NATIONAL BANK

DECISION No 280 of 7 November 2024

on the approval of the Regulation on the requirements for the prevention and combating of money laundering and terrorism financing in the activity of non-bank financial institutions

Published: 15.11.2024 in the OFFICIAL GAZETTE No 470-472 Article 897

Pursuant to Article 27, paragraph (1), (c) of Law No 548/1995 on the National Bank of Moldova (republished in the Official Gazette of the Republic of Moldova, 2015, No 297-300, Article 544), Article 106 paragraph (11), of Law No 92/2022 on Insurance and Reinsurance activity (Official Gazette of the Republic of Moldova, 2022, No 129-133 Article 229), Article 13, paragraphs (3) and (14), Article 15, paragraph (2) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing (Official Gazette of the Republic of Moldova, 2018, No 58-66, Article 133), the Executive Board of the National Bank of Moldova

DECIDES:

1. The Regulation on the requirements for the prevention and combating of money laundering and terrorism financing in the activity of non-bank financial institutions, as set out in the Annex, is hereby approved.

2. This Decision shall enter into force on the date of its publication in the Official Gazette of the Republic of Moldova.

CHAIRMAN
OF THE EXECUTIVE BOARD **Anca-Dana DRAGU**

No 280 Chişinău, 7 November 2024

Annex
to the Decision of the Executive Board
of the National Bank of Moldova
No 280 of November 7, 2024

REGULATION
on the requirements for the prevention and combating of money laundering and terrorism financing in the activity of non-bank financial institutions

CHAPTER I
GENERAL PROVISIONS

1. The Regulation on the requirements for the prevention and combating of money laundering and terrorism financing in the activity of non-bank financial institutions (hereinafter - the Regulation) applies to reporting entities established under Article 4, paragraph (1), (e) and (g) of Law No 308/2017 for the prevention and combating of money laundering and terrorism financing, as well as for their foreign branches and representative offices (hereinafter referred to as non-bank financial institutions), as follows:

a) non-bank credit organizations;

b) savings and loan associations;

c) insurers or reinsurers and insurance and/or reinsurance intermediaries carrying on business within the classes of life insurance, including those with investment participation.

2. Non-bank financial institutions apply this Regulation in their business relations with their customers and when conducting transactions (payments) with them.

3. This Regulation lays down the requirements for: internal programme, identification and assessment by the non-bank financial institution of the risks of money laundering and terrorism financing; application of due diligence measures concerning customers, including simplified and enhanced due diligence measures; reporting suspicious activities and transactions; data retention; organization and implementation of elements related to the internal control system; implementation of financial sanctions related to terrorist activities and proliferation of weapons of mass destruction.

4. The terms and expressions used in this Regulation have the meanings provided in Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, Law No 92/2022 on Insurance and Reinsurance activity, Law No 1/2018 on non-bank credit organizations, Law No 139/2007 on savings and loan associations, Law No 548/1995 on the National Bank of Moldova, as well as in the normative acts of the National Bank of Moldova and the Office for Prevention and Fight against Money Laundering related to the field of prevention and combating of money laundering and terrorism financing. The following terms are used for the purposes of this Regulation:

significant transaction – a transaction (operation) that exceeds the value limit set in the internal policies of the non-bank financial institution, taking into account the risks associated with the customers and the transactions performed;

legal entity identifier – an alphanumeric code, consisting of 20 characters, uniquely identifying a legal entity, established in accordance with ISO 17442 standard.

CHAPTER II
RESPONSIBILITIES

5. The non-bank financial institution develops and implements the internal programme for the prevention and combating of money laundering and terrorism financing.

6. The non-bank financial institution has an adequate internal control system to identify, assess, monitor, and understand the risks of money laundering and terrorism financing. It takes the necessary measures, involving sufficient resources, to minimize and effectively manage the identified risks.

7. The non-bank financial institution is responsible for the approval and effective implementation of the internal programme for the prevention and combating of money laundering and terrorism financing and compliance of the activity with the provisions of the legislation on the prevention and combating of money laundering and terrorism financing.

8. The non-bank financial institution designates individuals from among the members of the board and/or the executive body, including senior management and/or the administrator, entrusted with the duties of enforcing the requirements of the regulatory acts in the field of prevention and combating of money laundering and terrorism financing, and ensuring compliance of policies and procedures with these requirements.

9. The internal audit subdivision of the non-bank financial institution or an external audit entity/auditor conducts, at least annually, an assessment of the adequacy and compliance of the non-bank financial institution 's activities with the internal programme for the prevention and combating of money laundering and terrorism financing. The results of the assessment must be communicated to the manager/members of the board and/or the executive body and, upon request, to the National Bank of Moldova.

CHAPTER III
REQUIREMENTS REGARDING THE INTERNAL PROGRAMME FOR THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORISM FINANCING

10. Non-bank financial institution develops the internal programme for the prevention and combating of money laundering and terrorism financing in accordance with the provisions of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, the present Regulation, the regulatory acts of the Office for Prevention and Fight against Money Laundering, issued for the execution of this law taking into account the generally accepted practice in this field, including the documents of the Financial Action Task Force (FATF). The internal programme for the prevention and combating of money laundering and terrorism financing represents policies, methods, practices, procedures, and internal controls, including know-your-customer rules, that promote ethical and professional standards in the non-bank sector and that aim to

prevent the use of non-bank financial institutions for the purpose of money laundering or terrorism financing by organized criminal groups or their associates. This programme must ensure that operations are conducted in a safe and prudent manner.

11. In developing the internal programme, the size, complexity, nature, and volume of the non-bank financial institution's activities are taken into account, along with the types (categories) of customers, the degree (level) of risk associated with different customers or their categories and the operations conducted by them, as well as the agents and branches through which they operate. The internal programme is approved by the designated senior management person responsible for ensuring compliance of the non-bank financial institution's policies and procedures with the legal requirements on preventing and combating money laundering and terrorism financing.

