the Administration in the form of a report in electronic form no later than three working days from the day of the payment, payment or in both cases.

(9) When providers of services related to virtual assets perform activities, i.e. provide services for the exchange of virtual assets and fiat currencies or money within the meaning of the law, they shall submit data on the executed transactions in the amount of 1,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day of execution of the transaction, in the form of one or more related transactions, to the Administration in the form of a report in electronic form no later than three working days from the day of execution of the transaction.

(10) The enforcement agents shall submit the collected data on sales made by oral public auction and sales contracts by direct agreement, which acquire the right to ownership of property worth 15,000 euros or more in denar equivalent according to the middle exchange rate of the National Bank of the Republic of North Macedonia on the day they are compiled, to the Administration in the form of a report in electronic form no later than three working days from the day of the sale, i.e. the day of compiling the sales contract by direct agreement.

(11) The reports referred to in paragraphs (1), (2), (3), (4), (5), (6), (7), (8), (9) and (10) of this Article shall contain data on the unique personal identification number or other identification number of the person, name and surname, date and place of birth, gender and citizenship.

(12) The Minister of Finance, upon proposal of the Director of the Administration, shall prescribe the format of the reports, the type and categories of data from paragraphs (1), (2), (3), (4), (5), (6), (7), (8), (9), (10) and (11) of this Article and the manner of electronic submission to the Administration.

Article 65

(1) Entities are obliged to submit the collected data, information and documents to the Administration when:

- 1) they know, suspect or have grounds for suspecting that money laundering and/or terrorist financing has been committed or an attempt has been made or an attempt is being made to launder money and/or terrorist financing, regardless of the amount of the transaction;
- 2) they know, suspect or have grounds for suspecting that the property constitutes the proceeds of a criminal offence or
- 3) they know, suspect or have grounds for suspecting that the property is related to the financing of a terrorist act, a terrorist organisation or a terrorist or a person who finances terrorism or the financing of weapons of mass destruction.

(2) If the entity becomes aware of the grounds for suspicion referred to in paragraph (1) of this Article before executing the transaction, it is obliged to immediately notify the Administration and to hold the transaction for a maximum of two hours from the notification to the Administration.

(3) If the entity becomes aware of the grounds for suspicion referred to in paragraph (1) of this Article during the execution of the transaction, it is obliged to immediately notify the Administration and to hold the transaction for a maximum of four hours from the notification to the Administration.

(4) The subject of suspicions referred to in paragraph (1) of this Article is obliged to submit accurate data, information and documents to the Administration in the form of a report no later than 24 hours from the date of becoming aware of the grounds for suspicion.

(5) If the submitted data from paragraphs (2), (3) and (4) of this Article are insufficient, the Administration may request additional information, data and documentation from the entity.

(6) If the Administration does not notify the entity of further activities within the deadlines specified in paragraphs (2) and (3) of this Article, the entity may execute or reject the transaction.

(7) Entities, with the exception of notaries, lawyers and law firms, are obliged to notify in writing the competent supervisory authority referred to in Article 151 of this Law that they have submitted a report referred to in paragraph (4) of this Article to the Administration, within three working days of the submission of the report.

(8) The Administration shall be obliged to notify the entity of the receipt and the performed checks of the report referred to in paragraph (4) of this Article.

(9) The report referred to in paragraph (4) of this Article shall contain data on the unique personal identification number or other identification number of the person, name and surname, date and place of birth, gender and citizenship.

(10) The Minister of Finance, upon proposal of the Director of the Administration, shall prescribe the format, type and categories of data from the report referred to in paragraph (4) of this Article.

Article 66

The entity shall determine the grounds for suspicion referred to in Article 65 paragraph (1) of this Law on the basis of:

- direct knowledge of the client,
- the list of indicators for recognizing suspicious transactions determined by the Administration, the entities and the supervisory authorities,
- the consolidated list maintained in accordance with the regulations on restrictive measures,
- typologies and trends of money laundering or terrorist financing determined by the Administration,
- the estimated risk of money laundering and terrorist financing and the determined risk profile of the client, and
- other relevant information.

Article 67

- (1) Entities shall submit reports to the Administration via protected electronic means. If this method of submission is impossible for technical reasons, entities shall submit reports in writing.
- (2) Notifications given to the Administration by telephone should be confirmed in accordance with paragraph (1) of this Article within 24 hours at the latest.
- (3) The Administration may not disclose the identity of the employee of the entity submitting the report, except in cases where there is suspicion that the employee or entity has committed a criminal offense of money laundering and/or financing of terrorism, upon written request of the competent court when it is necessary to establish facts in the course of criminal proceedings.

Secure ways to submit data and information to competent authorities

Article 67-a

- (1) Unless otherwise prescribed by another law, entities shall be obliged to submit the data and information to the competent authorities referred to in Articles 130 and 151 of this Law via protected electronic means. If such method of submission is impossible for technical reasons, entities shall submit the data and information in writing.
- (2) The competent authorities referred to in paragraph (1) of this Article may not disclose the entity and the identity of the employee of the entity that submits the data and information, except in cases where there is suspicion that the employee or entity has committed a criminal offense of money laundering and/or financing of terrorism, upon written request of the competent court when it is necessary to establish facts in the course of criminal proceedings.

Appointment of an authorized person and establishment of a department for the prevention of money laundering and terrorist financing

Article 68

- (1) Entities are obliged to appoint an authorized person and his/her deputy.
- (2) An entity employing only one person is not obliged to appoint a deputy of the authorized person in accordance with paragraph (1) of this Article.
- (3) If the entity employs more than 50 persons who are directly related to the activities for which they are obliged to implement measures and actions for the prevention of money laundering and

terrorist financing, in addition to the obligation referred to in paragraph (1) of this Article, the entity shall, within the framework of its operations, be obliged to establish a separate department for the prevention of money laundering and terrorist financing.

(4) The department referred to in paragraph (3) of this Article shall employ at least four persons if the entity employs 50 to 300 persons, and the number of employees in the department shall increase by one person for every additional 100 employees.

(5) The entity may, based on the results of the risk assessment in the department referred to in paragraph (3) of this Article, employ more persons than the number of persons envisaged in accordance with paragraph (4) of this Article.

(6) The operations of the department referred to in paragraph (3) of this Article shall be managed by the authorized person referred to in paragraph (1) of this Article.

(7) The authorized person, his/her deputy, as well as the employees of the department should meet the following requirements:

a) they have not been convicted of crimes against property, crimes against public finances, payment transactions and the economy, crimes against official duty, crimes against public order and crimes against humanity and international law, etc.;

b) they have at least secondary education, appropriate professional knowledge and experience to perform tasks in the field of preventing money laundering and financing of terrorism and

c) they have good knowledge of the business activity and work processes of the entity.

(8) The heads of the departments referred to in paragraph (6) of this Article and the authorized persons of the money remittance service providers (fast money transfer) shall meet the following conditions:

a) they have not been convicted of crimes against property, crimes against public finances, payment operations and the economy, crimes against official duty, crimes against public order and crimes against humanity and international law, etc.;

b) they have higher education, appropriate professional knowledge and experience to perform tasks in the field of preventing money laundering and financing of terrorism and

c) they have good knowledge of the business activity and work processes of the entity.

(9) In the entities referred to in paragraph (3) of this Article, the authorized person, his deputy, as well as all persons employed in the department referred to in paragraphs (4) and (5) of this Article, are subject to security checks in accordance with the regulations on security of classified information and are required to have a security certificate.

(10) For the purpose of efficient operation of the authorized person, his/her deputy and the employees of the department, the entity shall be obliged to ensure the fulfillment of at least the following conditions:

- separation of the activities of the authorized person, i.e. the department, from other business activities of the entity, which are not related to the activities of preventing money laundering and terrorist financing and control of compliance of operations with regulations,

- independence of the authorized person and the department in the implementation of measures and actions for detecting and preventing money laundering and terrorist financing in accordance with this Law,

- right of direct access to electronic databases and timely access to all information necessary for the smooth implementation of the program and provisions of this Law and

- establishment of direct communication with the management bodies of the entity and other.

(11) Banks and providers of money transfer services (fast money transfers) shall be obliged to appoint an authorized person on duty and his/her deputy who, in the event of an emergency (terrorist act, threats of a terrorist act), shall be immediately available to the Administration, and no later than within three hours. The authorized person on duty and his/her deputy shall meet the requirements of paragraphs (8) and (9) of this Article.

(12) Banks and money transfer service providers (fast money transfer) are obliged to provide the authorized person on duty and his/her deputy with the necessary working conditions in accordance with paragraph (10) of this Article in order to fulfill the obligations of the authorized person on duty and his/her deputy.

(13) The entity shall adopt measures to ensure that employees performing tasks in the field of prevention and detection of money laundering and terrorist financing in accordance with this Law are familiar with the provisions of this Law, including appropriate measures regarding data protection. The measures must be proportionate to the type and size of the entity and the assessed risk of money laundering and terrorist financing.

(14) The entity is obliged to provide regular professional training in the field of prevention and detection of money laundering and terrorist financing in accordance with this Law for all employees.

(15) Entities are obliged to submit to the Administration electronically data on the persons (name, surname and contact) from paragraphs (1) and (11) of this Article, as well as to notify the Administration of any changes. If such method of submission is impossible for technical reasons, the entities shall submit the notification in writing until the moment of removal of such obstacles, i.e. reasons.

Internal control obligation Article 69

Entities are obliged to perform internal control over the implementation of measures and actions for the prevention of money laundering and terrorist financing at least once a year in the current year for the previous year and to prepare documentation on the findings of the internal control conducted.

Implementation of software for automatic data processing Article 70

(1) Banks are obliged to implement and regularly upgrade automatic data processing software in accordance with the characteristics of the automatic data processing software that should meet the regulations on personal data protection.

(2) The Minister of Finance, upon proposal of the Director of the Administration, shall prescribe the characteristics of the software for automatic data processing.

Use of data provided by this law by entities Article 71

(1) The data provided on the basis of this law, including personal data, shall be used solely for the detection and prevention of money laundering and terrorist financing in accordance with the law.

(2) The submission of the data referred to in paragraph (1) of this Article to the Administration and to the relevant supervisory authority under this Law when carrying out supervision in accordance with this Law shall not be considered as disclosure of a business secret or disclosure of classified data and information.

(3) Employees of entities and persons managing entities that have an obligation to take measures and actions to detect and prevent money laundering and terrorist financing, in accordance with this Law, may not use personal data from client files for purposes other than for implementing measures and actions to detect and prevent money laundering and terrorist financing in accordance with the purposes provided for by this Law.

Prohibition on disclosure of data and information

Article 72

(1) The entity and its employees, including the members of the management and supervisory board or other persons to whom the data provided in accordance with this Law or the by-laws adopted in accordance with this Law are accessible in any way, may not notify the client or a third party that:

- 1) an analysis is underway or is possible to determine grounds for suspicion of money laundering or terrorist financing by the Administration;
- 2) data, information or documentation regarding the client or third party or transaction has been or will be submitted to the Administration;
- 3) the Administration has issued an order for monitoring a business relationship or a written order for temporary retention of a transaction;
- 4) pre-investigation actions, investigation or criminal proceedings for money laundering or terrorist financing have been initiated or may be initiated against the client or third party.

(2) The data, information and documentation referred to in paragraph (1) of this Article are classified data for which an appropriate level of classification has been determined in accordance with the regulations for the protection of classified information.

(3) The entity is obliged to take technical and organizational measures to protect the data provided in accordance with the provisions of this Law, which are necessary for the purpose of their protection against accidental loss, destruction or unauthorized access, unauthorized use and any other misuse, and to establish an obligation for the employees who process the data to sign a confidentiality statement.

(4) The prohibition on disclosure of data and information referred to in paragraph (1) of this Article shall not apply, unless the Administration decides otherwise, when:

- a) data and information are exchanged between financial institutions that are part of the same group, provided that they implement the regulations arising from the applicable international regulations and standards for the prevention of money laundering and the financing of terrorism;
- b) data and information are exchanged between entities referred to in Article 5, item 2 of this Law from countries that have the same provisions for the detection and prevention of money laundering and the financing of terrorism as the provisions of this Law, and who carry out their professional activity as part of the same legal entity or as part of a larger ownership or management structure to which the legal entity belongs.

(5) The prohibition on disclosure of data and information referred to in paragraph (1) of this Article shall not apply to data and information relating to the same client or the same transaction involving two or more entities, provided that they implement measures to prevent money laundering and terrorist financing, carry out the same type of activity and are subject to obligations for the protection of business secrets and the protection of personal data.

(6) It shall not be considered disclosure of data and information if the entities referred to in Article 5 of this Law inform the client of the consequences of engaging in or carrying out activities contrary to the law.

Exemption from liability for notification and retention

Article 73

(1) No procedure for determining liability for disclosure of a business secret shall be initiated against persons or the management body and employees of the entities, as well as the supervisory bodies referred to in Article 151 paragraph (1) of this Law, who have submitted information or reports regarding suspicious transactions to the Administration.

(2) No civil or criminal liability procedure may be initiated against the officials or responsible persons, the management body or employees of the entities, as well as the supervisory bodies referred to in Article 151 paragraph (1) of this Law, who have submitted data, information, documents or reports in accordance with the provisions of this Law, even in cases where the procedure based on the information and reports provided has not led to a determination of liability, i.e. a final judgment.

(3) No civil or criminal liability proceedings may be initiated against the officials or responsible persons, the management body and employees of the entities, as well as the supervisory bodies referred to in Article 151, paragraph (1) of this Law, due to material or immaterial damage incurred as a result of withholding transactions in accordance with the provisions of this Law, unless such withholding meets the requirements of a criminal act.

(4) It is prohibited for persons or the management body and employees of the entities, as well as the supervisory bodies referred to in Article 151 paragraph (1) of this Law, who have submitted information or reports regarding suspicious transactions to the Administration to be exposed to threats, retaliatory or hostile actions, negative or discriminatory actions in the employment relationship.

(5) Persons or the management body and employees of the entities, as well as the supervisory bodies referred to in Article 151 paragraph (1) of this Law, who have submitted information or reports regarding suspicious transactions to the Administration, and who are exposed to threats, retaliatory or hostile actions or negative or discriminatory actions in the employment relationship for reporting suspicions of money laundering or terrorist financing, have the right to an effective legal remedy for the protection of their rights in accordance with the law.

Trade secret
Article 74

The invocation of a business secret cannot be accepted as a basis for refusing to provide, submit and provide data, information and documents under this law.

CHAPTER IV.
FINANCIAL INTELLIGENCE ADMINISTRATION
Article 75

(1) The Directorate is a financial intelligence unit of the Republic of North Macedonia, established for the purposes of collecting and analyzing reports on suspicious transactions and other information of importance for preventing and detecting money laundering and terrorist financing and submitting the results of the analysis and other additional relevant information to the competent authorities when there are grounds for suspicion of money laundering and terrorist financing.

(2) The Administration is a state administration body within the Ministry of Finance, with the status of a legal entity.

(3) The Administration shall have the following powers:

- collect, process, analyze, store and submit data obtained on the basis of this Law,
- obtain data, information and documents necessary for the exercise of its powers,
- prepare and submit reports to the competent state authorities whenever there are grounds for suspicion of a crime of money laundering or terrorist financing,
- prepare and submit a notification to the competent state authorities on the existence of grounds for suspicion of another crime,
- issue a written order to the entity temporarily suspending the transaction,

- submit a request for submitting a proposal for determining temporary measures to the competent public prosecutor,
- submit an order for monitoring the business relationship to the entity,
- issue a misdemeanor payment order,
- submit a request for initiating a misdemeanor procedure before the competent court,
- prepare strategic analyses for determining the trends and typologies of money laundering and terrorist financing,
- cooperate with the entities referred to in Article 5 of this Law, with the Ministry of Interior, the Ministry of Defense, the Ministry of Justice, The Ministry of Foreign Affairs, the Public Prosecutor's Office of the Republic of North Macedonia, the Intelligence Agency, the National Security Agency, the Financial Police Directorate, the Customs Administration, the Public Revenue Administration, the State Foreign Exchange Inspectorate, the Securities Commission of the Republic of North Macedonia, the National Bank of the Republic of North Macedonia, the Agency for Supervision of Fully Funded Pension Insurance, the Insurance Supervision Agency, the State Commission for the Prevention of Corruption, the State Audit Office, the Central Registry of the Republic of North Macedonia and other state bodies and institutions, as well as with other organizations, institutions and international bodies for the fight against money laundering and the financing of terrorism,
- concludes cooperation agreements and exchanges data and information with financial intelligence units of other states and international organizations involved in the fight against money laundering and the financing of terrorism,
- independently or in cooperation with the supervisory authorities referred to in Article 151 of this Law, supervises the entities for the implementation of the measures and actions determined by this Law,
- participates in the implementation of a national assessment of the risk of money laundering and the financing of terrorism and conducts risk assessments of certain categories of entities,
- initiates initiatives or provides opinions on laws and bylaws relating to the prevention of money laundering and terrorist financing,
- may assist in the professional development of authorized persons and employees in the department for the prevention of money laundering and terrorist financing in the entities referred to in Article 5 of this Law,
- determines lists of indicators for the recognition of suspicious transactions in cooperation with the entities and bodies that supervise their operations and regularly updates them,
- plans and conducts training for the development and training of employees in the Administration,
- conducts activities aimed at raising awareness of the non-governmental sector about the risks of their possible misuse for the purposes of financing terrorism,
- provides clarification in the application of the regulations for the prevention of money laundering and terrorist financing,
- keeps records, as well as comprehensive statistics for the purposes of assessing the efficiency of the system for combating money laundering and terrorist financing,
- acts in accordance with the provisions of the Law on Restrictive Measures and the by-laws adopted on its basis and
- performs other tasks specified by law.