12. The internal programme for the prevention and combating of money laundering and terrorism financing includes, without being limited to, the following:

1) obligations of the members of the board, the executive body, including the person responsible for senior management positions, and/or the manager of the non-bank financial institution, which include at a minimum:

a) determination of the areas of activity of the non-bank financial institution vulnerable to the risk of money laundering and terrorism financing. The areas of activity vulnerable to the risk of money laundering and terrorism financing may include, but are not limited to: operations carried out by insurance and reinsurance companies, insurance and/or reinsurance intermediaries engaged in the "life insurance" category, including those with participation in investments and other types of annuities, brokerage and trust management operations, non-bank lending, lending/credit granting and acceptance of savings deposits, financial leasing, factoring operations;

b) development of the necessary measures for implementing the policies and procedures for customer due diligence, including those with a higher risk level;

c) designation of persons entrusted with the duties of enforcing of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, including those with senior management functions;

d) approval of significant transactions of high-risk customers;

e) implementation of the internal programme for the prevention and combating of money laundering and terrorism financing, including the description of responsibilities of staff at different hierarchical levels;

f) implementation of internal procedures regarding the access within reasonable time for responsible staff to information necessary for the performance of their duties;

g) determination of the protection mechanism for the persons responsible for ensuring compliance and employees who report violations of legislation on the prevention and combating of money laundering and terrorism financing;

h) addressing identified deficiencies in the area of preventing and combating money laundering and terrorism financing, including the reporting of suspicious transactions to the Office for Prevention and Fight against Money Laundering.

2) procedures for identifying, assessing, controlling, and undertaking measures to minimize the risks of money laundering and terrorism financing.

3) customer acceptance procedures establishing at least the categories of customers that the non-bank financial institution aims to attract and the hierarchical level of staff approving the initiation of business relationship with them, depending on the degree of associated risk and the types of products and services that are provided to them;

4) measures to identify, verify and monitor customers and beneficial owners according to the degree of associated risk (know-your-customer rules), the criteria and the way to move customers from one risk category to another;

5) procedures and requirements for the application of customer due diligence measures, including simplified and enhanced due diligence measures for each category of customers, products, services or transactions subject to such measures, as well as risk management measures in the case of establishing the business relationship until the verification of the identity of the customer and the beneficial owner;

6) procedures for monitoring customer transactions in order to detect significant, complex and unusual transactions without a clear legal or economic purpose, suspicious activities and transactions;

7) measures to identify and monitor customers and their transactions with countries/jurisdictions that do not have effective systems in place to prevent and combat money laundering and terrorism financing, or are at higher risk due to high levels of criminality and corruption and/or are involved in terrorist activities;

8) the method of collecting and storing data, as well as how access to it is established;

9) internal reporting procedures and reporting to the competent authorities regarding suspicious money laundering or terrorism financing activities and transactions, or non-compliance with internal procedures or regulatory acts in the field of prevention and combating of money laundering and terrorism financing;

10) procedures and measures for verifying compliance with the rules developed and assessing their effectiveness;

11) standards for the selection, hiring and ongoing training programmes for staff in the field of prevention and combating of money laundering and terrorism financing;

12) procedures for identifying and assessing money laundering and terrorism financing risks, including measures to minimize them, related to the use of information technologies, including new ones, procured, or developed within the products and services offered by the non-bank financial institution.

13. The non-bank financial institution reviews (updates), whenever necessary, the internal programme for the prevention and combating of money laundering and terrorism financing, but at least annually, taking into account the provisions of the legislation in the field of prevention and combating of money laundering and terrorism financing.

CHAPTER IV
ASSESSMENT OF MONEY LAUNDERING AND TERRORISM FINANCING RISKS. THE RISK-BASED APPROACH

14. The non-bank financial institution is obliged to:

1) undertake actions on the identification and assessment of money laundering and terrorism financing risks in its own area of activity, taking into account the assessment of money laundering and terrorism financing risks at national level, as well as, where appropriate, the criteria and factors established by the National Bank of Moldova and the Office for Prevention and Fight against Money Laundering;

2) document the results of the assessment of the risks of money laundering and terrorism financing within its own area of activity in an evaluation report, which are approved by the person in a senior management position responsible for ensuring the compliance of policies and procedures with the legal requirements regarding the prevention and combating of money laundering and terrorism financing within the institution. Upon request, the report is submitted to the Office for Prevention and Fight against Money Laundering and/or the National Bank of Moldova.

15. The non-bank financial institution, based on the results of the money laundering and terrorism financing risk assessment, ensures the implementation of a risk-based approach, including by allocating appropriate technological, material, and human resources, so that the actions to prevent and mitigate money laundering and terrorism financing are proportionate to the risks identified in its area of activity.

16. For the purposes of implementing point 14, the non-bank financial institution conducts and updates annually the risk assessment in its area of activity, a process which involves at least:

1) preparation of a written report identifying the countries or geographic jurisdictions, the products and services provided, their distribution channel, customers and higher-risk operations, along with their weight and impact on its business;

2) drawing up an action plan aimed at minimizing the identified money laundering and terrorism financing risks.

17. The non-bank financial institution identifies and assesses the risks of money laundering and terrorism financing up to:

1) the launch and development of new products and services;

2) the use of new or emerging technologies for both new and existing products and services.

18. In the process of assessing the risks of money laundering and terrorism financing, the non-bank financial institution uses various sources of information to identify, manage and mitigate the risks related to its area of activity. This includes consideration of typologies, risk indicators, guidelines and/or recommendations issued by national and international competent authorities. In identifying and assessing the money laundering and terrorism financing risks to which it may be exposed, the non-bank financial institution considers at least the following factors:

1) the purpose of initiating a business relationship or conducting an occasional transaction, which will include information regarding the type of products and/or services requested, the destination of the payment, the volume of assets deposited, or the size of transactions carried out by the customer, the frequency of transactions and the duration of the business relationship.