(4) In order to exercise its powers, the Administration shall have timely direct or indirect electronic access to data, information and documentation held by entities, state bodies and institutions and other legal or natural persons in accordance with the provisions of this Law.

(5) The Administration shall carry out the activities within its competence in accordance with the law and the ratified international agreements regulating the prevention of money laundering and terrorist financing.

(6) Personal data collected for the purposes of this Law shall be used in accordance with this Law and the regulations on personal data protection.

(7) The Administration shall prepare an annual report on the matters within its competence and a work program for the following year and submit them to the Minister of Finance and the Government of the Republic of North Macedonia. The Administration may also submit another report upon request of the Minister of Finance or the Government of the Republic of North Macedonia.

Article 76

(1) The Administration shall exercise its powers throughout the territory of the Republic of North Macedonia.

(2) The seat of the Administration is in Skopje.

Basic principles of the Administration

Article 77

(1) The basic principles of the work of the Administration are:

1) legality - all actions and activities undertaken in the Administration are in accordance with the Constitution of the Republic of North Macedonia, laws and international agreements ratified in accordance with the Constitution and the law;

2) proportionality - in the application of the powers prescribed by law, the powers must be proportionate to the needs for which they are undertaken, taking into account the seriousness of the risks arising from their application, as well as achieving the goal with the least harmful consequences;

3) efficiency - in undertaking the actions and activities, their duration, as well as rational spending of public funds for their effective implementation and

4) impartiality - undertaking the actions and activities without any influence of political, personal financial interests or the existence of any cases of conflict of interest in accordance with the law.

Autonomy and operational independence of the Administration

Article 78

The Administration is autonomous and operationally independent in the exercise of its powers prescribed by this Law and has the authority to exercise its powers completely freely, including making decisions regarding the analysis, request, forwarding and submission of the results of its analyses and information, data and documentation to the competent authorities and financial intelligence units of another country.

Financing the Administration

Article 79

The necessary financial resources for financing the Administration are provided from the Budget of the Republic of North Macedonia.

Article 80

(1) The Administration and its employees shall not be liable for the damage caused to the entities, the clients of the entities or third parties in cases where they act in accordance with the provisions of this Law or the by-laws adopted on its basis.

(2) The Republic of North Macedonia shall not be liable for any damages that may be caused by the application of the provisions of this Law or the by-laws adopted on its basis.

(3) As an exception, the provisions of paragraphs (1) and (2) of this Article shall not apply if the damage was caused intentionally.

Article 81

(1) The Director of the Administration shall be appointed and dismissed by the Government of the Republic of North Macedonia upon the proposal of the Minister of Finance following a public announcement, published in three daily newspapers throughout the territory of the Republic of North Macedonia, one of which shall be published in the language spoken by at least 20% of the citizens who speak an official language other than Macedonian.

(2) The Director of the Administration has a mandate of five years with the possibility of re-election.

(3) A person who meets the following requirements may be appointed as a director:

- 1) to be a citizen of the Republic of North Macedonia;
- 2) to have acquired 240 credits according to ECTS or VII/1 level of education;
- 3) to have at least five years of work experience in the field of preventing money laundering and terrorist financing;
- 4) has not been convicted of crimes against property, crimes against public finances, payment transactions and the economy, crimes against official duty, crimes against public order and crimes against humanity and international law and other crimes and
- 5) possesses one of the following internationally recognized certificates or attestations for active knowledge of the English language:
 - TOEFL IBT at least 74 points,
 - IELTS - at least 6 points,
 - ILEC (Cambridge English: Legal) - at least B2 (B2) level,
 - FCE (Cambridge English: First) - passed,
 - BULATS (BULATS) - at least 60 points or
 - APTIS (APTIS) - at least B2 (B2) level;
- 6) actively uses the Macedonian language;
- 7) possesses a certificate for knowledge of computer programs for office work.

(4) The mandate of the director shall terminate:

- upon the expiration of five years from the date of his/her appointment,
- in the event of death,
- in the event of his/her resignation,
- in the event of dismissal,
- in the event of his/her conviction for a criminal offense with a sentence of imprisonment for a period of at least six months by a final judgment,
- when the court imposes a measure prohibiting him/her from performing the activity of a managerial person in the institution and
- if he/she has lost his/her legal capacity.

(5) The Director may be dismissed due to:

- illegal operations,
- unprofessional performance of the duties of the Director,

- in the event of a long-term serious illness that prevents him from performing his duties and
- at his request.

(6) The Director manages and represents the Administration, organizes and ensures the legal, efficient and professional performance of the Administration's affairs, adopts decisions, orders and internal orders, instructions, plans and programs, warnings with recommendations and other acts in accordance with the law.

(7) The Director may authorize a financial intelligence officer from category A referred to in Article 87, paragraph (1) of this Law, in the event of his absence or inability to sign acts referred to in paragraph (6) of this Article.

Article 82

The Director of the Directorate and its employees are subject to security checks in accordance with the regulations for the security of classified information.

Article 83

(1) In the Administration, the employee positions are grouped into groups and subgroups in accordance with the Law on Public Sector Employees:

- 1) positions of administrative servants;
- 2) positions of authorized officials and
- 3) positions of auxiliary and technical personnel.

Article 84

(1) The employees of the Administration referred to in Article 83 of this Law shall have an official identification card.

(2) The form, content, manner of issuing, confiscating and using the official identification card shall be prescribed by the Minister of Finance upon the proposal of the Director.

Article 85

(1) Employees of the Administration who perform tasks of an administrative nature have the status of administrative servants.

(2) The provisions of the Law on Administrative Servants shall apply to issues relating to classification, employment, salary system, promotion, professional development and training, performance measurement and other issues related to the employment relationship of administrative servants.

Article 86

(1) Employees of the Administration who perform support and technical work have the status of support and technical personnel.

(2) For issues related to the classification, records, employment and mobility of employees referred to in paragraph (1) of this Article, the Law on Public Sector Employees shall apply, and for other issues related to the employment relationship, the general regulations on employment relations and collective agreements shall apply.

CHAPTER V.
RIGHTS, OBLIGATIONS AND RESPONSIBILITIES OF EMPLOYED AUTHORIZED OFFICIALS IN THE
ADMINISTRATION

Classification of jobs of authorized officials in the Administration

Article 87

(1) The following job categories shall be established for authorized officials in the Administration:

- category A - managerial personnel - financial intelligence officers and
- category B - financial intelligence officers.

(2) Within category A, the following job levels are determined:

- level A1 - head of department - financial intelligence officer,
- level A2 - assistant head of department - financial intelligence officer and
- level A3 - head of department - financial intelligence officer.

(3) Within category B, the following job levels are determined:

- level B1 - independent financial intelligence officer,
- level B2 - senior financial intelligence officer,
- level B3 - financial intelligence officer and
- level B4 - junior financial intelligence officer.

Article 88

(1) This Law, the Law on Labor Relations, the Law on Public Sector Employees and the regulations in the field of health, pension and disability insurance and collective agreements shall apply to the authorized officials of the Administration, unless otherwise provided for by this Law.

(2) The employment of authorized officials in the Administration shall be carried out in accordance with the Law on Public Sector Employees.

(3) The mobility of authorized officials in the Administration shall be carried out in accordance with the Law on Public Sector Employees.

Hiring a financial intelligence officer

Article 89

(1) A person who meets the general conditions provided for by this Law and the special conditions provided for by this Law and the act on systematization of jobs in the Administration may be employed as a financial intelligence officer in the Administration.

(2) A person who meets the following general requirements may be employed as a financial intelligence officer:

- 1) is a citizen of the Republic of North Macedonia;
- 2) is psychophysically healthy (capable) to perform the tasks prescribed by the systematization act;
- 3) actively uses the Macedonian language;
- 4) is of legal age;
- 5) has not been sentenced by a final court verdict to a ban on performing a profession, activity or duty;
- 6) a security check by a competent authority has determined that there is no security risk from the person's employment.

(3) In addition to the general conditions referred to in paragraph (2) of this Article, a person who meets the following special conditions may be employed as a financial intelligence officer:

- 1) professional qualifications for all levels of category A and B - qualification level VI A according to the Macedonian Qualifications Framework and acquired at least 180 credits according to ECTS or

240 credits according to ECTS or completed VII/1 level of education.

2) to have work experience in the profession, as follows:

- for level A1 - at least seven years of work experience in the profession, of which at least three years in a managerial position in the public sector,
- for level A2 - at least six years of work experience in the profession, of which at least one year in a managerial position in the public sector,
- for level A3 - at least five years of work experience in the profession, of which at least one year in a public sector position,
- for level B1 - at least three years of work experience in the profession,
- for level B2 - at least two years of work experience in the profession,
- for level B3 - at least one year of work experience in the profession and
- for level B4 - with or without work experience;

3) to have completed appropriate education prescribed by the act on systematization of jobs in the Administration;

4) to have active knowledge of one of the three most commonly used languages (English, French or German) and

5) active knowledge of computer programs for office work.

Termination of employment of the financial intelligence officer

Article 90

(1) The employment of a financial intelligence officer shall be terminated if:

- a) he/she requests it himself/herself;
- b) he/she permanently loses the health capacity to perform the duties in the Directorate as a result of illness or a decrease in physical or mental capacities;
- c) if it is determined that during employment he/she has remained silent or provided false information regarding the general and special conditions of employment, with the date of the finality of the decision or with the expiration of the deadline for deciding on an appeal against the decision;
- d) he/she has been imposed a disciplinary measure of termination of employment with the date of delivery of the final decision;
- e) due to serving a prison sentence, he/she must be absent from work for longer than six months - with the date of the referral to serve the sentence;
- f) he/she meets the conditions for retirement in accordance with this Law and
- e) he/she is assessed with a grade of "unsatisfactory" three times consecutively or at least three times in the last five years.

(2) The Minister of Finance shall decide on the termination of the employment relationship.

Rights and obligations of the financial intelligence officer

Article 91

(1) Financial intelligence officers have the obligation:

- a) to perform their work tasks conscientiously, professionally, efficiently, orderly and timely in accordance with the Constitution, law and other regulations;
- b) to carry out the orders of their immediate superior and to act upon them in accordance with the Constitution, law and other regulations;

- c) to respect the prescribed working hours and
 - d) to use the equipment provided to them for the performance of their duties with due care and as a good steward in accordance with its intended purpose and not to use it for private purposes.
- (2) In addition to the obligations referred to in paragraph (1) of this Article, the financial intelligence officer shall also have the following obligations:
- a) to perform his/her work impartially and without influence from political parties, not to be guided by his/her political beliefs, personal financial interests, not to abuse his/her authority and status and to protect the reputation of the Administration;
 - b) to professionally improve his/her knowledge in order to advance professional requirements by constantly respecting and applying the regulations for the performance of his/her official duties;
 - c) to behave in accordance with the Code of Conduct for employees of the Administration;
 - d) to respect all security measures in order to avoid endangering his/her life and health, as well as the life and health of other employees of the Administration and
 - e) not to use privileges and exemptions, request or receive material or other benefits in the fulfillment of his/her official duties.
- (3) Financial intelligence officers are obliged to handle and store classified information in accordance with the regulations on classified information.
- (4) Financial intelligence officers are obliged to collect, process and store personal data in accordance with the provisions of this Law and the regulations on personal data protection.
- (5) Financial intelligence officers shall be subject to disciplinary, misdemeanor and criminal liability in accordance with the law for failure to comply with the obligations prescribed in paragraphs (1), (2), (3) and (4) of this Article.

Article 92

- (1) The Administration plans, organizes and conducts training for employees.
- (2) With an employee who is sent for training whose value exceeds ten average salaries paid in the Republic of North Macedonia in the last month prior to the referral, the Administration shall conclude a written agreement regulating the rights and obligations of the contracting parties.
- (3) The employee who fails to fulfill the obligations under the concluded contract referred to in paragraph (2) of this Article shall be obliged to reimburse the costs incurred for his training increased by three times.

Salary, insurance and benefits of a financial intelligence officer

Article 93

- (1) Financial intelligence officers are entitled to salaries, salary allowances and other benefits provided by the Budget of the Republic of North Macedonia.
- (2) The financial intelligence officer, due to the specifics of the work he performs, is entitled to a salary increased by 30% of the base salary determined by the act on payment of salary and allowances.
- (3) In the event of temporary incapacity for work, arising during or in connection with the performance of the work and tasks, the financial intelligence officer shall be entitled to compensation in the amount of the current salary for the period of absence from work.
- (4) In accordance with the regulations on pension and disability insurance, the insurance period of the financial intelligence officer shall be considered to have an increased duration, so that the age limit for acquiring the right to an old-age pension shall be reduced depending on the degree of increase in the length of service, by one year for every four years spent in jobs where 12 months effectively spent shall be considered as 15 months in the insurance period.

(5) The Administration shall insure financial intelligence officers in the event of death, bodily injury or loss of working capacity while performing the tasks within their jurisdiction.

Termination of employment contract of financial intelligence officer due to employee's age Article 94

The Administration terminates the employment contract of the financial intelligence officer when the employee reaches 64 years of age and 15 years of retirement service.

Right to a one-time compensation in the form of severance pay Article 95

A financial intelligence officer who has acquired the right to a pension is entitled to a one-time compensation in the form of severance pay, in accordance with a collective agreement.

Article 96

Financial intelligence officers, when exercising their powers, have special rights to enter and have free access to stations, airports, ports and public parking lots only upon presentation of official identification.

Article 97

(1) The financial intelligence officer, depending on the exceptional and above-average results achieved in his work, professional knowledge and abilities in work, commitment, creativity and conscientiousness in the performance of official duties, may be promoted to a higher position by decision of the director, and upon prior consent of the Minister of Finance.

(2) The financial intelligence officer may be promoted if he/she meets the following conditions:

- the position to which he/she is being promoted is vacant (unfilled or vacant),
- he/she fully meets the requirements set out in the act on systematization of positions for the position to which the promotion is being made,
- he/she has completed the trainings set out for the position to which he/she is being promoted,
- he/she has been assessed with the grades "outstanding" or "satisfactory" in the manner and under the conditions set out in this Law,
- at least one year has passed since his/her last promotion and
- in the last 12 months he/she has not been punished for violating the work order and discipline or failing to fulfill the work obligations set out in the law.

Article 98

(1) Financial intelligence officers shall be evaluated once a year during their work by their immediate superior financial intelligence officer. In the absence of an immediate superior financial intelligence officer, the evaluation shall be performed by the higher financial intelligence officer in accordance with the systematization act. In the absence of a higher financial intelligence officer in accordance with the systematization act, the evaluation shall be performed by the Director of the Directorate.

(2) Financial intelligence officers who have been justifiably absent from work for more than six months during the year (sick leave, unpaid leave, etc.) will not be evaluated.

(3) The evaluation of financial intelligence officers shall be carried out on the basis of data relating to the following criteria:

- professional knowledge and working skills,

- commitment,
- achieved results,
- creativity and
- conscientiousness.

(4) The criteria referred to in paragraph (3) of this Article shall be assessed individually, numerically with a score from one to four and descriptively with the following descriptive scores: "outstanding", "satisfactory", "partially satisfactory" and "not satisfactory".

(5) The financial intelligence officer who is not satisfied with the evaluation may, within eight days from the day of the evaluation, submit a request for review of the evaluation to the Evaluation Review Commission, which is formed by the director.

(6) The financial intelligence officer who is not satisfied with the decision of the Commission for review of the assessment within eight days from the date of delivery of the decision has the right to file an appeal through the Directorate to the State Commission for Decision-making in Administrative Procedures and Employment Procedures in Second Instance.

(7) The method of evaluating the performance of financial intelligence officers, the types of reports, the form and content of the evaluation form and other forms shall be prescribed by the Minister of Finance upon the proposal of the Director.

Article 99

(1) The Code of Conduct describes the standards of conduct that should be observed by all employees and provides guidance and instructions for resolving ethical issues for those who work in the Authority and those who cooperate and work with the employees of the Authority.

(2) The Code of Conduct shall be prescribed by the Minister of Finance upon the proposal of the Director.

Article 100

(1) For violation of work rules and discipline or failure to fulfill work obligations, the financial intelligence officer shall be subject to disciplinary action.

(2) Liability for a committed criminal act does not exclude the disciplinary liability of the financial intelligence officer.

Article 101

(1) The financial intelligence officer shall be subject to disciplinary action for disciplinary misconduct and disciplinary offense.

(2) Disciplinary misconduct, within the meaning of paragraph (1) of this Article, is a minor violation of work discipline, work tasks, the reputation of the Administration and the employees.

(3) A disciplinary offense, within the meaning of paragraph (1) of this Article, is a serious violation of work discipline, work tasks, the reputation of the Administration and the employees.