2) customer and related third parties (e.g. beneficial owners of customers/third parties), customers with unusual or complex ownership and control structure, politically exposed persons, identified with a high-risk level, and the source of their assets and/or the source of the wealth held by them;

3) countries of destination (jurisdictions) with which the non-bank financial institution conducts transactions, in particular, those with high levels of criminality, corruption or other criminal activities, countries that are subject to sanctions, embargoes or similar measures imposed by relevant international organizations; countries that do not have effective systems in place to prevent and combat money laundering and terrorism financing; countries that provide financing or support for terrorist activities or in whose territory designated terrorist organizations operate; and high-risk countries (jurisdictions) designated/monitored by the Financial Action Task Force (FATF);

4) distribution networks such as transactions, products and services offered directly to the customer and/or via agents, insurance and/or reinsurance intermediaries, long chains of intermediaries, sale of products and services (remotely) via online, postal or telephone electronic technologies;

5) the volume of assumed obligations, the size of transactions, taking into account the activity of the non-bank financial institution and the profile of its customers.

19. The non-bank financial institution keeps and updates, according to the internal programme, the statistical data in its field of activity necessary for the process of identification and assessment of the risks of money laundering and terrorism financing.

CHAPTER V
CUSTOMER DUE DILIGENCE MEASURES
Section 1
Customer acceptance procedures

20. The customer acceptance procedure includes the identification and verification of the customer's identity, the customer's beneficial owner and, where applicable, the individuals authorized to act on their behalf, on the basis of information, data or documents obtained from a reliable and independent source. This also includes understanding the purpose and nature of the business relationship (where relevant) and, in higher risk situations, obtaining additional information.

21. Customer acceptance procedures will include several steps depending on the risk level of the customers. Decisions to initiate, continue or terminate business relationships with high-risk customers are made by the senior management person responsible for ensuring that policies and procedures are implemented and comply with the requirements to prevent and combat money laundering and terrorism financing.

22. The non-bank financial institution does not establish business relationships with individuals, groups or entities involved in terrorist activities and proliferation of weapons of mass destruction, included in the list referred to in Article 34, paragraph (11) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing. The non-bank financial institution informs the Office for Prevention and Fight against Money Laundering without delay about the refusal to establish business relationships with a customer, within 24 hours at the latest, submitting all the data held regarding the case.

23. The customer acceptance procedures do not affect the general public's access to the services offered by non-bank financial institution in the non-bank market.

Section 2
Customer due diligence measures

24. The non-bank financial institution applies, on a risk-sensitive basis, customer and beneficial owner due diligence measures:

1) at the initiation of business relationships;

2) when there is a suspicion of money laundering or terrorism financing, irrespective of any waivers, exemptions or limits established;

3) when there are suspicions regarding the veracity, sufficiency, and accuracy of previously obtained identification data.

25. When applying standard customer due diligence in the cases set out in point 24, the non-bank financial institution obtains at least the following information:

1) for customers who are natural persons:

a) name and surname;

b) date and place of birth;

c) citizenship and identity document details (IDNP, series and number, date of issue, code of the issuing body (if any) or other unique identifiers from an identity document containing the holder's photograph);

d) domicile and/or residence address;

e) telephone number, fax, email address (if available);

f) occupation, position held and/or name of employer;

g) source of income;

h) identity of the beneficial owner;

i) the purpose and nature of the business relationship or occasional transaction (the purpose of initiating the business relationship or carrying out the occasional transaction, the type of product and service requested, the type of transactions, the volume of assets expected to be deposited, the volume and frequency of transactions expected, the potential duration of the business relationship, etc.);

2) for legal entities and individual entrepreneurs:

a) name, legal form of organization, articles of incorporation and state registration document;

b) registered office/ business address;

c) state identification number (IDNO), according to the certificate of registration and/or the extract from the State Register issued by the competent authority with the right to carry out the state registration;

d) mailing address other than the registered office (if any);

e) identity of the natural person empowered to manage the account (representative), legality of the powers of attorney (in the absence of such a person, the administrator of the legal entity is indicated);

f) identity of the beneficial owner of the legal entity;

g) identity of persons holding senior management positions and their powers of representation;

h) rights and obligations of the company's senior management body, as evidenced by the primary registration documents or the articles of incorporation;

i) nature and purpose of the business, and their legitimacy;

j) the purpose and nature of the business relationship or occasional transaction (the purpose of initiating the business relationship or conducting the occasional transaction, the type of product and service requested, the type of transactions, the expected volume of assets to be deposited, the expected volume and frequency of transactions, the potential duration of the business relationship, etc.);

3) for trusts and similar legal arrangements:

a) name and proof of incorporation/registration, trust deed;

b) registered office/business address and country of registration;

c) nature, purpose and object of the activity (as an example: discretionary, testamentary, etc.);

d) the identity of the founder, administrator, protector (if any), beneficiaries or classes of beneficiaries and any other person who ultimately exercises effective control (in the case of other types of legal arrangements similar to trusts - the identity of persons holding equivalent positions);

e) description of the purpose/activity;

f) the purpose and nature of the business relationship or occasional transaction (the purpose of initiating the business relationship or conducting the occasional transaction, the type of product and service requested, the type of transactions, the expected volume of assets to be deposited, the expected volume and frequency of transactions, the potential duration of the business relationship, etc.);

4) for the beneficiaries of life insurance (life insurance policies) and insurance with investment participation (annuities), in addition, the following data will be obtained:

a) the name of the person in the case of beneficiaries who are persons identified by name (the full name of the beneficiary of the life insurance policy);

b) for beneficiaries designated by characteristics or category (e.g. spouse or children at the time the insured event occurs) or by other means (e.g. by will), sufficient information on the beneficiaries is obtained, so that the non-bank financial institution can establish their identity at the time of payment.

26. When identifying a higher degree of risk and applying enhanced customer due diligence measures, the non-bank financial institution obtains, in addition to the measures set out in point 25, the following information:

1) for the customer who is a natural person:

a) any other name used (married name, previously held name);

b) postal code, email address, mobile phone number;
c) resident/non-resident status;
(d) gender (sex);
e) name of employer, if any;
f) source of the customer's wealth;
g) source of funds related to the transaction;
2) for legal entities and individual entrepreneurs:
(a) unique company identifier, if any;
b) telephone number, email and fax (if any);
c) financial situation;
d) source of funds related to the transaction;
3) for trusts or similar legal arrangements:
a) telephone number, email address and fax (if any);
b) source of funds related to the transaction.

27. In the case of an assignment, in whole or in part, to a third party of life insurance and insurance with investment participation provided for in insurance legislation, the non-bank financial institution aware of the assignment identifies the beneficial owner at the time of the assignment to the natural person or legal entity who receives, for their own benefit, the value of the assigned policy.

28. The non-bank financial institution identifies the beneficial owner of the customer and take reasonable, appropriate, and risk-based measures to verify the beneficial owner's identity, ensuring that it knows who the beneficial owner is and understands the customer's ownership and control structure. For the identification of the beneficial owner, the non-bank financial institution obtains at least the information described in point 25, subpoint (1), (a) - (f), and, depending on the identified risk, additionally point 26, subpoint (1), (a)-(f).

29. When identifying the beneficial owner of the customer - legal entity, including in the case where the customer has a complex ownership structure (a legal entity whose direct owners are not natural persons), the non-bank financial institution determines the beneficial owner on the basis of the relevant registration documents. If there are no grounds for suspicion regarding the concealment of information about the beneficial owner and if, after exhausting all possible means established in accordance with point 28, it is determined that no individual meets the legal criteria to be identified as the beneficial owner (no natural person is a majority shareholder or exercises control directly or indirectly – through other means), then, as an exception, the natural person holding the position of administrator of the client is considered the beneficial owner. The non-bank financial institution keeps all the information and documents gathered in the process of determining the beneficial ownership of the legal entity customer, including those proving the exhaustion of all possible means of identification and submits them, upon request, to the National Bank of Moldova and to the Office for Prevention and Fight against Money Laundering. When identifying the beneficial owner of for-profit (commercial) legal entities, non-commercial organizations, trusts or similar legal arrangements or other types of legal entities (including those that manage and distribute funds), the non-bank financial institution takes into account the identification criteria set out in Article 52 of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing and the

Office for Prevention and Fight against Money Laundering regarding the identification of the beneficial owner.

30. When the customer or the controlling shareholder is a company whose securities are traded on a regulated market/multilateral trading system that imposes disclosure requirements, either through stock exchange rules or applicable law, to ensure adequate transparency of the beneficial owner, or when it is a majority-owned branch of such a company, there is no need to identify and verify the identity of any of the shareholders or beneficial owners of such companies. The non-bank financial institution obtains the relevant identification data from public registers, the customer or from other reliable sources.

31. The non-bank financial institution determines whether the natural or legal person initiating a business relationship is acting on their own behalf (the person's declaration regarding the beneficial owner). If the business relationship is initiated by a representative, the non-bank financial institution requests a power of attorney, legalized in accordance with the legal requirements. The non-bank financial institution applies measures to identify the representative and assesses the need for enhanced due diligence measures, in accordance with the provisions of this Regulation. The person's declaration regarding the beneficial owner is completed by the beneficial owner or their representative and contains information as outlined in point 25, subpoint (1), (a)-(f), and, depending on the identified risk, additionally point 26, subpoint (1), (a)-(f).

32. When identifying the customer, the non-bank financial institution verifies the information submitted which relates to both the customer and the beneficial owner.

33. The non-bank financial institution verifies the identity of the customer and of the beneficial owner at the initiation of the business relationship, and in low-risk situations, according to point 53 subpoint 1) of this Regulation.

34. The non-bank financial institution verifies the identity of the beneficiaries of the life insurance (life insurance policies) and insurance with investment participation (annuities) referred to in point 25 subpoint 4), at the time of payment.

35. The non-bank financial institution uses documents, data and information obtained from reliable and independent sources to verify the information submitted when identifying customers and beneficial owners. The measures applied must be proportionate to the risk posed by the customer and the types of documents presented. To this end, the non-bank financial institution uses documentary and non-documentary verification procedures:

1) for customers – natural persons:

a) confirmation of the identity of the customer or beneficial owner from an identity document or other equivalent valid document issued by competent public authorities, which includes a photograph of the holder (e.g. identity card, passport, residence permit, etc.);

b) confirmation of the date and place of birth from an identity document or other equivalent valid document issued by competent public authorities (e.g. birth certificate, identity card, passport, residence permit, etc.);

c) confirmation of the validity of official identity documents provided by an authorized person (e.g. notaries, consulates, etc., by accessing public state registers or other private registers);

d) confirmation of the residence address by requesting utility bills, tax payment documents, information from public authorities or other persons;

e) confirmation of the information submitted after opening the account/establishing the business relationship - by contacting the customer by phone or sending a letter to confirm the information provided, fax or email (if any);

f) verification of the reference provided by another non-bank financial institution/bank;

g) verification of information by using public, private or other reliable and independent sources (e.g. references provided by credit history bureaus);

2) for customers - legal entities and individual entrepreneurs - by any appropriate method depending on the degree of risk, so that the non-bank financial institution can ensure the veracity of the information, such as:

a) verifying the legal existence of the legal entity by checking the entry in the State Register of Legal Entities or, as the case may be, in another public or private register or other reliable independent sources (as an example: lawyers, accountants, etc.).

b) obtaining a copy of the articles of incorporation or the memorandum of association, partnership agreement;

c) checking information about the client in public or private databases regarding existing business relationships;

d) analysing the financial situation, if applicable;

e) conducting a verification and/or investigation either individually or through another person to determine, the existence of insolvency or liquidation, sale or resolution of other potential financial problems;

f) obtaining the reference of a non-bank financial institution/bank with which the customer has had previous business relationships, if any;

g) contacting the customer by telephone or fax, by postal services or e-mail, checking the information placed on the customer's website, if any, or visiting the headquarters or other business address indicated by the legal entity and the individual entrepreneur;

h) verifying the company's unique identifier and the related data in the public access database.