Article 102

(1) The financial intelligence officer commits disciplinary misconduct, i.e. a minor violation of work discipline, work tasks, the reputation of the Directorate and its employees, when:

- 1) does not respect the work order and discipline;
- 2) does not perform or performs work obligations negligently and untimely;

- 3) does not comply with the regulations applicable to the performance of work at the workplace;
- 4) does not comply with the established working hours, schedule and use of working hours;
- 5) does not request leave or does not promptly notify the director in writing, i.e. the immediate manager or another responsible employee of the absence from work;
- 6) is absent from work due to illness or justified reasons, and does not immediately or at the latest within 24 hours notify the director, i.e. the immediate manager or another responsible employee;
- 7) does not handle work equipment conscientiously or in accordance with the technical work instructions;
- 8) damage, operational error or loss occurs, and does not immediately notify the director, i.e. the head of the organizational unit or another responsible employee;
- 9) fails to maintain the means and equipment for occupational safety in accordance with the regulations for occupational safety;
- 10) causes disorder and behaves violently during work;
- 11) illegally or without authorization uses the assets of the Administration and
- 12) avoids training.

Article 103

The financial intelligence officer commits a disciplinary offense, i.e. a serious violation of work discipline, work tasks, the reputation of the Administration and its employees, if:

- 1) is unjustifiably absent from work for three consecutive working days or five working days within a year;
- 2) abuses sick leave;
- 3) fails to comply with the regulations on health protection, occupational safety, fire, explosion, harmful effects of poisons and other hazardous substances and violates the regulations on environmental protection;
- 4) brings in, uses or is under the influence of alcohol and narcotics;
- 5) commits theft or in connection with work intentionally or through extreme negligence causes damage to the Administration;
- 6) fails to comply with the provisions of the Law on Classified Information;
- 7) misuses personal data;
- 8) abuses or exceeds legal obligations and authorizations;
- 9) avoids a medical examination to determine working capacity;
- 10) unlawfully obtains personal benefit in connection with the performance of the work and tasks;
- 11) performs a service or enables a service to another person with money or other valuable things entrusted to the financial intelligence officer in the performance of the work and tasks and
- 12) establishes, manages, represents, presents a political party, is a member of the party's bodies determined by its statute, expresses and represents party positions and beliefs in the performance of the work and tasks, carries or displays party symbols in the premises or in the official vehicles of the Administration and organizes or acts in a party manner within the Administration.

Article 104

(1) In case of disciplinary misconduct, the financial intelligence officer may be imposed one of the following disciplinary measures by decision:

- 1) a written warning or
- 2) a fine in the amount of 15% of the last paid monthly net salary of the financial intelligence officer, for a period of one to three months.

(2) In the event of a disciplinary offense, the financial intelligence officer may be imposed one of the following disciplinary measures by decision:

- 1) a fine in the amount of 15% of the last paid monthly net salary of the financial intelligence officer, for a period of three to six months;
- 2) assignment to a job that, in accordance with the hierarchy of jobs determined in the act on systematization of jobs in the Directorate, is one level lower than the job from which the financial intelligence officer was assigned or
- 3) termination of the employment contract.

(3) When imposing the disciplinary measures referred to in paragraphs (1) and (2) of this Article, the degree of responsibility, the conditions under which the violation of work discipline was committed, the work tasks, the reputation of the Administration and the employees, the previous work and behavior of the employee, the severity of the violation and its consequences, the circumstances under which the violation was committed and other mitigating and aggravating circumstances shall be taken into account.

Article 105

The sum of fines imposed on a financial intelligence officer in one month for violation of work discipline, work tasks, the reputation of the Administration and its employees cannot exceed 20% of the amount of his total net salary for that month.

Article 106

(1) Disciplinary measures against a financial intelligence officer for disciplinary misconduct shall be imposed upon a proposal from the immediate superior financial intelligence officer, the higher superior financial intelligence officer or superior financial intelligence officer at the same level, which shall be simultaneously submitted to the director and to the financial intelligence officer against whom the proposal is submitted.

(2) The financial intelligence officer against whom the proposal is submitted has the right, within three days from the date of receipt of the proposal referred to in paragraph (1) of this Article, to comment on the proposal, i.e. to provide a written response.

(3) The director shall impose disciplinary measures against the financial intelligence officer for disciplinary misconduct within eight days from the date of receipt of the written response referred to in paragraph (2) of this Article.

(4) Against the decision referred to in paragraph (3) of this Article, the dissatisfied financial intelligence officer has the right to file an appeal with the State Commission for Decision-making in Administrative Procedures and Labor Procedures in Second Instance within eight days from the receipt of the decision.

Article 107

A proposal to initiate a procedure for determining the disciplinary liability of a financial intelligence officer for a disciplinary offense may be submitted by the immediate managing financial intelligence officer, the higher managing financial intelligence officer or the managing financial intelligence officer at the same level. The proposal must be substantiated and supported by facts and evidence.

Article 108

- (1) In order to conduct a procedure for determining disciplinary liability of the financial intelligence officer for a disciplinary offense in the cases determined by this Law, the director shall, within eight days from the date of submission of a proposal for initiating a disciplinary procedure, establish a commission for determining disciplinary liability.
- (2) The Commission referred to in paragraph (1) of this Article shall be composed of financial intelligence officers, namely a chairman from among the senior financial intelligence officers and two members, one of whom, if possible, shall be a financial intelligence officer with the same rank as the financial intelligence officer against whom disciplinary proceedings are being conducted. The chairman and the members shall have their deputies.
- (3) The Commission referred to in paragraph (1) of this Article shall conduct the procedure for determining disciplinary liability in accordance with this Law.
- (4) The Commission referred to in paragraph (1) of this Article, after conducting the disciplinary procedure, if it determines that the financial intelligence officer is responsible, shall propose to the director to adopt an appropriate disciplinary measure.
- (5) If the committee referred to in paragraph (1) of this Article determines that the financial intelligence unit is not responsible, it shall propose to the director to reject the proposal or to stop the procedure.
- (6) The Director, based on the proposal of the Commission, shall adopt a decision to impose a disciplinary measure, reject the proposal or terminate the procedure within three days of receiving the proposal referred to in paragraph (5) of this Article. The decision to impose a disciplinary measure shall also contain an explanation of the grounds and reasons for imposing the disciplinary measure.
- (7) The decision to impose a disciplinary measure shall be delivered personally to the financial intelligence officer, as a rule, at the office of the Directorate, i.e. at the address of the residence or place of stay.
- (8) If the financial intelligence officer refuses the delivery, the decision shall be published on the notice board in the Office. After three working days from the date of publication on the notice board, the delivery shall be deemed to have been made.
- (9) Against the decision to impose a disciplinary measure or reject the proposal, i.e. to stop the procedure, the financial intelligence officer has the right to appeal through the Directorate to the State Commission for Decision-making in Administrative Procedures and Employment Procedures in Second Instance, within eight days from the date of delivery of the decision.
- (10) The appeal shall stay the execution of the decision until a final decision is made or the deadline for the State Commission for Decision-Making in Administrative Procedures and Employment Procedures in Second Instance has expired. The Administration shall be obliged to submit the appeal, with the accompanying documents, to the State Commission for Decision-Making in Administrative Procedures and Employment Procedures in Second Instance, within eight days of receipt of the appeal.
- (11) The disciplinary procedure shall be completed within 60 days from the date of adoption of the decision to establish the commission referred to in paragraph (1) of this Article.

Article 109

- (1) Until a decision is made in a disciplinary procedure conducted against a financial intelligence officer, the financial intelligence officer shall be removed from the workplace and from the Directorate by a written decision - decision in the cases determined by the regulations on labor relations, if one of the following situations occurs:

- the life or health of workers or other persons is directly endangered or assets of greater value are damaged,
- the presence at the workplace and further work will have a detrimental effect on the operations of the Directorate and
- when criminal proceedings have been initiated against the financial intelligence officer for a crime committed at work or in connection with the work.

(2) During the period of removal from the workplace and from the Directorate, the financial intelligence officer shall be determined and paid compensation in the amount of 60% of the net salary that the financial intelligence officer earned in the month prior to the removal from the workplace.

(3) The decision referred to in paragraph (1) of this Article shall be adopted by the director.

(4) The decision referred to in paragraph (1) of this Article shall be delivered personally to the financial intelligence officer, as a rule, at the office of the Administration, i.e. at the address of the residence or place of stay.

(5) If the financial intelligence officer refuses the delivery, the decision shall be published on the notice board in the Directorate. After three working days from the date of publication on the notice board, the delivery shall be deemed to have been made.

(6) The financial intelligence officer has the right to appeal against the decision referred to in paragraph (1) of this Article to the State Commission for Decision-making in Administrative Procedures and Employment Procedures in Second Instance, within eight days from the date of delivery of the decision.

(7) The appeal against the decision referred to in paragraph (1) of this Article shall not postpone the execution of the decision.

(8) In the event of reinstatement and if no disciplinary liability is established, the financial intelligence officer shall be entitled to retroactive compensation in the amount of 100% of the net salary.

Article 110

If a financial intelligence officer is ordered to terminate his employment contract due to a disciplinary offense, the financial intelligence officer has the right to a notice period of 30 days from the date of delivery of the decision to terminate the employment contract.

Article 111

During the notice period, the Directorate is obliged to allow the financial intelligence officer six hours of leave from work during the working week to seek new employment.

Article 112

During the notice period and absence from work due to seeking new employment, the financial intelligence officer shall be determined and paid compensation in the amount of the salary that the financial intelligence officer earned in the month prior to the adoption of the decision to terminate the employment contract.

Article 113

(1) Disciplinary proceedings against a financial intelligence officer may not be initiated if one month has passed from the day on which the immediate or higher-ranking financial intelligence officer or the director learned of the committed disciplinary offense.

(2) Disciplinary proceedings against a financial intelligence officer may not be initiated if three months have passed since the day the disciplinary offense was committed.

(3) When a criminal procedure is initiated against the financial intelligence officer for a committed disciplinary offense, the decision to impose a disciplinary measure shall be adopted no later than the expiration of the statute of limitations for criminal prosecution of the relevant criminal offense.

Article 114

(1) The financial intelligence officer shall be liable for any damage caused to the Administration during or in connection with his/her work, whether intentionally or through gross negligence.

(2) The Director shall form a commission for determining the material liability of the financial intelligence officer, composed of financial intelligence officers employed by the Administration, including a chairman from among the senior financial intelligence officers and two members, one of whom, if possible, shall be a financial intelligence officer with the same title as the financial intelligence officer against whom disciplinary proceedings are being conducted. The chairman and the members shall have their deputies.

(3) The Commission referred to in paragraph (2) of this Article shall determine the material liability for the existence of material damage, its amount and the manner of committing it, who caused the damage and who will compensate for it.

(4) The Commission referred to in paragraph (2) of this Article shall submit a report on the established factual situation, on the basis of which the Director shall adopt a decision on compensation for damage.

Article 115

A proposal to initiate a procedure for determining material liability against a financial intelligence officer shall be submitted by the immediate superior financial intelligence officer, the higher superior financial intelligence officer or the superior financial intelligence officer at the same level.

Article 116

The procedure for determining material liability cannot be initiated if 60 days have passed from the day when the directly managing financial intelligence officer or the higher managing financial intelligence officer learned about it.

Article 117

The procedure for determining material liability cannot be initiated if one year has passed since the day the material damage was committed.

Article 118

The procedure for determining material liability cannot be conducted for longer than 60 days, counted from the day of adoption of the decision to establish the commission for determining the material liability of the financial intelligence officer.

Article 119

(1) The financial intelligence officer has the right to appeal against the decision on compensation for damage to the State Commission for Decision-making in Administrative Procedures and Employment Procedures in Second Instance through the Directorate, within eight days from the date of delivery of the decision.

(2) The appeal shall stay the execution of the decision until a final decision is made or the expiry of the deadline within which the State Commission for Decision-Making in Administrative Procedures and Employment Procedures in Second Instance should have made a decision.

Article 120

The procedure for determining the material liability of the financial intelligence officer is regulated by a decision adopted by the director.

Article 121

If the financial intelligence unit fails to compensate the damage within three months of the finality of the decision on compensation for damage, the Directorate shall initiate proceedings before the competent court.

Article 122

The Director may fully or partially exempt the financial intelligence officer from compensation for damage, if it was not caused intentionally or if the payment of compensation for damage endangers the existence of the financial intelligence officer and his family.

Article 123

(1) For many years of professional work, organizational promotions, success in performing work tasks, and improving the reputation of the service, financial intelligence officers are awarded recognition.

(2) Financial intelligence officers may also receive a one-time cash reward for achieving above-average, exceptional results in their work.

Article 124

(1) The awards and prizes referred to in Article 123 of this Law shall, as a rule, be awarded on the day of the Administration.

(2) The Minister of Finance shall decide on the awarding of awards and cash prizes upon the proposal of the Director.

(3) The Day of the Board is March 1.

Analysis and processing of data, information and documentation

Article 125

The Administration is competent to collect and perform analysis based on the following types of data, information and documentation:

- 1) on suspicion of money laundering and terrorist financing submitted by entities based on Article 65 of this Law;
- 2) submitted by entities based on Articles 63 and 64 of this Law;
- 3) initiative of the competent authorities in accordance with Article 130 of this Law;
- 4) submitted by the Customs Administration based on Article 141 of this Law;
- 5) submitted on the basis of Article 156 of this Law and
- 6) received from the financial intelligence units of other countries.

Article 126

The data, information and documentation collected by the Administration in accordance with this Law shall be analyzed within the framework of:

a) operational analysis relating to persons, transactions, activities, property covered by data, information and documentation at the disposal of the Administration in accordance with this Law and

b) strategic analysis relating to determining trends and typologies of money laundering or terrorist financing.

Article 127

(1) The data, information and documentation collected, analyzed, processed and submitted by the Administration in accordance with this Law are classified and have an appropriate level of classification determined in accordance with the regulations on classified data.

(2) The data, information and documentation collected, analyzed, processed and submitted by the Administration shall be used in accordance with this Law.

Request for data, information and documentation by the Administration

Article 128

(1) In order to exercise its powers, the Administration may request data, information and documentation from state bodies, entities or other legal or natural persons in accordance with the provisions of this Law.

(2) State bodies, entities or other legal or natural persons shall be obliged to submit the requested data to the Administration by protected electronic means, no later than ten working days from the date of receipt of the request referred to in paragraph (1) of this Article. If such a method of submission is impossible for technical reasons, the requested data shall be submitted in writing or through the National Interoperability Platform.

(3) If the Administration urgently requests data, state bodies, entities or other legal or natural persons are obliged to submit the requested data by protected electronic means or through the National Interoperability Platform within four hours at the latest. If this method of submission is impossible for technical reasons, the requested data shall be submitted in writing.

Electronic access to data, information and documentation by the Administration

Article 129

(1) In order to carry out the powers determined by this Law, the Administration shall be provided with electronic access and the right to use data from the databases, free of charge, from:

1) Ministry of Internal Affairs, data on: personal name; parents' names; maiden name (or last name before marriage); date of birth; EMBG; citizenship; gender; place and country of birth; municipality; address of residence (place, municipality, street, number and country); ID card number; authority that issued the ID card; nationality; former citizenship, i.e. citizenship acquired; passport number; whether departure abroad has been reported; whether a missing, lost and incorrect travel document has been reported; foreigner (EMBG, ID card); entry and exit from the country; household members; criminal records; possession of collector's weapons; ownership of motor vehicles and watercraft, etc.;

2) Ministry of Justice data on corruption and money laundering cases from the electronic case management system for international legal assistance;

3) Pension and Disability Insurance Fund data on a natural person (name, surname and EMBG) insured in accordance with the regulations on pension and disability insurance and status, for years of service, pensioner (name, surname and EMBG) and pensioner status; 4

) Health Insurance Fund data on a natural person (name, surname and EMBG) insured in accordance with the regulations on compulsory health insurance;

5) Public Revenue Office data on: legal (EMBS and EDB) or natural person (name, surname and EMBG) from the tax register; data from tax returns; paid, collected and refunded VAT, tax audits conducted, taxpayers making cash payments and authorized accountants (legal entity (EMBS and

EDB) or natural person (name, surname and EMBG)) of legal entities;

6) Employment Agency data on: natural person (name, surname and EMBG) contained in (historical) M1/M2 form, list of natural persons (name, surname and EMBG) employed in a certain legal entity (EMBS and EDB) and other;

7) Real Estate Cadastre Agency data on: natural person (name, surname and EMBG) and legal entity (EMBS and EDB) for ownership, for property list, for movement of property ownership, for spatial unit, data on prices and leases and other;

8) Central Securities Depository data on: natural person (name, surname and EMBG) and legal entity (EMBS and EDB) for ownership of securities, for settlements of trade transactions, for non-trade transfer of securities, borrowed securities and other;

9) Data from a single register of transaction accounts - Clearing House "KIBS" AD Skopje for natural persons (name, surname and EMBG) and legal entities (EMBS and EDB) holders of active denar transaction accounts;

10) Credit bureau data on credit exposure of a natural person (name, surname and EMBG) and a legal entity (EMBS and EDB) from the portal MY.MKB.MK;

11) Central register of data on a natural person (name, surname and EMBG) and a legal person (EMBS and EDB) appearing in:

- trade register and register of other legal entities,
- register of annual accounts,
- pledge register,
- leasing register,
- register of investments in real estate,
- register of rights to real estate,
- register of direct investments of residents abroad,
- register of direct investments of non-residents in the Republic of North Macedonia,
- register of natural and legal persons who have been imposed a sanction of prohibition from performing a profession, activity or duty and a temporary prohibition from performing a certain activity,
- register of secondary penalties for committed criminal acts of legal persons,
- register for security by transfer of ownership of objects and transfer of rights (fiduciary register),
- register for sale of movables with retention of the right of ownership,
- register of beneficial owners and
- single register of accounts;

12) Customs Administration of the Republic of North Macedonia data on a natural person (name, surname and EMBG) and a legal entity (EMBS and EDB) from the following records:

- for customs declarations of a natural person,
- for customs declarations of a legal entity,
- for executed imports and executed exports,
- for excise duty bonds,
- for a single customs document,
- for imported, exported foreign currency and securities,
- for filed criminal charges and misdemeanor proceedings;

13) Financial Police Administration data on a natural person (name, surname and EMBG) and a legal entity (EMBS and EDB) for filed criminal charges;

14) Courts for data on a natural person (name, surname and EMBG) and a legal entity (EMBS and EDB) from:

- records of conducting criminal proceedings against a certain person,
- judgments passed,
- criminal records,

- records of a ban imposed on a certain person to perform an activity,
 - records of revoked or limited business capacity of persons,
 - records of achieved international cooperation;
- 15) Ministry of Social Policy, Demography and Youth data on a natural person (name, surname and EMBG) beneficiary of social assistance;
- 16) State Audit Office data on a legal entity (EMBS and EDB) on performed audits and other data from the electronic audit management system;
- 17) Macedonian Stock Exchange data on a legal entity (EMBS and EDB) contained in MB NET, on concluded transactions, including block transactions and other;
- 18) Public Prosecutor's Office of the Republic of North Macedonia data on natural persons (name, surname and EMBG) and legal entities (EMBS and EDB) for criminal charges received, charges filed, measures imposed to secure property during the procedure, international inter-prosecutorial cooperation achieved, etc.;
- 19) Ministry of Economy and Labor data on natural persons (name, surname and EMBG) and legal entities (EMBS and EDB) who have concluded concession agreements;
- 20) State Statistical Office statistical data by area, general and regional statistics, population and social statistics, income, consumption and prices, economy and finance, industry, construction and energy, foreign trade, transport, tourism, trade and other services and multi-domain statistics;
- 21) Competent authority in accordance with the law for maintaining the Central Population Register, data on a natural person (name, surname and EMBG) from the Central Population Register and
- 22) Public Procurement Bureau data on a natural person (name, surname and EMBG) and a legal entity (name, EMBS and EDB) that have concluded a public procurement contract.
- (2) The access and manner of using the data from the databases of the authorities referred to in paragraph (1) of this Article is determined by the law governing electronic governance and electronic services and is regulated by memorandums of cooperation concluded between the Administration and the competent authority referred to in paragraph (1) of this Article.