3) fiduciaries or similar legal arrangements, the non-bank financial institution verifies the information at least by obtaining a copy of the document confirming the nature and legal existence of the account holder (e.g. fiduciary deed, trust declaration, register of charities, etc.). Other verification procedures may include:

a) confirmation of the documents submitted by an independent, reputable source such as a law firm /associate firm of lawyers, accountants, etc.;

b) obtaining the reference of the non-bank financial institution/bank until the business relationship is established;

c) accessing or searching private and public databases or other independent and trusted sources;

d) verification of the identity of the authorized persons and the beneficial owner;

4) for the beneficial owner - the measures set out in subpoint 1);

5) if a person is authorized on behalf of the customer to open an account or carry out transactions, the non-bank financial institution verifies the identity of that

person, as well as the identity of the person on whose behalf they are acting, using the same procedures as described in this Regulation.

36. Documents submitted for the purpose of identifying the customer and the beneficial owner, as well as verifying their identity, are valid on the date of their submission and copies of them are stored/archived by the non-bank financial institution in accordance with established internal procedures. The documents are submitted by the customer in original or certified copy (photocopy), in accordance with the applicable legislation. In the case of submission of documents in copy (photocopy) which are not duly certified, the non-bank financial institution requires the submission of the original documents to corroborate the information and data provided. In case of remote identification and verification of the customer's identity, the non-bank financial institution requests and obtains the necessary information and documents in accordance with the regulations of the National Bank of Moldova regarding the requirements for identification and verification of the customers' identity through electronic means.

37. When identifying and verifying the identity of the customer, the non-bank financial institution obtains and processes personal data, including through electronic identification means, in accordance with the requirements of Law No 133/2011 on the protection of personal data.

38. Throughout the business relationship, the non-bank financial institution reviews and updates the information regarding the identification of customers and beneficial owners according to the associated risk. It updates the information as necessary, taking into account the relevant factors, but at a minimum, for high-risk customers - annually, for medium-risk customers - every two years, and for low-risk customers - every three years. Relevant factors that may trigger the need to update the information include at a minimum: the previous non-application of identification measures, the period of their application, the adequacy of the data obtained, new regulatory requirements for due diligence measures and/or changes in relevant circumstances regarding the customer.

Section 3
Measures to monitor activities and transactions

3**9.** The non-bank financial institution adjusts the extent of the measures for monitoring customer activities and operations based on the institutional risk assessment and individual customer risk profiles. Enhanced monitoring is applied in higher risk situations. Monitoring systems must be reviewed periodically, but no less frequently than once a year.

40. The non-bank financial institution continuously monitors the activities, operations or business relationship with the customer. Continuous monitoring actions include:

1) determination of the customer's ordinary (specific) transactions;

2) a thorough examination of transactions throughout the business relationship to ensure that they are consistent with the information held by the non-bank financial institution, the activity and risk associated with the customer. The examination of transactions requires, at a minimum, that the non-bank financial institution has effective systems and procedures in place to detect suspicious activities or transactions. Detection of suspicious activities or transactions may be

achieved by setting transaction value limits for a particular group or category of transactions. Particular attention is paid to transactions that exceed these value limits and to transactions which have no clear economic purpose;

3) verifying whether the documents and information gathered in the process of monitoring customers and transactions are up to date and relevant, including for higher risk categories of customers or business relationships;

4) identifying suspicious activities and transactions, including suspicious activities and transactions, including potential ones, as well as the sources of the funds used in these activities and transactions;

5) reporting to the person responsible with senior management functions the information necessary to effectively identify, analyse and monitor customer accounts and transactions, including those of high-risk customers;

6) real-time monitoring of all transactions (payments) made by customers or potential customers in order to detect persons, groups or entities involved in terrorist activities and proliferation of weapons of mass destruction, including for the purpose of identifying payments to prevent them from being made in violation of sanctions, prohibitions or other applied restrictions.

41. The non-bank financial institution pays close attention to all significant, complex and unusual transactions that apparently have no legal or economic purpose. The non-bank financial institution examines the nature and purpose of such transactions, documents its findings in writing and takes enhanced due diligence measures in accordance with the requirements of this Regulation. In such cases, the non-bank financial institution obtains supporting documents when carrying out the transactions and determines the source of funds used (contracts, tax invoices/invoices, shipping documents, customs declarations, salary certificates, tax reports, activity reports, other documents).

42. The person in senior management at the non-bank financial institution is responsible for documenting, maintaining, and communicating the results of monitoring to the relevant staff, as well as addressing any issues that arise and ensuring their resolution.

43. The non-bank financial institution, ex officio or upon request, refrains from carrying out activities and transactions with goods, including financial assets, for a period of 5 working days, if it establishes suspicions that may indicate money laundering, predicate offenses, terrorism financing, or the proliferation of weapons of mass destruction, whether these are at the stage of preparation, attempt, ongoing or have been already completed.

44. The non-bank financial institution applies the requirements of point 43 at the request of the Office for Prevention and Fight against Money Laundering or on its own initiative. When applying the requirements of point 43 on its own initiative, the non-bank financial institution informs immediately, but not later than 24 hours from the time of refraining, the Office for Prevention and Fight against Money Laundering of the decision taken.

45. The non-bank financial institution, in case of application of the requirements of point 43, may require the customer to provide additional data and information, including supporting documents relating to the transactions carried out, in order to properly apply the due diligence measures, and in particular, to

understand the purpose and nature of the business relationship and the source of the assets involved.

46. The measures applied in accordance with point 43 may be terminated ex officio at the expiry of the term for which they were applied or before the expiry of the term only with the written permission of the Office for Prevention and Fight against Money Laundering. The provisions of this point do not exempt the non-bank financial institution from the obligations laid down in Article 5 paragraph (3) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing and the internal programme, developed in accordance with point 12.

47. The non-bank financial institution is obliged:

1) not to carry out any activity or transaction, including through a payment account, and not to enter into any business relationship, if it cannot ensure compliance with the requirements of points 25-28, 33-35 and 40, 41;

2) in the case of an existing business relationship, to terminate the business relationship if the non-bank financial institution cannot ensure compliance with the requirements of points 25-28, 33-35 and 40, 41;

3) when there is a suspicion of money laundering or terrorism financing and the non-bank financial institution reasonably believes that complying with the requirements of points 25-28, 33-35 and 40, 41 would result in a breach of the non-disclosure obligation, it does not complete the process of applying the due diligence measures in relation to the potential customer;

4) to submit the special forms on reporting suspicious activities and transactions in the circumstances indicated in subpoints 1) - 3) to the Office for Prevention and Fight against Money Laundering in accordance with Article 11 of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing. In this case, the non-bank financial institution is entitled not to explain the reason for refusal to the customer.

48. The non-bank financial institution does not open and maintain anonymous accounts, anonymous safety deposit boxes, accounts in fictitious names, anonymous passbooks, does not issue and accept payments made through the use of anonymous prepaid cards, does not establish or continue a business relationship with a fictitious non-bank financial institution/bank or with a non-bank financial institution/bank that is known to allow another fictitious non-bank financial institution/fictitious bank to use its accounts or to provide anonymous accounts for its customers.

Section 4
Information obtained from third parties

49. The non-bank financial institution may have recourse to information held by third parties in order to implement the measures set out in points 25-28, 33, 34 and 35 under the following conditions:

1) third parties represent the reporting entities as defined in Article 4 paragraph (1) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, whether resident or similar entities located in another country (jurisdiction), which are adequately supervised and meet similar requirements as those set out in Law No 308/2017 on the prevention and combating

of money laundering and terrorism financing, including through customer due diligence and data retention measures, and;

2) third parties are not resident in high-risk jurisdictions.

50. Non-bank financial institutions that use third parties have effective procedures in place to ensure that they immediately obtain from them:

1) all necessary information related to the measures provided in points 25 - 28, 33, 34 and 35;

2) upon request, copies of identification data and other documents related to the measures referred to in points 25 to 28, 33, 34 and 35, including data obtained by electronic means.

51. The non-bank financial institution bears ultimate responsibility for implementing the measures referred to in points 25 - 28, 33, 34 and 35 in case of recourse to third parties.

CHAPTER VI
SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

52. The non-bank financial institution applies simplified customer due diligence measures when, by their nature, they may present a low risk of money laundering or terrorism financing.

53. Simplified customer due diligence measures comprise the customer due diligence measures set out in points 24 and 25 under a simplified procedure related to the low risk of money laundering and terrorism financing, which include:

1) verifying the identity of the customer and the beneficial owner after establishing of the business relationship, when it is necessary in order not to interrupt normal business practices;

2) limiting the obtaining of specific information or taking specific action on the purpose and nature of the business relationship and deducing the purpose and nature of the business relationship from the type of transactions or established business relationship;

3) reducing the frequency of updating customer identification data in the case of an established business relationship;

4) reducing the degree of ongoing monitoring of the transaction or the business relationship.

If the identity of the customer and the beneficial owner has not been verified before the business relationship is established, the non-bank financial institution ensures that this is done as soon as possible after the initial contact, but no later than one month. Until the verification measures are completed, the non-bank financial institution does not allow transactions (operations) to be carried out through the account or set specific conditions for the use of the account (value limits, types of services or products, etc.) in accordance with internal policies and procedures.

54. The non-bank financial institution, on the basis of its own assessment and in accordance with the results of the national risk assessment, determines the factors which give rise to low risks of money laundering and terrorism financing, and which determine the need to apply simplified customer due diligence measures, which include at least the following factors:

a) for the non-bank lending sector:

1) reduced amounts for payments, deposits or cash withdrawals;

2) limited number of payments, deposits or redemptions, including cash withdrawals within a certain time period;

3) the account may only store limited amounts of funds related to a product or service;

4) the product or service can only be used nationwide;

5) the product or service is accepted by a limited number of agents whose activity is known to the non-bank financial institution;

6) funds are accepted as means of payment for limited types of low-risk products or services;

7) the customer is a company whose securities are traded on a regulated market/multilateral trading system, which imposes requirements to ensure adequate beneficial ownership transparency;

8) the customer has a long history with the non-bank financial institution or its agents (customer file includes information such as credit underwriting, updated customer identification measures);

9) products and services are limited and well-defined for a circle of clients, with the aim of increasing financial inclusion.

b) for the life insurance sector:

1) life insurance policies include an annual premium not exceeding 20 000 lei or a single premium not exceeding 50 000 lei;

2) when purchasing insurance policies for pension schemes, there is no surrender clause and the policy cannot be used as collateral;

3) when acquiring pension schemes, annuities or similar programmes that provide employees with pension benefits, contributions are made through payroll deductions and the rules of the scheme do not allow the rights of the beneficiaries to be transferred;

4) life insurance policies distributed through agents on a contractual basis to take out life insurance for their employees as part of a benefits package;

5) products that are paid out upon death and/or in case of disability;

6) the reinsurer or the insurance or reinsurance intermediary is a resident of a jurisdiction with a low level of corruption and criminality, which has an effective system to prevent and combat money laundering and terrorism financing in accordance with international standards and is regularly assessed by relevant international organizations;

7) the customer has a long history with the non-bank financial institution (the customer's file includes information such as insurance underwriting, updated customer identification measures).