Submitting an initiative to the Administration

Article 130

- (1) The Public Prosecutor's Office of the Republic of North Macedonia, the Ministry of Internal Affairs, the Ministry of Finance - Financial Police Directorate, the Ministry of Finance - Customs Directorate, the Intelligence Agency, the Ministry of Defense - Sector - Military Security and Intelligence Service, the National Security Agency and the State Commission for the Prevention of Corruption may submit an initiative to the Directorate, if there are reasons to suspect money laundering and terrorist financing.
- (2) The initiative to conduct an analysis referred to in paragraph (1) of this Article in writing, submitted in a secure manner, should contain:
- 1) data on the person to whom the initiative refers, namely:
 - natural person name, surname, date of birth, identification document number, place of residence, or residence, EMBG and
 - legal person name, registered office, EMBS, EDB and other data;
 - 2) the reasons for suspicion of money laundering and/or financing of terrorism, as well as data on the type and manner of committing a previous criminal act, which have been determined in the course of exercising the powers.
- (3) When the initiative referred to in paragraph (1) of this Article is not substantiated and does not contain the data referred to in paragraph (2) of this Article, the Administration shall return the initiative to the body that submitted it for additions and shall inform it that it will not act upon the

submitted initiative if the competent body fails to act within the deadline set by the Administration, which may not exceed 10 working days.

(4) When the Administration acts upon the initiative referred to in paragraph (1) of this Article and determines that there are grounds for suspicion of a crime of money laundering and/or financing of terrorism or another crime, the Administration shall act in accordance with Article 131 of this Law.

(5) The Administration may submit data in the form of a response to the body referred to in paragraph (1) of this Article that submitted the initiative in cases where the elements referred to in Article 131 paragraphs (1) and (4) of this Law have not been determined.

(6) For the purposes of combating money laundering, related criminal offences and the financing of terrorism, the Administration may exchange data available in its databases with the authorities referred to in paragraph (1) of this Article and Article 151 paragraph (1) of this Law upon their reasoned request in writing or on its own initiative.

Submission of data to competent authorities

Article 131

(1) Whenever there are grounds for suspicion of a crime of money laundering and/or financing of terrorism, the Directorate shall prepare and submit a report to the Basic Public Prosecutor's Office for the Prosecution of Organized Crime and Corruption.

(2) If the grounds for suspicion of a criminal offense of money laundering and/or terrorist financing are based on a prior initiative by the competent authorities referred to in Article 130 of this Law, the Administration shall prepare and submit a report to the Basic Public Prosecutor's Office for Prosecution of Organized Crime and Corruption and to the competent authority that submitted the initiative referred to in Article 130 of this Law.

(3) The report referred to in paragraphs (1) and (2) of this Article shall contain data, information and documents about the person and the actions suspected of being related to money laundering and/or terrorist financing.

(4) When there are grounds for suspicion of a criminal offense other than money laundering and terrorist financing, the Administration shall prepare and submit a report to the competent state authorities.

(5) The competent authorities referred to in paragraphs (1) and (2) of this Article shall be obliged to inform the Administration electronically and on a regular basis, at least every six months, about the results and outcome of the report referred to in paragraphs (1) and (2) of this Article and the notification referred to in paragraph (4) of this Article received from the Administration.

Order for monitoring a business relationship

Article 132

(1) When there is suspicion of money laundering and/or terrorist financing, the Administration may submit to the entity an order in writing to monitor the client's business relationship.

(2) The entity shall notify the Administration of the transactions that are carried out or are to be carried out within the framework of the business relationship in accordance with the instructions given in the order.

(3) In the order referred to in paragraph (1) of this Article, the Administration shall determine the deadlines within which the entity is obliged to submit the data on the transactions referred to in paragraph (2) of this Article.

(4) If, due to objective circumstances, the entity cannot notify the Administration within the deadlines referred to in paragraph (3) of this Article, it is obliged to notify the Administration

immediately after the circumstances have been eliminated and to explain the reason for not submitting the notification within the specified deadline.

(5) The monitoring of the business relationship referred to in paragraph (1) of this Article may last for a maximum of three months, and in justified cases the duration of the measure may be extended by one month, whereby the monitoring of the business relationship may last for a maximum of six months.

(6) As an exception to paragraph (5) of this Article, for the purposes of preventing terrorist financing, the duration of the measure may be extended as long as it is needed, depending on the purpose for which the measure is implemented.

Temporary measures

Article 133

(1) In case of suspicion of a criminal act of money laundering and/or financing of terrorism, the Administration may deliver to the entity a written order for temporary detention and/or prohibition of carrying out transactions or temporary freezing of assets.

(2) The detention and/or prohibition on carrying out transactions or temporary freezing of assets shall last until a court decision is rendered on the proposal, and no longer than 72 hours from the delivery of the written order for temporary detention and/or prohibition on carrying out transactions.

(3) When the period referred to in paragraph (2) of this Article includes Sundays, holidays or other non-working days, the temporary detention and/or prohibition on carrying out transactions or temporary freezing of assets shall last for a maximum of 120 hours from the issuance of the order.

(4) When, due to the nature or manner of execution of suspicious transactions, or the circumstances following the suspicious transaction, it is not possible to issue a written order to the entity, as well as in other urgent cases, the Administration may issue an oral order to the entity for temporary detention and/or prohibition of carrying out transactions or temporary freezing of assets.

(5) The Administration must confirm the oral order referred to in paragraph (4) of this Article with a written order no later than the first working day following the issuance of the oral order.

(6) The authorized person is obliged to compile a record of the received oral order referred to in paragraph (5) of this Article, which he shall keep in his records in accordance with Article 62 of this Law.

Article 134

(1) The Administration, upon delivery of the order referred to in Article 133 of this Law, shall submit to the competent public prosecutor a request for submitting a proposal for determining interim measures.

(2) The request for submitting a proposal for determining interim measures under this Law shall contain data on the facts and circumstances that justify the need to apply the interim measure, data on the natural person (unique personal identification number or other identification number of the person, name and surname, date and place of birth, gender and citizenship) or legal entity for which the application of the interim measure is requested, the number of the transaction account(s) and the amount of money or type of property and data on the property.

(3) With the request referred to in paragraph (2) of this Article, the Administration may also submit a report in accordance with Article 131 of this Law.

Article 135

(1) The competent public prosecutor shall review the request for submitting a proposal for determining interim measures under this Law and, if he/she determines that it is well-founded, shall, without delay, submit a proposal for determining interim measures to the judge of the competent basic court in accordance with this Law and the Law on Criminal Procedure.

(2) If the competent public prosecutor determines that the request for submission of a proposal for determination of interim measures under this Law is unfounded, he/she shall be obliged to notify the Administration without delay that the request has been rejected. Upon receipt of the notification from the public prosecutor, the Administration shall without delay submit a written notification to the entity rejecting the request.

Article 136

(1) The judge of the competent basic court shall be obliged, without delay, to issue a decision on the application of a temporary measure or on the rejection of the proposal of the public prosecutor in accordance with this Law and the Law on Criminal Procedure.

(2) If the decision imposes interim measures, the judge is obliged to deliver the decision to the public prosecutor, the entity and the client.

(3) If a decision is made to reject the public prosecutor's proposal, the judge is obliged to submit the decision to the public prosecutor.

(4) The competent public prosecutor is obliged to immediately notify the Administration of the decision made by the judge referred to in paragraph (1) of this Article.

(5) Against the decision of the judge referred to in paragraph (1) of this Article, the competent public prosecutor and the client have the right to appeal to the criminal council of the competent basic court within three days from the date of receipt of the decision, which shall not postpone the execution of the decision.

Statistical data

Article 137

(1) For the purposes of preparing a national risk assessment, assessing the efficiency of the system for combating money laundering and terrorist financing, as well as conducting strategic analyses, the Administration shall collect and maintain the following statistical data on:

- number, size, type, importance and economic significance of certain groups of entities, including the number of entities and the number of employees in them,
- number of reports received on suspicious transactions in accordance with Article 65 of this Law,
- number or percentage of reports received on suspicious transactions in accordance with Article 65 of this Law that resulted in further investigations, including an annual report on the significance and usability of the data from the reports of the entities,
- number of reports received in accordance with Articles 63 and 64 of this Law,
- number of initiatives and requests received from competent authorities in accordance with Article 130 of this Law,
- number of information and data received from supervisory authorities in accordance with Article 155 of this Law,
- number of reports and notifications submitted to competent authorities,
- number of reports and notifications submitted by the Administration upon which the competent authorities acted,

- number of spontaneous information received and submitted from/to financial intelligence units of other countries,
- number of submitted, received, rejected and responded to requests from financial intelligence units of other countries and other data,
- number of supervisions performed, settlement procedures conducted, misdemeanor payment orders issued and misdemeanor procedures initiated,
- number of submitted orders for monitoring a business relationship,
- number of cases and value of property covered by temporary measures in accordance with this Law and
- allocated human resources, i.e. number of employees in the Administration, separately for the execution of each of its legal competencies.

(2) The Administration shall publish on its website information on current techniques, methods and trends in money laundering and terrorist financing, examples of detected cases of money laundering and terrorist financing, an annual review of supervision carried out and other acts arising from this Law or from membership in international bodies and organizations.

(3) For the purposes of assessing the efficiency of the system for combating money laundering and terrorist financing, the courts, the Public Prosecutor's Office of the Republic of North Macedonia, the Judicial Council of the Republic of North Macedonia, the Ministry of Interior, the Financial Police Directorate, the Customs Administration, the Agency for the Management of Seized Property and other competent authorities shall collect and maintain statistical data on:

- number of orders issued for the conduct of investigative procedures and number of persons for whom investigations have been conducted for money laundering and/or terrorist financing,
- number of criminal charges and number of persons for whom a criminal charge has been filed for money laundering and/or terrorist financing,
- number of indictments and number of persons for whom an indictment has been filed for money laundering and/or terrorist financing,
- number of cases and number of persons covered by requests for international legal assistance for money laundering and/or terrorist financing,
- number of cases in which the criminal offense of money laundering and/or terrorist financing has been reclassified during the criminal procedure, and conversely,
- number of convictions and number of persons convicted of money laundering and/or terrorist financing,
- number and type of related criminal offenses and
- number of cases and value of property frozen, seized and confiscated in cases of money laundering and/or terrorist financing in the Republic of North Macedonia and other countries and other data.

(4) The supervisory authorities under this Law are obliged to collect and store data on:

- 1) the number of employees assigned to work positions for supervision of the implementation of the provisions of this Law by the entities;
- 2) the number of supervisions carried out, the number of violations found and the number and type of sanctions imposed.

(5) The competent authorities referred to in paragraphs (3) and (4) of this Article shall submit the data referred to in paragraphs (3) and (4) of this Article to the Administration, at least once a year, no later than 31 January of the current year for the previous year or at the request of the Administration.

(6) The Administration shall publish on its website once a year a consolidated report on the statistical data maintained in accordance with this Article.

Electronic case tracking system
Article 138

- (1) The Financial Intelligence Unit shall, for the purposes of this law, operate and maintain an electronic system for monitoring cases arising from the competences of the Unit.
- (2) The competent authorities acting in accordance with Article 131 of this Law shall mandatorily enter data and information into the electronic system referred to in paragraph (1) of this Article.
- (3) The form, content, manner and deadlines for entering and updating data in the system and the manner of monitoring the cases referred to in paragraph (1) of this Article shall be prescribed by the Minister of Finance upon the proposal of the Director of the Administration.¹⁷
- (4) The data, information and documentation provided in accordance with this Article shall be kept for ten years from the date of the last entered data, information and documentation and shall be deleted after the expiry of this period.

Interinstitutional cooperation **Article 139**

For the purposes of more detailed regulation of inter-institutional cooperation, the Administration may sign Memorandums or Protocols for cooperation with the competent state bodies for the purpose of fulfilling the objectives provided for in this Law.

Council for Combating Money Laundering and Terrorist Financing **Article 140**

- (1) In order to promote inter-institutional cooperation in accordance with the objectives of this Law, to coordinate the activities for the implementation of a national risk assessment and to improve the system for combating money laundering and terrorist financing, the Government of the Republic of North Macedonia, upon the proposal of the Minister of Finance, shall establish a Council for Combating Money Laundering and Terrorist Financing (hereinafter: the Council).
- (2) The work of the Council referred to in paragraph (1) of this Article shall be led by the Director of the Administration, and its members shall be managerial and responsible persons from the Ministry of Interior, the Ministry of Justice, the Ministry of Finance, the Basic Public Prosecutor's Office for Prosecution of Organized Crime and Corruption, the Financial Police Administration, the Customs Administration, the Public Revenue Administration, the National Bank of the Republic of North Macedonia, the Securities and Exchange Commission, the Insurance Supervision Agency, the Fully Funded Pension Insurance Supervision Agency, the Postal Agency, as well as representatives of the Bar Association, the Notary Chamber, the Institute of Certified Auditors and the Institute of Accountants and Certified Public Accountants.
- (3) The members of the Council have deputies who are appointed from among the employees of the bodies and institutions referred to in paragraph (2) of this Article who have appropriate knowledge in the field of detecting and preventing money laundering and terrorist financing.
- (4) For the purposes of its work, the Council shall establish permanent or temporary working bodies composed of employees or representatives of the bodies and institutions referred to in paragraph (2) of this Article, whose management and responsible persons are members of the Council by function.¹⁸
- (5) The members of the Council, depending on the human resources available to the bodies and institutions referred to in paragraph (2) of this Article, shall nominate a person or persons, employees or active members of the bodies and institutions referred to in paragraph (2) of this Article, to participate in the working bodies and who have appropriate professional knowledge for the work of the working body.

(6) As an exception to paragraph (4) of this Article, and upon the proposal of the President or members of the Council, representatives of professional organizations and associations of entities, as well as external experts, may also participate in the work of the working bodies.

(7) The Council referred to in paragraph (1) of this Article shall adopt Rules of Procedure for its operation.

(8) The professional and administrative work for the Council shall be carried out by the Administration.

Customs Administration

Article 141

(1) The Customs Administration shall mandatorily record every entry and exit of money and physically transferable means of payment through the customs line of the Republic of North Macedonia, if the amount exceeds the maximum permitted by law or other regulation.

(2) When recording under paragraph (1) of this Article, the Customs Administration shall mandatorily collect data on:

- the identity of the person who, for himself or for another, imports or exports money and physically portable means of payment, data on the name and surname, date and place of birth, travel document number and citizenship,
- the identity of the owner of the money and physically portable means of payment,
- the identity of the real owner,
- the amount and currency of the money and physically portable means of payment imported or exported through the customs line,
- a statement on the origin of the money and physically portable means of payment, signed by the person importing or exporting them,
- the intention to import or export the money and physically portable means of payment and
- the place and time of crossing the customs line.

(3) The Customs Administration shall report to the Administration, by protected electronic means, and in cases where this is not possible, in writing, the entry or exit of money and physically transferable means of payment exceeding 10,000 euros in denar equivalent, no later than three working days from the date of recording.