The non-bank financial institution, on the basis of the assessment of money laundering and terrorism financing risks at national level, as well as on the basis of the criteria and factors established by the National Bank of Moldova, accumulates sufficient information to identify whether the customer, transactions or business relationships meet the conditions referred to in this point.

55. The non-bank financial institution does not apply simplified customer due diligence measures in cases where there is suspicion of money laundering or terrorism financing.

CHAPTER VII
ENHANCED CUSTOMER DUE DILIGENCE MEASURES

56. In order to apply the legislation on the prevention and combating of money laundering and terrorism financing, the non-bank financial institution establishes the categories of customers, activities and transactions that present a higher degree of risk, based on indicators established according to the volume of transactions carried out, the type of services requested, the type of activity carried out, the economic circumstances, the reputation of the customer's country of origin, the plausibility of the explanations provided by the customer, the pre-established value limits for each category of transactions.

57. Based on its own assessment, the non-bank financial institution identifies the factors that give rise to heightened risks and determine the need for enhanced customer due diligence measures. The risk-enhancing factors are as follows:

a) for the non-bank lending sector:

1) the customer is a legal entity whose structure makes it difficult to identify the beneficial owner or those who exercise control over it;

2) the customer is reluctant to provide information about the beneficial owner, information about the purchase of a product or provides incomplete, inaccurate or contradictory information;

3) the customer who does not present himself/herself in person for identification, except for the customer identified by electronic means;

4) business relationships or remote transactions without certain safeguards, such as electronic signatures;

5) legal entities acting as personal asset management structures;

6) the client always carries out transactions below the reporting limit;

7) the source of the customer's wealth and/or source of funds intended for the loan/credit or savings deposits is unclear;

8) transactions made/received from third parties unknown to the customer or not associated with the customer;

9) the transaction is not accompanied by the necessary information on the payer or payee;

10) the customer repays the loan/credit in advance before the contractual obligation is due, but is unable to provide proof of the source of funds;

11) the customer or a third party guarantees the loan/credit with high-value goods or other assets, without having an economic sense, having the possibility to use these goods or assets directly (without taking out a loan/credit);

12) the apparently unjustified non-repayment of the guaranteed loan/credit, in order to trigger the procedure for exercising the right of pledge/mortgage;

13) the customer requests a very short repayment period of the loan/credit, contrary to their financial capacity, without any plausible explanations and documents confirming the source of funds;

14) the asset/good was purchased in cash and immediately pledged;

15) mortgage loans are paid in full before the first instalment is due, contrary to their financial capacity, without any plausible explanations or documents confirming the source of funds;

16) the pledged asset/good is located in a high-risk jurisdiction;

17) the customer requests a change in the usual method of repayment of the loan/credit, without any clear and well-founded arguments;

18) payments received from unknown or unrelated third parties;

19) the leased asset is used by a third party in the absence of a specific legal relationship with the lessee;

20) other factors identified in the risk assessment.

b) for the life insurance sector:

1) the customer is not interested in the features of the insurance product;

2) the customer's age is unusual for the type of product requested (e.g. the customer is very young or very old);

3) the customer's profession or activities are considered to be likely linked to money laundering activities, for example, they are known to generate very large cash flows or are exposed to a high risk of corruption;

4) the requested insurance product does not meet the client's needs;

5) the customer is reluctant to provide identifying information when purchasing a product or provides minimal or apparently fictitious information;

6) unjustified heightened interest in the conditions for termination of the insurance contract;

7) unjustified early termination of the insurance contract, regardless of the conditions, even with penalties, in particular when the sums are paid into different bank accounts;

8) payment of an insurance premium or high value assets compared to the client's income;

9) amendments to the insurance contract in order to establish the new insured party, the beneficiary of the insurance or to direct the benefit (premium, indemnity, annuities, etc.) to new injured third parties;

10) the insurer is only made aware of the change of beneficiary when the claim is submitted, and the customer incurs a high cost by requesting the termination of the insurance;

11) the insurer, customer, beneficiary or beneficial owner of the beneficiary are in different jurisdictions;

12) the brokerage assistant does not comply with the requirements of the insurance and/or reinsurance broker's anti-money laundering and combating the financing of terrorism programme related to the application of customer due diligence measures;

13) borrowing up to the maximum amount in life insurance in advance;

14) advance/excess payment of insurance premiums, with the early submission of the reimbursement request;

15) payment of the insurance premium from a foreign jurisdiction associated with a high risk of money laundering and terrorism financing;

16) unusual intermediary actions, such as very high commissions (including those in excess of the insurer's acquisition costs for the insurance product), refunds, lack of customer due diligence and unusual sales practices;

17) life insurance policyholders and/or contract beneficiary are companies whose structure makes it difficult to identify the beneficial owner;

18) the life insurance policyholders and/or the beneficiary of the insurance contract are companies with shareholders in custody;

19) the customer's request to change or increase the sum insured and/or premium payment is unusual or excessive;

20) the transactions carried out, insurance premiums paid by third parties unknown to the customer or not associated with the customer;

21) the beneficiary of the insurance policy and/or the agent/intermediary in insurance and/or reinsurance has residence in or is associated with jurisdictions with a high risk of money laundering and terrorism financing;

22) the client is represented by another person authorized to act on their behalf;

23) other factors identified during the risk assessment.