(4) The Customs Administration shall mandatorily report in writing to the Administration the import or export of money and physically transferable means of payment, regardless of the amount, whenever there is a basis for suspicion of money laundering or terrorist financing, no later than 24 hours from the date of becoming aware of the suspicious nature of the import or export of money and physically transferable means of payment.

(5) The Customs Administration shall be obliged to keep all data on the entry or exit of money and physically transferable means of payment through the customs line for ten years from the date of the transfer.

International cooperation

Article 142

(1) The Administration shall establish international cooperation with financial intelligence units of other countries through the exchange of relevant data, information and documentation, spontaneously or upon request, for the purposes of preventing and detecting money laundering and terrorist financing in accordance with the provisions of this Law.

(2) The international exchange of relevant data, information and documentation referred to in paragraph (1) of this Article shall be carried out on the basis of:

- a request for exchange of data, information and documentation submitted by the Administration to the financial intelligence unit of another country,
- a request for exchange of data, information and documentation received by the Administration from the financial intelligence unit of another country,
- submission of data, information and documentation by the Administration to the financial intelligence unit of another country or
- submission of data, information and documentation by a financial intelligence unit of another country to the Administration.

(3) The Directorate shall establish international cooperation with financial intelligence units of other countries regardless of their organizational form, the type of related criminal offenses, even when the related criminal offenses are not prescribed as such at the time of the exchange of data, information and documentation.¹⁹

(4) The Administration may conclude cooperation agreements with financial intelligence units of other countries, as well as with international organizations involved in the fight against money laundering and terrorist financing for the purposes of preventing and detecting money laundering and terrorist financing. The signing of cooperation agreements is not a prerequisite for the Administration to carry out international cooperation with financial intelligence units of other countries.

**Request for data exchange submitted by the Administration to the financial intelligence unit
of another country
Article 143**

(1) The Administration, in order to implement its competencies in accordance with the provisions of this Law, may submit a request for exchange of data, information and documentation to a financial intelligence unit of another country.

(2) The request for exchange of data, information and documentation referred to in paragraph (1) of this Article should be explained with the relevant known facts indicating money laundering and/or terrorist financing, the reasons and the purpose for which the requested data and information will be used.

(3) The Administration shall be obliged to use the data, information and documentation provided in accordance with paragraph (1) of this Article for the implementation of its competencies in accordance with the provisions of this Law, in accordance with the limitations and conditions determined by the financial intelligence unit of the state that provided them.

(4) The Administration may exchange the data, information and documentation provided in accordance with paragraph (1) of this Article with competent authorities, after obtaining prior consent from the financial intelligence unit of the state that provided them and in accordance with their limitations and conditions.

(5) The data, information and documentation provided in accordance with paragraph (1) of this Article shall be classified and marked with at least the same level of classification as determined by the financial intelligence unit of the state that provided them.

**Request for exchange of data, information and documentation received by the
Administration from the financial intelligence unit of another country
Article 144**

(1) Upon a request for exchange of data, information and documentation from a financial intelligence unit of another country submitted in writing, the Administration may submit data,

information and documentation that it has in its databases and/or that it provides in accordance with the competencies determined by this Law.

(2) The request for exchange of data, information and documentation referred to in paragraph (1) of this Article should be substantiated by the relevant known facts indicating money laundering and/or terrorist financing and the purpose for which the requested data and information will be used.

(3) The Administration may refuse the request for exchange of data referred to in paragraph (1) of this Article if it is contrary to this Law or would impede the conduct of an investigation by another competent state body or criminal proceedings against the person for whom the data are requested or which are otherwise contrary to the fundamental principles of national legislation. The Administration shall be obliged to explain the reasons for refusing the request.

(4) Upon the request referred to in paragraph (1) of this Article, the Administration shall act promptly and without delay.

(5) The data, information and documentation provided in accordance with paragraph (1) of this Article shall be classified and marked with at least the same level of classification as determined by the financial intelligence unit of the state that provided them.

(6) At the request of a financial intelligence unit of another country referred to in paragraph (1) of this Article, the Administration shall submit consent for forwarding the data, information and documentation provided in accordance with paragraph (1) of this Article to the competent authorities of the country, regardless of the type of related criminal offenses.

(7) The Administration may refuse to grant consent for forwarding the data, information and documentation with a written explanation to the financial intelligence unit referred to in paragraph (1) of this Article, if the request for consent is contrary to this Law or impedes the conduct of the investigation in the criminal procedure or is otherwise contrary to the fundamental principles of national legislation.

Submission of data, information and documentation of the Administration to the financial intelligence unit of another country

Article 145

(1) The Administration may, when there is suspicion of money laundering or terrorist financing and without a request from a financial intelligence unit of another country, submit the data, information and documentation it provides in accordance with the competencies determined by this Law to the same.

(2) The provisions of this Law shall apply to the data, information and documentation submitted by the Administration in accordance with paragraph (1) of this Article.

Interim measures and an order to monitor a business relationship within the framework of international cooperation

Article 146

(1) The provisions of Articles 132, 133, 134, 135 and 136 of this Law shall apply when a financial intelligence unit of another country requests the monitoring of a business relationship, temporary detention and/or prohibition of transactions or temporary freezing of assets.

(2) The request referred to in paragraph (1) of this Article shall be justified and shall refer to a transaction related to money laundering and/or terrorist financing and whether the transaction could, in accordance with the law, be the subject of a domestic suspicious transaction report.

(3) The Administration may refuse the request referred to in paragraph (1) of this Article if it is contrary to this Law or would impede the conduct of an investigation by another competent state body or criminal proceedings against the person for whom the data are requested or which are

otherwise contrary to the fundamental principles of national legislation. The Administration shall be obliged to explain the reasons for refusing the request.

(4) The Administration may submit a request to a financial intelligence unit of another country for monitoring a business relationship, for temporary retention and/or prohibition of transactions or temporary freezing of assets, in case of suspicion of money laundering and/or terrorist financing.

Feedback Article 147

(1) The Administration, upon request of a financial intelligence unit of another country, shall provide feedback on the use of the submitted data, information and documentation.

(2) The Administration may request feedback from the financial intelligence unit of another country on the use of the submitted data, information and documentation.

Safe ways to achieve international cooperation Article 148

The exchange of data, information and documentation between the Administration and the financial intelligence units of other countries, in accordance with this law, will take place through secure electronic international communication systems, through designated person(s) employed by the Administration - financial intelligence officer(s).

Article 149

(1) The Administration may indirectly exchange data, information and documentation with authorities responsible for detecting and preventing money laundering and terrorist financing of other countries, but such exchange must be conducted through the financial intelligence unit of the state through secure electronic international communication systems.

(2) When exchanging data, information and documentation in accordance with paragraph (1) of this Article, the provisions of this Law regulating international cooperation shall apply.

Storage of data, information and documentation by the Administration Article 150

The Administration is obliged to keep the data, information and documentation provided in accordance with this law for ten years from their receipt and after the expiration of this period is obliged to destroy them.

CHAPTER VI. SUPERVISION Article 151

(1) The supervision over the implementation of the measures and actions determined by this Law shall be carried out by the supervisory authorities within the meaning of this Law, namely:

- 1) The National Bank of the Republic of North Macedonia over banks, savings houses, exchange offices and providers of money remittance services (fast money transfer) and other financial institutions that provide payment services in accordance with the law;
- 2) The Insurance Supervision Agency over legal and natural persons that carry out insurance, representation and/or mediation in life insurance with a savings and/or investment component and other related insurance with a savings and/or investment component, such as: insurance

companies; insurance brokerage companies and representation companies and insurance agents;
3) The Securities Commission of the Republic of North Macedonia over brokerage houses, banks licensed to operate with securities, persons providing services to investment advisors, investment advisory companies, companies managing open-end, closed-end and private investment funds and open-end, closed-end and private investment funds;

4) The Agency for Supervision of Fully Funded Pension Insurance over companies managing voluntary pension funds;

5) The Public Revenue Office over organizers of games of chance, legal entities and individuals providing the following services: real estate brokerage, tax advice and legal entities providing the following services: receiving movable property and real estate as collateral;

6) The Postal Agency over AD Post of North Macedonia;

7) Commission of Notaries within the Notary Chamber of the Republic of North Macedonia on notaries and

8) Commission of Lawyers within the Bar Chamber of the Republic of North Macedonia on lawyers and law firms.

(2) The Administration shall supervise the application of the measures and actions determined by this Law on the entities not covered by paragraph (1) of this Article, as well as on the legal entities whose activity is the purchase and sale of new vehicles and the perpetrators.

(3) The Administration shall, independently or in cooperation with the bodies referred to in paragraph (1), items 1), 2), 3) and 4) of this Article, carry out extraordinary, control supervision over the application of the measures and actions determined by this Law on the entities.

(4) The Administration shall, independently or in cooperation with the bodies referred to in paragraph (1), items 5), 6), 7) and 8) of this Article, supervise the application of the measures and actions determined by this Law on the entities.

(5) The Administration, upon receipt of a notification from the registry administrator, shall conduct supervision in accordance with this Law over the legal entities referred to in Article 35, paragraph (2) of this Law.

(6) The Administration shall supervise the legal entities referred to in Article 28, paragraph (1) of this Law and determine whether they possess, keep and have entered in the register appropriate, accurate and complete data on the beneficial owner.

(7) The Administration and the bodies referred to in paragraph (1) of this Article shall undertake activities aimed at harmonizing the methodological approach in conducting supervision.

(8) The Public Revenue Office, in accordance with its competences, shall supervise legal entities and individuals with regard to the implementation of the prohibition on cash payments under Article 58 of this Law.

(9) The supervisory authorities of this Article, when they identify violations that are subject to criminal sanctions, are obliged to promptly notify the Public Prosecutor's Office.

Supervision according to risk assessment

Article 152

(1) When conducting supervision over entities, the supervisory authorities referred to in Article 151 of this Law shall apply the approach based on the assessment of the risk of money laundering and terrorist financing.

(2) When preparing and implementing the annual program or annual supervision plan, the supervisory authorities referred to in Article 151 of this Law shall at least take into account:

- data on identified risks of money laundering or terrorist financing in accordance with the findings of the national risk assessment report referred to in this Law,
- data on specific national or international risks related to clients, products, services and

distribution channels,

- data on the risk of individual categories of entities, individual entities and other available data on entities and

- significant events or changes related to the management of the entity and any change in its business activities.

Special competencies

Article 153

(1) The supervisory authority under this Law or another competent authority, if, on the basis of another law, it issues licenses to entities in accordance with Article 5 of this Law, i.e. authorizations to entities in order to confirm compliance with the prescribed conditions for issuing an operating permit, i.e. approvals or functions of a member of the management body in accordance with the regulations, is obliged to obtain ex officio data on convictions, i.e. non-convictions of persons in relation to whom the fulfillment of the conditions for persons of repute or their associates is being checked, unless otherwise regulated by another law.

(2) A collaborator within the meaning of paragraph (1) of this Article, unless otherwise regulated by another law, is a natural person who, together with a natural person who is a founder, partner or beneficial owner of the entity, a shareholder with a qualifying holding in the entity in accordance with other laws regulating qualifying holding or together with a natural person who is proposed as a member of the senior management of the entity, directly or indirectly and/or through an agreement, exercises control over a domestic or foreign company.

(3) A person who does not possess a reputation in accordance with paragraph (1) of this Article, unless otherwise regulated by another law, shall be considered a person who has been sentenced by a final court verdict to an unconditional prison sentence of over six months, as long as the legal consequences of the verdict persist and/or has an associate who has been sentenced by a final court verdict to an unconditional prison sentence of over six months, as long as the legal consequences of the verdict persist.

(4) The data referred to in paragraph (1) of this Article shall be used only for the purposes for which they were provided and may not be disclosed or made available to third parties.

International cooperation in the field of supervision

Article 154

(1) The authority competent for supervision under this Law, unless otherwise provided for by another law, may, on its own initiative or based on a reasoned written request from an authority of a foreign country competent for supervision, exchange data, information and documentation regarding:

- 1) regulations in the area in which the supervised entity operates, as well as other relevant regulations for supervision;
- 2) the sector in which the supervised entity operates;
- 3) supervision, i.e. supervision of the entity; and
- 4) transactions or persons for which there are grounds for suspicion that they are related to money laundering or terrorist financing or another related criminal offense on the basis of which proceeds of a criminal offense were acquired that can be used for the purposes of money laundering or terrorist financing.

(2) The manner of submitting data, information and documentation, unless otherwise regulated by another law, may be regulated by the authorities referred to in paragraph (1) of this Article by

concluding a memorandum or agreement for cooperation in the field of supervision and in a manner that ensures the integrity of such data as well as protection from unauthorized access.

(3) The supervisory authorities referred to in paragraph (1) of this Article, unless otherwise provided for by another law, in accordance with the principles of reciprocity and confidentiality, may request mutual assistance in conducting supervision within the framework of their powers over an entity that is part of a group and that carries out its business activity in the country requesting assistance.

(4) The supervisory authorities referred to in paragraph (1) of this Article shall use data, information and documentation only:

1) to exercise their powers in accordance with this Law;

2) in the event of an appeal or other legal remedy filed against the decision of the authority competent for supervision, including court proceedings.

(5) The supervisory authority referred to in paragraph (1) of this Article may not disclose and exchange data, information and documentation with third parties obtained within the framework of cooperation in the field of supervision in accordance with the provisions of this Article without the express consent of the supervisory authority that provided such information, data or documentation, nor may they be used for any purpose other than that for which the authority issued its consent.

(6) The obligation to maintain secrecy, i.e. confidentiality of data in accordance with the provisions of this Law as well as other laws regulating the powers and functions of the supervisory authority referred to in paragraph (1) of this Article, shall apply to all persons who work or have worked in the supervisory authority.

Cooperation in the field of supervision

Article 155

(1) The Directorate and the supervisory authorities referred to in Article 151, paragraph (1) of this Law shall be obliged to mutually coordinate their activities in conducting supervision over the entities referred to in this Law.

(2) The Administration and the bodies referred to in paragraph (1) of this Article shall be obliged to prepare an annual program or plan for supervising the implementation of the measures and actions specified in this Law and to harmonize them with each other.

(3) The Administration and the bodies referred to in paragraph (1) of this Article may prescribe a manner of appropriate implementation of the measures for the prevention of money laundering and terrorist financing for the entities for whose supervision they are responsible.

(4) The Administration and the bodies referred to in paragraph (1) of this Article shall cooperate in the performance of their tasks and powers in exercising supervision in order to ensure the efficiency of measures and supervision in the fight against money laundering and the financing of terrorism.

(5) The Administration may submit a proposal to the bodies referred to in paragraph (1) of this Article to supervise a certain entity based on the findings arising from the data and information at its disposal, as well as on the basis of the strategic and operational analyses carried out.

(6) The Administration and the bodies referred to in paragraph (1) of this Article shall undertake activities aimed at harmonizing the methodological approach in conducting supervision.

(7) The Administration and the supervisory authorities referred to in paragraph (1) of this Article may, for the purposes of supervising the entities prescribed in Article 151 paragraph (1) of this Law, request and exchange financial, administrative information and information obtained on the basis of supervision and other data on the entity subject to supervision and for the purposes of

preparing for supervision, including data on typologies and trends for the prevention of money laundering and terrorist financing.

Submission of information and data to the Administration by supervisory authorities **Article 156**

(1) The authorities referred to in Article 151 paragraph (1) of this Law shall submit a report to the Administration in cases where:

1) if, during supervision, they establish suspicion of money laundering and/or terrorist financing;
2) when performing tasks, activities or transactions carried out in accordance with the competencies specified in other laws, they establish suspicion of money laundering and/or terrorist financing.

(2) In the cases referred to in paragraph (1) item 2) of this Article, the authorities referred to in Article 151 paragraph (1) may refuse or postpone the transaction and notify the Administration thereof.

(3) The report referred to in paragraph (1) of this Article shall be submitted by the authorities referred to in Article 151 paragraph (1) of this Law via protected electronic means. If such a method of submission is impossible for technical reasons, the authorities referred to in Article 151 paragraph (1) shall submit the report in writing.

(4) The report referred to in paragraph (1) of this Article shall contain:

1) information and data on the natural or legal person suspected of being involved in the crime in accordance with paragraph (1) of this Article, namely:

- for a natural person, name, surname, date of birth, number of the valid identification document, place of residence, or place of stay, EMBG and

- for a legal person: name, registered office, EMBS, EDB and other data;

2) the reasons for suspicion of money laundering and/or financing of terrorism, accompanied by information, data supported by appropriate documentation.

(5) In order to exercise the powers arising from this Law, the Administration may request additional data and information of importance for the prevention of money laundering and terrorist financing from the supervisory authorities referred to in Article 151, paragraph (1) of this Law in relation to the cases referred to in paragraphs (1) and (2) of this Article.

(6) The submission of the data referred to in this Article to the Administration shall not be considered as the disclosure of confidential data or the disclosure of classified data and information.

(7) When the Administration acts upon the report referred to in paragraph (1) of this Article and determines that there are grounds for suspicion of the commission of a criminal offense of money laundering and/or financing of terrorism or another criminal offense, the Administration shall act in accordance with Article 131 of this Law.

(8) The Administration shall notify the supervisory authorities referred to in Article 151, paragraph (1) of this Law of the outcome of the action taken pursuant to the report referred to in paragraph (1) of this Article.

Article 157

(1) The provisions of Article 169 of this Law, which refer to the authorizations of financial intelligence officers performing supervision, shall apply accordingly to the authorizations of persons performing supervision by the supervisory authorities referred to in Article 151, paragraph (1) of this Law, unless otherwise provided for by the law by which they were established and which regulates the manner of their work.

- (2) The persons performing supervision by the bodies referred to in Article 151, paragraph (1) of this Law shall be persons who:
- 1) possess high integrity;
 - 2) possess appropriate knowledge and experience in the field of preventing money laundering and terrorist financing and
 - 3) meet the requirements in accordance with the regulations governing the field of preventing conflicts of interest.

Article 158

Persons employed and persons who have worked in the supervisory bodies under this Law, as well as auditors or experts who act or have acted on behalf of the supervisory body, are obliged to keep the data and information to which they have or had access for the purposes of performing supervision as a professional secret in accordance with the law.

- (2) The information that the persons referred to in paragraph (1) of this Article receive in the course of exercising their powers in accordance with this Law may be published only in aggregate form, in such a way that individual financial institutions cannot be identified.

Competences of the Administration in the supervision procedure

Article 159

- (1) The supervision carried out independently by the Administration may be field supervision, regular, extraordinary and control supervision, as well as permanent monitoring of the entities.
- (2) The field supervision referred to in paragraph (1) of this Article may be regular, extraordinary and control.
- (3) The regular supervision referred to in paragraph (1) of this Article is an announced supervision in accordance with the annual supervision program, while the extraordinary supervision is carried out without prior announcement.
- (4) The field supervision conducted by the Administration may last a maximum of 45 working days, with the possibility of extension, but not longer than 60 working days.

Article 160

- (1) The supervision referred to in Article 159 of this Law shall be carried out by financial intelligence officers, employees of the Administration who meet the general conditions set out in this Law, the law on public sector employees and the conditions set out in the act on systematization of jobs in the Administration.
- (2) The financial intelligence officers referred to in paragraph (1) of this Article shall be persons who:
- 1) possess high integrity;
 - 2) possess appropriate knowledge and experience in the field of preventing money laundering and terrorist financing and
 - 3) meet the requirements in accordance with the regulations governing the field of preventing conflicts of interest.
- (3) Based on the supervision referred to in paragraph (1) of this Article, the Administration may:
- initiate a procedure for implementing corrective measures;²¹
 - to propose a settlement procedure by issuing a misdemeanor payment order and
 - to submit a request for initiating a misdemeanor procedure.

(4) The Director of the Administration shall adopt an annual program for conducting supervision no later than January 31 for the current year.

(5) The Minister of Finance shall prescribe the form and content of the order for supervision by the Administration.

Constant monitoring of entities by the Administration

Article 161

(1) The continuous monitoring of the entities consists of an analysis of the data, information and documentation available to the Administration, as well as analyses of the data, information and documentation obtained on the basis of previously submitted requests to the entities supervised by the Administration in accordance with this Law.

(2) The entities referred to in this Law are obliged to submit to the Administration the requested data, information and documentation referred to in paragraph (1) of this Article within a deadline set by the Administration from the day of submission of the request.

(3) The entities shall be obliged to submit the requested data, information and documentation referred to in paragraph (2) of this Article to the Administration by protected electronic means. If such method of submission is impossible for technical reasons, the entities shall submit the requested data, information and documentation in writing or in any other manner described in the request.

(4) The data, information and documentation referred to in paragraphs (2) and (3) of this Article, as well as the data, information and documents available to the Administration on the basis of the provisions of this Law, shall be used for supervisory purposes in accordance with the risk assessment referred to in Article 152 of this Law.

(5) The Director of the Administration shall determine a methodology for conducting continuous monitoring of the entities.

Field supervision

Article 162

(1) Field supervision shall be conducted on the basis of the annual supervision program in accordance with this Law.

(2) The Director of the Administration shall issue a written order for supervision based on the annual program referred to in paragraph (1) of this Article.

(3) As an exception to paragraph (2) of this Article, the director shall also issue a written order to conduct field supervision over entities that are not foreseen in accordance with the annual supervision program.

(4) Field supervision begins with the delivery of the supervision order to the entity, i.e. a responsible person in the entity or a representative of the entity.

(5) If the entity subject to supervision, i.e. the responsible person in the entity or the representative of the entity, refuses to receive and/or sign the supervision order or fails to act upon the supervision order, the financial intelligence officer shall prepare a written note stating the reasons for the refusal, failure to sign or failure to act upon the supervision order.

Article 163

If objective reasons arise related to an act of force majeure that make it impossible to effectively and efficiently conduct the supervision in the manner and within the deadlines described in this

law, the financial intelligence officer shall issue a conclusion to stop the supervision procedure until the reasons for which the procedure was forcibly stopped are eliminated.

Elimination of established irregularities and violations

Article 164

(1) When performing the supervision carried out by the Administration, the financial intelligence officer, in order to eliminate the established irregularities or misdemeanors, has the right and obligation to the entity:

- 1) to initiate a procedure for implementing corrective measures;
- 2) to propose a settlement procedure by issuing a misdemeanor payment order or
- 3) to submit a request for initiating a misdemeanor procedure or to initiate another appropriate procedure.

(2) When deciding on the measures referred to in paragraph (1) of this Article to be taken, financial intelligence officers shall be guided by:

- 1) the type and seriousness of the illegality and/or irregularity;
- 2) the impact or potential impact of the measure on the entity;
- 3) whether the omission of the required actions, i.e. the irregularity was intentional and/or repeated;
- 4) the circumstances under which the violation was committed, as well as the readiness of the entity to eliminate the established illegalities and irregularities; and²²
- 5) other circumstances under which the misdemeanor, i.e. irregularity, was committed.

Corrective measures

Article 165

(1) Financial intelligence officers performing supervision in accordance with the provisions of this Law shall initiate a procedure for corrective measures in the event of established irregularities in the operations of the entity that do not have the characteristics and elements of the misdemeanors described in this Law, but represent inadequate or incomplete implementation of measures and actions for the prevention of money laundering and/or terrorist financing that may affect the exposure of the entity to the risk of money laundering and terrorist financing.

(2) In the cases referred to in paragraph (1) of this Article, the financial intelligence officers performing supervision may issue a report to the entity with a recommendation/s for the elimination of the identified deficiencies with deadlines for action.

(3) Within ten working days from the expiry of the deadlines referred to in paragraph (2) of this Article, the entity shall be obliged to submit to the Administration a report on the activities undertaken and documented evidence that it has acted in accordance with the measures referred to in paragraph (2) of this Article.

Procedure for imposing corrective measures

Article 166

(1) The procedure for imposing corrective measures begins with a recommendation/s for the elimination of the identified deficiencies and irregularities with deadlines for action that are an integral part of the minutes of the supervision performed from the moment of signing or receipt of the minutes by the entity being supervised.

(2) The Administration shall keep records of the procedures implemented for the imposition of corrective measures.

(3) The form and content of the records of implemented procedures for imposed corrective measures shall be prescribed by the Minister of Finance upon the proposal of the Director of the Administration.

Control supervision Article 167

(1) Control supervision is carried out ex officio in order for the financial intelligence officers performing supervision to determine whether the entity subject to supervision, after the expiry of the deadline set, during a previously performed regular or extraordinary supervision:

- 1) acted upon the imposed corrective measures;
- 2) partially acted upon the imposed corrective measures or
- 3) did not act upon the imposed corrective measures.

(2) If the entity has acted upon the imposed corrective measures in accordance with this Law, the financial intelligence officers performing supervision shall state this in the minutes of the conducted control supervision.

(3) Failure to act, i.e. partial action upon the imposed corrective measures under this Law shall be recorded in the minutes of the control supervision and shall constitute grounds for initiating a procedure for settlement and issuing a misdemeanor payment order, i.e. submitting a request for initiating a misdemeanor procedure before a competent court.²³

Article 168

(1) When performing the supervision carried out by the Directorate, the financial intelligence officer has the obligation:

- 1) to act upon the order for supervision;
- 2) to undertake preparatory activities for supervision;
- 3) to notify the responsible and authorized person of the entity of the beginning of the supervision, the legal basis, the purpose and the scope of the supervision, except in the case of extraordinary and control supervision;
- 4) to identify himself before the entity, i.e. before the authorized person of the entity;
- 5) to maintain the confidentiality of the data;
- 6) to act legally, timely and in accordance with the Code of Ethics of Financial Intelligence Officers Performing Supervision;
- 7) to draw up a report on the supervision performed;
- 8) to propose a settlement procedure and issue a misdemeanor payment order;
- 9) to initiate a procedure for imposing corrective measures;
- 10) to submit a request for initiating a misdemeanor procedure;
- 11) to collect, process and store personal data in accordance with the provisions of this Law and the regulations on personal data protection and
- 12) to adopt a conclusion to stop the surveillance in accordance with Article 163 of this Law.

(2) In addition to the obligations under paragraph (1) of this Article, the financial intelligence officer shall be obliged to arrange the prepared documentation for the conducted supervision in a file in the following order:

- 1) documents collected in the preparation of the supervision;
- 2) a request from the departments of the Administration, another body or institution if the supervision was conducted at their request;
- 3) a supervision order;
- 4) a report on the conducted supervision;

- 5) a report from the conducted control supervision;
- 6) a conclusion in accordance with Article 163 of this Law;
- 7) a report from the conducted settlement;
- 8) a misdemeanor payment order;
- 9) a request for initiating a misdemeanor procedure and
- 10) legally binding and enforceable decisions from a court procedure.

Article 169

(1) When performing the supervision carried out by the Directorate, the financial intelligence officer is authorized to:

- 1) check and collect general and individual acts, files, documents, evidence and information in a volume according to the subject of the supervision, as well as to request the preparation of necessary copies and documents;
- 2) to request from the entity to be provided with office conditions for work in the business premises of the entity and a person who will be present during the supervision, in order to timely provide documentation and information regarding the subject of supervision;
- 3) to enter and conduct an inspection in the business premises of the entity and its business units;
- 4) to request assistance from a competent state administration body for the removal of a person who obstructs the performance of the supervision under conditions and in a procedure established by law;
- 5) to check identification documents of persons in order to confirm their identity in accordance with the law;
- 6) to request from the entity or its employees a written or oral explanation regarding issues within the scope of the supervision;
- 7) to seek expert opinions from experts when necessary for the supervision;
- 8) to conduct an inventory of documents found in the business premises;
- 9) to have access to the database management system used by the entity for the purpose of conducting an inspection using information technology and
- 10) to provide other necessary documents, data and information related to the supervision.

(2) The entity shall certify the copy with the original of the files, documents, evidence and information referred to in paragraph (1) of this Article with the signature of the authorized person.

(3) The Financial Intelligence Unit is authorized to initiate a procedure for implementing corrective measures, a procedure for issuing a misdemeanor payment order and a misdemeanor procedure in accordance with the law.

Article 170

(1) When performing the supervision carried out by the Directorate, the financial intelligence officer, in order to eliminate the established violations, has the right and obligation to the entity:

- 1) to initiate a procedure for imposing corrective measures;
- 2) to issue a misdemeanor payment order or
- 3) to submit a request for initiating a misdemeanor procedure.

Article 171

- (1) The chambers of advocates and chambers of notaries shall, within their competences, establish committees to supervise the application of the provisions of this Law to the work of their members.
- (2) The members of the committees referred to in paragraph (1) of this Article shall be appointed for a term of four years, unless otherwise provided for by another law.
- (3) The Administration shall be notified of the appointment and composition of the committees referred to in paragraph (1) of this Article within seven days.

Article 172

- (1) The supervisory authorities referred to in Article 151 paragraph (1) of this Law shall be obliged to notify the Administration of:
 - the findings from the supervision carried out over the implementation of the measures and actions determined by this Law,
 - corrective or other measures imposed,
 - misdemeanor payment orders issued and collected,
 - requests submitted for initiating misdemeanor proceedings for a misdemeanor committed by the entities they supervise and the outcome of these proceedings,
 - the perpetrator of the misdemeanor, namely: name and registered office of the legal entity, name and surname of the responsible person in the legal entity, name and surname of the natural person, person exercising public authorization and authorized official,
 - the misdemeanor: description of the action constituting a misdemeanor and
 - the misdemeanor sanction imposed.
- (2) The supervisory authorities referred to in Article 151, paragraph (1) of this Law shall be obliged to notify the Administration at least once a year of the data related to the supervision carried out pursuant to paragraph (1) of this Article.
- (3) The Administration shall report once a year to the appropriate supervisory authority under this Law on the supervision carried out over the entities and on the findings from the supervision carried out.

Procedure for reporting a committed offense

Article 173

- (1) The entity is obliged to establish a procedure for reporting a committed offense through an independent and anonymous reporting channel, which will enable employees to report a violation of the provisions of this Law.
- (2) The procedure for reporting a committed offense referred to in paragraph (1) of this Article should contain clear rules for receiving and processing reports of a committed offense, proportionate to the nature and size of the entity.
- (3) The entity may not disclose the identity of the person who submitted a report for a committed misdemeanor without obtaining his/her prior consent, except in cases where this is necessary for the purposes of conducting a pre-investigation or criminal procedure.

Article 174

- (1) The supervisory authorities referred to in Article 151 paragraph (1) of this Law shall establish efficient procedures for reporting a committed offence that will enable employees of the entities to report a violation of the provisions of this Law, which will ensure:
 - a simple and easily accessible method of submitting reports of a committed offence,
 - internal rules for receiving and processing reports of a committed offence, and

- protection of the personal data of the person who submitted a report of a committed offence in accordance with the regulations on the protection of personal data.

(2) The supervisory authorities referred to in Article 151, paragraph (1) of this Law may not disclose the identity of the person who submitted a report on a committed offence without obtaining his prior consent.

(3) It is prohibited for persons referred to in paragraph (1) of this Article who have reported a violation of the provisions of this Law to be exposed to threats, retaliatory or hostile actions, negative or discriminatory actions for the employment relationship.

(4) Persons referred to in paragraph (1) of this Article who have reported a violation of the provisions of this Law, and who are exposed to threats, retaliatory or hostile actions or negative or discriminatory actions for the employment relationship due to reporting suspicions of money laundering or terrorist financing, shall have the right to an effective legal remedy for the protection of their rights in accordance with the law.

Disclosure of information regarding supervision Article 175

(1) For the purposes of preventing and deterring the performance of activities that are considered misdemeanors in accordance with this Law, the supervisory authorities referred to in Article 151 paragraph (1) of this Law shall publicly publish information on imposed misdemeanor sanctions based on a final court decision, unless the publication of the information may hinder the conduct of pre-investigation or criminal proceedings.

(2) The information referred to in paragraph (1) of this Article shall contain data on:

- the perpetrator of the misdemeanor, namely: name and registered office of the legal entity, name and surname of the responsible person in the legal entity, name and surname of the natural person, person exercising public authorization and authorized official,
- the misdemeanor: description of the action constituting a misdemeanor and
- the misdemeanor sanction imposed.

(3) The information referred to in paragraph (2) of this Article shall be published on the website of the supervisory authorities referred to in Article 151 paragraph (1) of this Law and shall be available within five years from the date of publication.

(4) Where a supervisory authority referred to in Article 151 paragraph (1) of this Law, in an individual assessment of a specific case, considers that the publication of data on the perpetrator of the misdemeanor is disproportionate to the aim to be achieved or where the publication endangers the stability of financial markets or the ongoing investigation, it may:

- a) postpone the publication of the decision referred to in paragraph (1) of this Article until the moment when the reasons for non-publication cease to exist;
- b) publish the decision referred to in paragraph (1) of this Article in a manner that does not share personal data or
- c) not publish the decision referred to in paragraph (1) of this Article at all.

(5) The supervisory authorities referred to in Article 151 paragraph (1) of this Law shall publish the decisions against which an appeal has been lodged on their website, immediately publishing the information regarding the appeal lodged and all subsequent information related to the decision, including the annulment or revocation of the previously adopted decision.

CHAPTER VII.
COLLECTION, PROCESSING, ANALYSIS, ASSESSMENT, EVALUATION, USE, TRANSFER, STORAGE
AND DELETION OF DATA AND PROCESSING OF PERSONAL DATA

Article 176

- (1) The Administration shall collect, process, analyze, evaluate, assess, use, transfer, store and delete data, process personal data under the conditions and in the manner determined by this and a separate law, and keep records of personal and other data the collection of which it is authorized by this law, for the purpose of preventing money laundering and/or financing of terrorism.
- (2) The Administration processes personal data when there is suspicion of money laundering and/or terrorist financing in accordance with the law.
- (3) Data on a legal entity are collected when there are grounds for suspicion of money laundering and/or terrorist financing.

Article 177

Personal data, within the meaning of this law, are personal name, birth data (day, month and year), place of residence or stay, unique identification number, residential address and citizenship, as well as other data through which a specific person can be directly or indirectly identified.

Article 178

The Administration collects personal and other necessary data from entities, competent state bodies, public institutions, establishments, international organizations and other legal and natural persons only for the purposes determined by this Law.

Article 179

- (1) The Directorate shall keep records of:
- 1) persons for whom a suspicious activity report has been submitted;
 - 2) persons for whom a report has been submitted for a cash transaction in the amount of 15,000 euros in denar equivalent or more, regardless of whether it is a single transaction or several apparently related transactions;
 - 3) persons for whom a report has been submitted by a notary for a drawn up notarial deed and a notarized signature on a contract;
 - 4) persons for whom a report has been submitted by an executor for a sale carried out by means of an oral public auction and a direct settlement concluded;
 - 5) persons for whom a report has been submitted for a disbursed loan;
 - 6) persons for whom a report has been submitted for a given and/or received loan;
 - 7) persons for whom a report has been submitted for a transaction carried out through a fast money transfer;
 - 8) persons for whom a report has been submitted for the conclusion of a life insurance policy;
 - 9) persons for whom a report has been submitted for the purchase and sale of vehicles;
 - 10) persons for whom a report has been submitted for the purchase or payment of chips or credits in a gambling house (casino);
 - 11) persons for whom a report has been submitted for the payment of winnings or payment of a deposit or/and in all cases with other organizers of games of chance;
 - 12) persons for whom a report has been submitted for a transaction related to virtual funds;
 - 13) persons for whom a report of suspicion of money laundering and terrorist financing has been submitted to the competent authorities;

- 14) persons for whom a notification of suspicion of another criminal act has been submitted to the competent authorities;
 - 15) persons for whom an order for monitoring a business relationship has been issued;
 - 16) persons for whom an order for the application of interim measures has been issued;
 - 17) persons for whom an initiative and request have been submitted by the competent authorities in the Republic of North Macedonia;
 - 18) persons for whom data has been exchanged with financial intelligence units of other countries;
 - 19) persons who have transferred money or physically transferable means of payment through the customs line of the Republic of North Macedonia;
 - 20) persons for whom misdemeanor payment orders have been issued and
 - 21) persons for whom data has been exchanged between supervisory authorities.
- (2) The records referred to in paragraph (1) of this Article shall contain personal data: (unique personal identification number or other identification number, name and surname, date and place of birth, gender and citizenship) in accordance with this Law for the holder of the personal data and for a third party.

Article 180

The records referred to in Article 179 of this Law may be structured and kept as:

- 1) records of a submitted suspicious activity report;
- 2) records of a submitted cash transaction report in the amount of 15,000 euros in denar equivalent or more, regardless of whether it is a single transaction or several apparently related transactions;
- 3) records of a submitted notary public report on a drawn up notarial deed and notarized signature on a contract;
- 4) records of a submitted executor report on a concluded contract for an immediate settlement;
- 5) records of a submitted credit report;
- 6) records of a submitted loan report;
- 7) records of a submitted transaction report made through a fast money transfer;
- 8) records of a submitted report on the conclusion of a life insurance policy;
- 9) records of a submitted vehicle purchase and sale report;
- 10) records of a submitted report for the purchase or payment of chips or credits in a gambling house (casino);
- 11) records of a submitted report for the payment of winnings and the payment of a deposit or/and in both cases with other organizers of games of chance;
- 12) records of a submitted report for suspicion of money laundering and terrorist financing to the competent authorities;
- 13) records of a submitted report for a transaction related to virtual savings;25
- 14) records of submitted reports of suspicion of another criminal offense to the competent authorities;
- 15) records of issued orders for monitoring a business relationship;
- 16) records of issued orders for the application of interim measures;
- 17) records of submitted initiatives and requests from the competent authorities in the Republic of North Macedonia;
- 18) records of exchanged data with financial intelligence units of other countries;
- 19) records of submitted reports on transferred money or physically portable means of payment through the customs line of the Republic of North Macedonia;
- 20) records of performed supervision over the entities referred to in Article 5 of this Law;
- 21) records of performed supervision over the legal entities referred to in Article 28 of this Law;
- 22) records of issued misdemeanor payment orders;

- 23) records of implemented corrective measures and
- 24) records of exchanged data between supervisory authorities.

Article 181

(1) The data for which the Administration keeps records in accordance with Articles 179 and 180 of this Law shall be used for the performance of the Administration's responsibilities in accordance with this Law, for statistical and analytical purposes, as well as for the purposes of conducting a national risk assessment and assessing the efficiency of the system for preventing money laundering and terrorist financing.

(2) Personal data may be submitted to entities, competent state authorities, public institutions, institutions, financial intelligence units of other countries and other legal and natural persons in accordance with law and ratified international agreements.

Article 182

Personal data may be used in accordance with the purposes prescribed by this law and in accordance with the regulations governing the protection of personal data.

(2) The processing of personal data for the purposes of preventing money laundering and terrorist financing constitutes a public interest.

(3) The right of access to the client's personal data may be partially or fully restricted by the entity, in order to:

- enable the entity or the competent authority to exercise its powers and
- to avoid obstructing the conduct of a procedure for detecting money laundering and terrorist financing.

Article 183

Personal data entered into the records referred to in Articles 179 and 180 of this Law shall be immediately deleted in cases where it is determined that they are incorrect or the reasons, i.e. the conditions for which the personal data was entered into the records have ceased to exist.

Article 184

The data contained in the records referred to in Articles 179 and 180 of this Law, from their entry until their deletion, may be exchanged under the conditions and in the manner provided for by this Law.

Article 185

The data from the records referred to in Articles 179 and 180 of this Law shall be kept for a period of ten years from the date of their receipt.

CHAPTER VIII. MINOR PROVISIONS

Article 186

(1) A fine in the amount of 80,000 to 120,000 euros in denar equivalent shall be imposed for a misdemeanor on a legal entity (large trader), if:

- it fails to conduct a client analysis procedure in accordance with Article 13 of this Law,
- it fails to conduct an enhanced analysis when establishing a correspondent relationship in

accordance with Article 40 of this Law,

- it fails to refuse to establish a business relationship or execute a transaction or terminate the business relationship with the client in accordance with Article 46 paragraphs (1) and (2) of this Law,
- it establishes or continues a business relationship with a shell bank and starts or continues a correspondent business relationship with a bank that it knows allows the opening and operation of shell bank accounts contrary to Article 59 paragraph (1) of this Law,
- if it performs financial activities of a shell bank contrary to Article 59 paragraph (2) of this Law,
- it opens and maintains accounts, savings books and safes in anonymous form, encrypted form or under fictitious names, i.e. performs other services that indirectly or directly enable concealment of the client's identity, i.e. anonymity in accordance with Article 60 paragraph (1) of this Law,
- provides services related to virtual assets that indirectly or directly enable concealment of the client's identity as well as performs transactions with such virtual assets in accordance with Article 60 paragraph (2) of this Law,
- uses resources or means through an information system that enable or facilitate concealment of the client's identity or that make it impossible or difficult to monitor transactions related to virtual assets in accordance with Article 60 paragraph (3) of this Law,
- accepts payments made using an anonymous payment card with a subscription (prepaid card) in accordance with Article 61 of this Law,
- fails to submit data, information and documents to the Administration in accordance with Article 65 paragraph (1) of this Law,
- the bank fails to put into use or upgrade the software for automatic processing of data in accordance with Article 70 of this Law,
- invokes a business secret contrary to Article 74 of this Law,
- fails to submit the requested data, submits incomplete or incorrect data or fails to submit them within the deadline in accordance with Article 128 of this Law,
- fails to act in accordance with the order for monitoring a business relationship in accordance with Article 132 of this Law,
- fails to withhold the transaction based on the issued order in accordance with Article 133 of this Law and
- refuses to receive and/or sign the supervision order or fails to act in accordance with the supervision order in accordance with Article 162 paragraph (5) of this Law.

(2) For the actions referred to in paragraph (1) of this Article, a legal entity (medium-sized trader) shall be fined in the amount of 60,000 to 80,000 euros in denar equivalent.

(3) For the actions referred to in paragraph (1) of this Article, a legal entity (small trader) shall be fined in the amount of 40,000 to 60,000 euros in denar equivalent.

(4) For the actions referred to in paragraph (1) of this Article, a legal entity (micro-merchant) shall be fined in the amount of 20,000 to 40,000 euros in denar equivalent.

(5) For the actions referred to in paragraph (1) of this Article, the legal entities referred to in paragraphs (1), (2), (3) and (4) of this Article may be imposed a misdemeanor sanction of a temporary ban on performing a particular activity in accordance with the law. The Administration may submit a reasoned proposal for temporary or permanent revocation of a license, i.e. a permit to operate, of the legal entity to the authorities competent for their issuance in accordance with the law.

(6) A fine in the amount of 12,000 to 18,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (1) of this Article.

(7) A fine in the amount of 9,000 to 12,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (2) of this Article.

(8) A fine in the amount of 6,000 to 9,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (3) of this Article.

(9) A fine in the amount of 3,000 to 6,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (4) of this Article.

(10) The responsible person in the legal entity referred to in paragraphs (1), (2), (3) and (4) of this Article may, in addition to a fine, be imposed a misdemeanor sanction of prohibition from performing a profession, activity or duty in accordance with the law for the actions referred to in paragraph (1) of this Article.

(11) For the actions referred to in paragraph (1) of this Article committed intentionally, in an organized manner or which are repeated, which cause significant damage or result in significant property gain, the entity referred to in Article 5 of this Law, with the exception of financial institutions, shall be imposed a fine of at most double the amount of the gain achieved or, if this cannot be determined, at least 1,000,000 euros in denar equivalent.

(12) By way of exception to paragraph (11) of this Article, for the actions referred to in paragraph (1) of this Article committed intentionally, in an organized manner or which are repeated, which cause significant damage or result in significant material gain, the entity referred to in Article 5 of this Law - the financial institution shall be imposed a fine in the amount of 10% of the income generated in the previous fiscal year or at least 5,000,000 euros in denar equivalent.

(13) In addition to the fines referred to in paragraphs (11) and (12) of this Article, the entity referred to in Article 5 of this Law may also be imposed a misdemeanor sanction of a temporary ban on performing a specific activity in accordance with the law, and the responsible person may also be imposed a misdemeanor sanction of a ban on performing a profession, activity or duty in accordance with the law.

(14) For the actions referred to in paragraphs (11) and (12) of this Article, the entity referred to in Article 5 of this Law who benefits shall also be imposed a fine if the actions referred to in paragraphs (11) and (12) of this Article were committed by:

- a natural person who acted individually or as a member of a body of the legal entity and is a senior management of the legal entity or
- a natural person employed in the legal entity, due to the absence of control by a natural person who is a senior management of the legal entity.

Article 187

(1) A fine in the amount of 30,000 to 40,000 euros in denar equivalent shall be imposed for a misdemeanor on a legal entity (large trader), if it:

- fails to notify the Administration in accordance with Article 8 of this Law,
- fails to conduct a risk assessment in accordance with Article 11 of this Law,
- fails to prepare and implement a program in accordance with Article 12 paragraph (1) of this Law,
- fails to adopt a program, regularly monitors and assesses its suitability, compliance and efficiency in accordance with Article 12 paragraph (3) of this Law,
- acts contrary to the exceptions for customer due diligence in relation to electronic money in Article 14 of this Law,
- fails to implement the customer due diligence measures in Article 15 of this Law,
- fails to identify and confirm the identity of the customer, the person acting on behalf of and for the

- account of the customer or the beneficial owner in accordance with Article 16 of this Law,
- fails to identify and confirm the identity of the customer in accordance with Article 17 of this Law law,
 - does not identify and confirm the identity of the person acting on behalf of and for the account of the client in accordance with Article 18 of this Law,
 - does not identify and confirm the identity of the beneficial owner in accordance with Article 19 of this Law,
 - does not act in accordance with Article 32 of this Law,
 - does not monitor the business relationship in accordance with Article 37 of this Law,
 - does not conduct enhanced due diligence on the client in accordance with Article 39 of this Law,
 - does not conduct enhanced due diligence on a client who is not physically present in accordance with Article 41 of this Law,
 - does not conduct enhanced due diligence on a client - a public office holder in accordance with Article 42 of this Law,
 - does not conduct enhanced due diligence when the business relationship or transaction involves a high-risk country in accordance with Article 43 of this Law,
 - does not conduct enhanced due diligence in relation to business relationships and transactions with non-profit organizations in accordance with Article 44 of this Law,
 - does not conduct enhanced due diligence on complex and unusual transactions in accordance with Article 45 of this Law,
 - failed to ensure the implementation of measures and actions for the prevention of money laundering and terrorist financing in accordance with Article 48 of this Law,
 - entrusted the obligations for analyzing the client to third parties contrary to Article 49 of this Law,
 - failed to act in accordance with Articles 50, 50-a, 50-b, 50-c, 50-d and 50-e of this Law,
 - failed to act in accordance with Articles 51, 51-a, 51-b, 51-c and 51-d of this Law,
 - failed to establish the identity of a client in accordance with Article 52 paragraph (1) of this Law,
 - failed to act in accordance with Article 52 paragraph (2) of this Law,
 - failed to establish the identity of a client in accordance with Article 53 of this Law,
 - fails to establish the identity of a client in accordance with Article 54 of this Law,
 - fails to establish the identity of a client in accordance with Article 56 of this Law,
 - fails to establish the identity of a client in accordance with Article 57 of this Law,
 - receives cash in accordance with Article 58 of this Law,
 - performs registration of securities, other property or legal matters or for reporting or performing the transfer of money, securities or other property, in accordance with Article 58 paragraph (2) of this Law,
 - fails to keep the data, information or documents in accordance with Article 62 of this Law,
 - fails to submit to the Administration the collected data, information and documents in the case of a cash transaction in the amount of 15,000 euros in denar equivalent or more, regardless of whether it is a single transaction or several obviously related transactions in accordance with Article 63 of this Law,
 - fails to submit data to the Administration in accordance with Article 64 of this Law,
 - fails to notify the Administration and fails to retain the transaction in accordance with Article 65 paragraphs (2) and (3) of this Law,
 - do not submit to the Administration data, information and documents in the form of a report in accordance with Article 65 paragraph (4) of this Law,
 - do not submit the reports to the Administration in accordance with Article 67 of this Law,
 - do not appoint an authorized person and his deputy in accordance with Article 68 paragraph (1) of this Law,
 - do not establish a special department for the prevention of money laundering and terrorist

- financing in accordance with Article 68 paragraph (3) of this Law,
- do not establish a special department for the prevention of money laundering and terrorist financing in accordance with Article 68 paragraph (4) of this Law,
 - do not ensure the fulfillment of the conditions in accordance with Article 68 paragraph (10) of this Law;
 - fails to appoint an authorized person on duty and his/her deputy in accordance with Article 68 paragraph (11) of this Law,
 - fails to perform internal control in accordance with Article 69 of this Law,
 - uses the data provided by this Law contrary to Article 71 of this Law,
 - notifies the client or a third party contrary to Article 72 paragraph (1) of this Law,
 - fails to take necessary measures for data protection in accordance with Article 72 paragraph (3) of this Law and
 - fails to submit to the Administration the requested data, information and documentation in accordance with Article 161 paragraph (2) of this Law.
- (2) For the actions referred to in paragraph (1) of this Article, a legal entity (medium-sized trader) shall be fined in the amount of 20,000 to 30,000 euros in denar equivalent.
- (3) For the actions referred to in paragraph (1) of this Article, a legal entity (small trader) shall be fined in the amount of 10,000 to 20,000 euros in denar equivalent.
- (4) For the actions referred to in paragraph (1) of this Article, a legal entity (micro-merchant) shall be fined in the amount of 5,000 to 10,000 euros in denar equivalent.
- (5) For the actions referred to in paragraph (1) of this Article, the legal entities referred to in paragraphs (1), (2), (3) and (4) of this Article may be imposed a misdemeanor sanction of a temporary ban on performing a specific activity in accordance with the law.
- (6) A fine in the amount of 4,500 to 6,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (1) of this Article.
- (7) A fine in the amount of 3,000 to 4,500 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (2) of this Article.
- (8) A fine in the amount of 1,500 to 3,000 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (3) of this Article.
- (9) A fine in the amount of 750 to 1,500 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (4) of this Article.
- (10) The responsible person in the legal entity referred to in paragraphs (1), (2), (3) and (4) of this Article may, in addition to a fine, be imposed a misdemeanor sanction of prohibition from performing a profession, activity or duty in accordance with the law for the actions referred to in paragraph (1) of this Article.

Article 188

- (1) A fine in the amount of 5,000 to 10,000 euros in denar equivalent shall be imposed for a misdemeanor on a legal entity (large trader), if:
- it fails to notify the Administration in accordance with Article 6 paragraph (6) of this Law,
 - it fails to notify the Administration in accordance with Article 7 paragraph (2) of this Law,
 - it fails to conduct a simplified analysis of the client in accordance with Article 38 of this Law,
 - it fails to record the data in chronological order in a numbered register with a provider of services related to virtual assets in accordance with Article 52 paragraph (3) of this Law,

- it fails to record the data in chronological order in a numbered register with exchange operations in accordance with Article 53 of this Law,
- it fails to record the data in chronological order in a numbered register with brokerage houses and banks licensed to operate with securities in accordance with Article 55 of this Law,
- it fails to record the data in chronological order in a numbered register with persons trading or acting as intermediaries in the trade of works of art in accordance with Article 56 of this Law,
- fails to record data in chronological order in a numbered register of persons who trade or act as intermediaries in the trade of works of art when the activity takes place in free zones in accordance with Article 57 of this Law,
- fails to notify the competent supervisory authority under this Law that they have submitted a report to the Administration in accordance with Article 65 paragraph (7) of this Law,
- employs in the department persons who do not meet the requirements of Article 68 paragraphs (7), (8) and (13) of this Law,
- fails to provide regular professional training in accordance with Article 68 paragraph (14) of this Law,
- fails to submit data to the Administration in accordance with Article 68 paragraph (15) of this Law and
- fails to act or partially act upon the imposed corrective measures in accordance with Article 167 of this Law.

(2) For the actions referred to in paragraph (1) of this Article, a legal entity (medium-sized trader) shall be fined in the amount of 4,000 to 8,000 euros in denar equivalent.

(3) For the actions referred to in paragraph (1) of this Article, a legal entity (small trader) shall be fined in the amount of 3,000 to 4,000 euros in denar equivalent.

(4) For the actions referred to in paragraph (1) of this Article, a legal entity (micro-merchant) shall be fined in the amount of 2,000 to 3,000 euros in denar equivalent.

(5) A fine in the amount of 750 to 1,500 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (1) of this Article.

(6) A fine in the amount of 600 to 1,200 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (2) of this Article.

(7) A fine in the amount of 300 to 450 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (3) of this Article.

(8) A fine in the amount of 150 to 300 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (4) of this Article.

Article 189

(1) A fine in the amount of 30,000 to 40,000 euros in denar equivalent shall be imposed for a misdemeanor on a person exercising public authorization or a natural person, if:

- fails to conduct a client analysis procedure in accordance with Article 13 of this Law,
- fails to refuse to establish a business relationship or execute a transaction or fails to terminate the business relationship with the client in accordance with Article 46 paragraphs (1) and (2) of this Law,
- performs services that indirectly or directly enable concealment of the client's identity, i.e. anonymity in accordance with Article 60 paragraph (1) of this Law,
- accepts payments made using an anonymous prepaid payment card in accordance with Article 61

of this Law,

- fails to submit data, information and documents to the Administration in accordance with Article 65 paragraph (1) of this Law,
- invokes a business secret contrary to Article 74 of this Law,
- fails to submit the requested data, submits incomplete or incorrect data or fails to submit them within the deadline in accordance with Article 128 of this Law,
- fails to act in accordance with the order for monitoring a business relationship in accordance with Article 132 of this Law,
- fails to withhold the transaction based on the issued order in accordance with Article 133 of this Law and
- refuses to receive and/or sign the supervision order or fails to act on the supervision order in accordance with Article 162 paragraph (5) of this Law.

(2) In addition to the fine, the person exercising public authority or the natural person may be imposed a misdemeanor sanction of prohibition from performing a profession, activity or duty in accordance with the law for the actions referred to in paragraph (1) of this Article.

(3) For the actions referred to in paragraph (1) of this Article committed intentionally, in an organized manner or which are repeated, which cause significant damage or result in significant property gain, the person exercising public authority or the natural person shall be fined a maximum of double the amount of the gain or, if the latter cannot be determined, at least 1,000,000 euros in denar equivalent.

Article 190

(1) A fine in the amount of 12,000 to 15,000 euros in denar equivalent shall be imposed for a misdemeanor on a person exercising public authorization or a natural person, if:

- upon request of the Administration, they fail to submit a written explanation in accordance with Article 7 paragraph (2) of this Law,
- fail to conduct a risk assessment in accordance with Article 11 of this Law,
- fail to prepare and implement a program in accordance with Article 12 paragraph (1) of this Law,
- fail to adopt a program, regularly monitor and assess its suitability, compliance and efficiency in accordance with Article 12 paragraph (3) of this Law,
- fail to implement the measures for analysis of the client in accordance with Article 15 of this Law,
- fail to identify and confirm the identity of the client, the person acting in the name and on behalf of the client or the beneficial owner in accordance with Article 16 of this Law,
- fail to identify and confirm the identity of the client in accordance with Article 17 of this Law,
- fail to identify and confirm the identity of the person who acts on behalf of and for the account of the client in accordance with Article 18 of this Law,
- does not identify and confirm the identity of the beneficial owner in accordance with Article 19 of this Law,
- does not act in accordance with Article 32 of this Law,
- does not monitor the business relationship in accordance with Article 37 of this Law,
- does not conduct enhanced due diligence on the client in accordance with Article 39 of this Law,
- does not conduct enhanced due diligence on a client who is not physically present in accordance with Article 41 of this Law,
- does not conduct enhanced due diligence on a client - a public office holder in accordance with Article 42 of this Law,
- does not conduct enhanced due diligence when the business relationship or transaction involves a high-risk country in accordance with Article 43 of this Law,
- does not conduct enhanced due diligence in relation to business relationships and transactions

- with non-profit organizations in accordance with Article 44 of this Law,
- does not conduct enhanced due diligence on complex and unusual transactions in accordance with Article 45 of this Law,
 - does not ensure the application of the measures and the actions for the prevention of money laundering and terrorist financing in accordance with Article 48 of this Law,
 - entrusts the obligations for the analysis of the client to third parties contrary to Article 49 of this Law,
 - receives cash contrary to Article 58 of this Law,
 - does not keep the data, information or documents in accordance with Article 62 of this Law,
 - does not submit data to the Administration in accordance with Article 64 of this Law,
 - does not notify the Administration and does not retain the transaction in accordance with Article 65 paragraphs (2) and (3) of this Law,
 - does not submit to the Administration data, information and documents in the form of a report in accordance with Article 65 paragraph (4) of this Law,
 - fails to submit reports to the Administration in accordance with Article 67 of this Law,
 - fails to appoint an authorized person and his/her deputy in accordance with Article 68 paragraph (1) of this Law,
 - fails to establish a special department for the prevention of money laundering and terrorist financing in accordance with Article 68 paragraph (3) of this Law,
 - fails to establish a special department for the prevention of money laundering and terrorist financing in accordance with Article 68 paragraph (4) of this Law,
 - fails to ensure the fulfillment of conditions in accordance with Article 68 paragraph (10) of this Law,
 - fails to perform internal control in accordance with Article 69 of this Law,
 - uses the data provided by this Law contrary to Article 71 of this Law,
 - notifies the client or a third party in accordance with Article 72 paragraph (1) of this Law,
 - fails to take necessary measures for data protection in accordance with Article 72 paragraph (3) of this Law.
- (2) In addition to the fine, the person exercising public authority or the natural person may be imposed a misdemeanor sanction of prohibition from performing a profession, activity or duty in accordance with the law for the actions referred to in paragraph (1) of this Article.

Article 191

- A fine in the amount of 2,000 to 2,500 euros in denar equivalent shall be imposed for a misdemeanor on a person exercising public authorization or a natural person, if:
- fails to notify the Administration in accordance with Article 6 paragraph (6) of this Law,
 - fails to conduct a simplified analysis of the client in accordance with Article 38 of this Law,
 - employs in the department persons who do not meet the requirements of Article 68 paragraphs (7), (8) and (13) of this Law,
 - fails to provide regular professional training in accordance with Article 68 paragraph (14) of this Law,
 - fails to submit data to the Administration in accordance with Article 68 paragraph (15) of this Law and
 - fails to act or partially act upon the imposed corrective measures in accordance with Article 167 of this Law.

Article 192

(1) A fine in the amount of 10,000 to 15,000 euros in denar equivalent shall be imposed on the legal entity (large trader) for a misdemeanor under Article 28 paragraph (1) of this Law, if:

- it does not possess and keep appropriate, accurate and up-to-date data on the beneficial owner in accordance with Article 28 paragraph (2),
- it does not enter the data on the beneficial owner(s), as well as the data on the changes in beneficial owner(s) in the register in accordance with Article 31 of this Law and
- it refuses to receive and/or sign the supervision order or fails to act upon the supervision order in accordance with Article 162 paragraph (5) of this Law.

(2) For the actions referred to in paragraph (1) of this Article, the legal entity (medium-sized trader) shall be fined in the amount of 8,000 to 12,000 euros in denar equivalent.

(3) For the actions referred to in paragraph (1) of this Article, the legal entity (small trader) shall be fined in the amount of 6,000 to 8,000 euros in denar equivalent.

(4) For the actions referred to in paragraph (1) of this Article, the legal entity (micro-merchant) shall be fined in the amount of 5,000 to 6,000 euros in denar equivalent.

(5) A fine in the amount of 1,500 to 2,250 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (1) of this Article.

(6) A fine in the amount of 1,200 to 1,800 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (2) of this Article.

(7) A fine in the amount of 900 to 1,200 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (3) of this Article.

(8) A fine in the amount of 750 to 900 euros in denar equivalent for the actions referred to in paragraph (1) of this Article shall also be imposed on the responsible person in the legal entity referred to in paragraph (4) of this Article.

Article 192-a

A fine in the amount of 10,000 to 15,000 euros in denar equivalent shall be imposed for a misdemeanor on a manager/trustee of a trust or similar legal arrangement, i.e. a person acting on behalf of and for the account of a trust under Article 22 of this Law, if:

- he fails to notify the entity and provide information supported by documents that he is acting in that capacity, as well as to provide information on the identity of the persons specified in Article 22 of this Law,
- he fails to possess and keep appropriate, accurate and up-to-date data on the beneficial owner in accordance with Article 28 of this Law and
- he fails to enter the data on the beneficial owner(s), as well as the data on changes in beneficial owner(s) in the register in accordance with Article 31 of this Law.

Article 193

A fine in the amount of 500 to 1,000 euros in denar equivalent shall be imposed for a misdemeanor on the bankruptcy trustee or liquidation trustee if he or she fails to take measures and actions in a case where the entity is in bankruptcy and liquidation proceedings in accordance with Article 10 of this Law.

Article 194

A fine in the amount of 500 to 1,000 euros in denar equivalent shall be imposed for a misdemeanor on an authorized official, if:

- they fail to submit the required data in accordance with Article 128 of this Law,
- they fail to inform the Administration about the result and outcome of the submitted reports or notifications in accordance with Article 131 paragraph (5) of this Law,
- they fail to submit statistical data to the Administration in accordance with Article 137 paragraph (5) of this Law,
- they fail to record every entry and exit of money or physically portable means of payment through the customs line of the Republic of North Macedonia in accordance with Article 141 paragraph (1) of this Law,
- they fail to collect data in accordance with Article 141 paragraph (2) of this Law,
- they fail to report to the Administration the entry or exit of money or physically portable means of payment over 10,000 euros in denar equivalent in accordance with Article 141 paragraph (3) of this Law,
- does not report to the Administration the suspicion of money laundering and/or financing of terrorism in accordance with Article 141 paragraph (4) of this Law,
- does not keep all data on the entry or exit of money or physically transferable means of payment through the customs line for at least ten years from the date of the transfer in accordance with Article 141 paragraph (5) of this Law,
- does not prepare annual programs or plans for supervising the implementation of measures and actions in accordance with Article 155 paragraph (2) of this Law,
- does not notify the Administration when they establish suspicion of money laundering and/or financing of terrorism as well as violation of the provisions of this Law in accordance with Article 156 of this Law,
- does not establish committees for supervision in accordance with Article 171 paragraph (1) of this Law,
- does not notify the Administration in accordance with Article 171 paragraph (3) of this Law,
- does not notify the Administration of the submitted request for initiating a misdemeanor procedure in accordance with Article 172 of this Law and
- refuses to receive and/or sign the supervision order or fails to act upon the supervision order in accordance with Article 162 paragraph (5) of this Law.

Procedure for issuing a misdemeanor payment order Article 195

(1) For the misdemeanors under this Law, the supervisory authorities under Article 151 of this Law, upon ascertaining a misdemeanor, are obliged to propose to the perpetrator of the misdemeanor a settlement procedure by issuing a misdemeanor payment order, before submitting the request for initiating a misdemeanor procedure.

(2) If the supervisory authorities referred to in Article 151 of this Law establish a misdemeanor in accordance with this Law, they shall draw up a record in which they shall record the important elements of the action from which the legal character of the misdemeanor arises, personal name, address and unique identification number of the citizen, if it is a foreigner and the number of the travel document and country, and for a legal entity, name, registered office and tax number, the time, place and manner of committing the misdemeanor, a description of the action, the legal qualification of the misdemeanor and the persons found at the scene, as well as provide a proposal for settlement by issuing a misdemeanor payment order. The record shall be signed by the supervisory authority, the authorized official and the perpetrator.

- (3) In the settlement procedure, the fine in the misdemeanor payment order shall be imposed in a fixed amount prescribed by law, and if the fine is prescribed in a range, the minimum prescribed amount for the misdemeanor shall be imposed.
- (4) The perpetrator is obliged to pay the misdemeanor payment order issued in accordance with paragraph (3) of this Article within eight days of receipt of the order to the account indicated in the payment order.
- (5) The perpetrator who pays the fine within the deadline referred to in paragraph (4) of this Article shall pay half of the imposed fine, as provided for in the legal instruction.
- (6) In the procedure that ends with the payment of a misdemeanor payment order, no costs of the procedure shall be paid.
- (7) The perpetrator who, by leaving for a stay abroad, could avoid paying the fine, is obliged to immediately pay the fine imposed by the misdemeanor payment order.
- (8) If the perpetrator fails to pay the misdemeanor payment order within the deadline referred to in paragraph (4) of this Article, the supervisory authorities referred to in Article 151 of this Law shall submit a request for the initiation of misdemeanor proceedings to the competent court.
- (9) The supervisory authorities referred to in Article 151 of this Law shall be obliged to keep records of the issued misdemeanor payment orders referred to in paragraph (1) of this Article and of the outcome of the initiated procedures.
- (10) The following data shall be collected, processed and stored in the records referred to in paragraph (9) of this Article: name and surname, i.e. title of the perpetrator of the misdemeanor, place of residence, i.e. place of stay, registered office, type of misdemeanor, number of misdemeanor payment order and the outcome of the procedure.
- (11) The personal data referred to in paragraph (10) of this Article shall be kept for ten years from the date of entry in the records.
- (12) The Minister of Finance shall prescribe the form and content of the misdemeanor payment order.

Article 196

A misdemeanor proceeding for a misdemeanor under this law may not be initiated or conducted if more than four years have passed since the day the misdemeanor was committed.

Article 197

The competent court shall decide on the misdemeanors prescribed by this law in a procedure prescribed by law.

- (2) When determining the misdemeanors in the procedure referred to in paragraph (1) of this Article, the competent court shall decide in accordance with the provisions of this Law.

CHAPTER IX. TRANSITIONAL AND FINAL PROVISIONS

Article 198

- (1) The by-laws adopted in accordance with the Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Macedonia" No. 120/18 and "Official Gazette of the Republic of North Macedonia" No. 275/19 and 317/20) shall continue to apply until the day of adoption of the by-laws determined by this Law.
- (2) The by-laws determined by this Law shall be adopted within 15 months from the date of entry into force of this Law.

Article 199

(1) The entities referred to in Article 5, paragraph (1), items 8), 9) and 10) of this Law shall be obliged to harmonize their operations with the provisions of this Law within nine months from the date of entry into force of this Law.

(2) By way of derogation from paragraph (1) of this Article, service providers related to virtual assets that, prior to the entry into force of this Law, have started to perform activities specified in this Law, shall be obliged to fulfill the reporting obligation referred to in Article 8 of this Law within 30 days from the date of adoption of the by-law referred to in Article 8, paragraph (6) of this Law.

Article 200

(1) The Financial Intelligence Unit shall, from the date of entry into force of this Law, continue to operate as the Financial Intelligence Unit in accordance with the competencies determined by this Law.

(2) The Director of the Administration appointed by the date of entry into force of this Law shall continue to hold office until the expiration of the term for which he/she was appointed.

Article 201

The Financial Intelligence Unit shall establish the electronic system for monitoring cases referred to in Article 138 of this Law within 30 days from the date of entry into force of this Law.

Article 202

(1) The Council for Combating Money Laundering and Terrorism Financing established by the date of entry into force of this Law shall continue to perform its function in accordance with the competencies determined by this Law.

(2) The oversight committees referred to in Article 171 of this Law established until the date of entry into force of this Law shall continue to perform their functions in accordance with the competencies determined by this Law.

Article 203

Misdemeanor proceedings initiated by the date of entry into force of this Law will be concluded in accordance with the provisions of the Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Macedonia" No. 120/18 and "Official Gazette of the Republic of North Macedonia" No. 275/19 and 317/20).

Article 204

(1) As of January 1, 2024, the prohibition on cash payments for goods and services referred to in Article 58 of this Law shall apply to cash payments in the amount of EUR 2,000 or more in denar equivalent in the form of one or more clearly linked transactions, which are not carried out through a bank, savings bank or through an account in another institution providing payment services.

(2) From 1 January 2025, the prohibition on cash payments for goods and services referred to in Article 58 of this Law shall apply to cash payments in the amount of EUR 1,000 or more in denar

equivalent in the form of one or more clearly linked transactions, which are not carried out through a bank, savings bank or through an account in another institution providing payment services.

Article 205

Legal entities whose shares are listed on an organized securities market referred to in Article 28 of this Law are obliged to enter the data on the beneficial owner referred to in this Law within three months from the date of entry into force of this Law.

Article 206

(1) The provisions of this Law relating to the entities referred to in Article 5, paragraph (1), items 8), 9) and 10) of this Law shall begin to apply within nine months from the date of entry into force of this Law.

(2) The provisions of Article 31, paragraph (2) of this Law shall enter into force on 1 January 2026.

Article 207

On the day of entry into force of this law, the Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Macedonia" No. 120/18 and "Official Gazette of the Republic of North Macedonia" No. 275/19 and 317/20) shall cease to be valid.

Article 208

This law shall enter into force on the eighth day from the date of its publication in the "Official Gazette of the Republic of North Macedonia".