58. Non-bank financial institutions apply enhanced customer due diligence measures, in addition to those set out in point 26, in situations which, by their nature, may present an increased risk of money laundering or terrorism financing, at least by:

1) obtaining additional information about the customer and the beneficial owner (type of activity, asset volume, turnover, other information available from public sources, the internet), as well as frequently updating the identification data of the customer and the beneficial owner;

2) obtaining additional information about the nature and purpose of the business relationship;

3) obtaining information about the source of the client's assets, the beneficial owner and the source of the wealth held by the client;

4) obtaining information about the purpose of the activity or transaction in preparation, in progress or already completed;

5) obtaining the approval of the person responsible for senior management for the initiation or continuation of the business relationship;

6) implementing enhanced monitoring of the business relationship by increasing the number and frequency of checks carried out by focusing on activities and transactions that require additional scrutiny;

7) requiring that the first payment of transactions be made through an account opened in the customer's name with a bank that applies similar customer due diligence measures;

8) implementing specialized IT systems to ensure the efficiency of information management with respect to the identification, analysis and monitoring of customers and their operations.

59. If the customer does not present themselves in person for identification (e.g. in the case of relationships by correspondence or by telephone, e-mail, internet or other electronic means), the non-bank financial institution applies enhanced precautions by using mechanisms such as electronic signature, biometric methods, session keys, etc. During the customer's first visit to the non-bank financial institution, documents and information will be requested in accordance with the requirements of this Regulation. In addition, the non-bank financial institution applies one or more of the following measures:

1) requests the client's identification documents issued by a competent authority or body, including a specimen signature, other documents, as appropriate, to complete the client's file;

2) takes measures to protect the authenticity of documents in electronic form transmitted to the non-bank financial institution;

3) uses information provided by a partner (provider, agent, bank) with which the customer has an account and which applies at least the same know-your-customer measures and is subject to effective supervision;

4) requires that the first payment be made on behalf of the customer through an account opened with another bank which applies at least the same know-your-customer measures and is subject to effective supervision, if necessary;

5) establishes and maintains a means of contact with the customer, independent of the method used for conducting remote transactions with the customer.

60. In transactions or business relationships with politically exposed persons, family members of politically exposed persons and persons known to be close associates of politically exposed persons, the non-bank financial institution, in addition to the due diligence measures outlined in points 25 and 26, takes measures that include:

1) developing and implementing appropriate risk management systems, including procedures based on risk assessment, to determine whether a customer, potential customer or beneficial owner of a customer is a politically exposed person;

2) obtaining the approval of the person responsible for senior management functions when establishing or continuing business relationships with such customers;

3) adopting and applying appropriate measures to establish the source of wealth and source of assets involved in the business relationship or in transactions with such clients;

4) conducting enhanced and continuous monitoring of the business relationship and/or transactions with these customers;

In business relationships or transactions with politically exposed persons, family members of politically exposed persons and persons known to be close associates of politically exposed persons, the non-bank financial institution applies the enhanced due diligence measures set out in subpoints 1) to 4) for a period of 12 months following the termination of the exercise of the relevant national or international public function. After this period expires, based on a risk assessment that determines whether the person still poses risks related to politically exposed persons, the bank applies the due diligence measures according to the identified risk.

61. Non-bank financial institutions - insurers/reinsurers/insurance and/or reinsurance intermediaries take measures to determine whether the beneficiaries of a life insurance policy or an endowment insurance policy and/or, where applicable, the beneficial owner of the beneficiary are politically exposed persons, persons known to be close associates or family members of such politically exposed persons. Those measures are adopted no later than at the time of the payment or at the time of granting all or part of the policy. If heightened risks have been identified, professional participants, in addition to the customer due diligence measures set out in points 25 to 28, take the following actions:

a) inform the person responsible for senior management functions before making the payment of the proceeds the insurance policy;

b) conduct an enhanced review of the entire business relationship with the insured;

c) report to the Office for Prevention and Fight against Money Laundering the payment transaction of the of the proceeds of the insurance policy.

62. In business relationships or transactions with customers and financial institutions from countries (jurisdictions) with an increased risk designated/monitored by FATF, in addition to the enhanced due diligence measures set out in this Chapter, the non-bank financial institution applies, in accordance with the actions required by the FATF and depending on the risk, one or more of the following measures:

1) limiting the conduct of business relationships and/or the carrying out of transactions in/from the country (jurisdiction) with heightened risk or with persons from that country (jurisdiction) or, where appropriate, terminating them;

2) assessing, modifying or, where appropriate, terminating the relationship with the correspondent institution - in the country (jurisdiction) of higher risk;

3) conducting the external audit of the branches or representative offices of the non-bank financial institution located in the countries (jurisdictions) concerned;

4) closing the branch or representative office of the non-bank financial institution located in the countries (jurisdictions) concerned.

63. The measures provided in point 62, as well as other enhanced due diligence measures, are to be applied also in case they are requested by the National Bank of Moldova or the Office for Prevention and Fight against Money Laundering.

CHAPTER VIII
BROKERAGE ASSISTANTS

64. Insurance and/or reinsurance brokers who operate through brokerage assistants must ensure their inclusion in the internal programme for the prevention and combating of money laundering and terrorism financing and monitor them in order to ensure compliance with the requirements of the legislation in the field of prevention and combating of money laundering and terrorism financing. In this regard, the internal procedures, policies, and methods of the insurance and/or reinsurance brokers will include, at a minimum, aspects such as:

1) application of due diligence measures regarding the brokerage assistant at the initiation of the business relationship (at the signing of the mandate contract) and obtaining information on its legal form (individual or legal entity), ownership and control structure of the brokerage assistant, including the identification of its beneficial owner and the subsequent registration of the brokerage assistant in the Register of Brokerage Assistants, maintained by the insurance and/or reinsurance broker;

2) establishment of rules and procedures for verifying the brokerage assistant in order to understand the nature, scope and complexity of its activities, particularly the risks related to life insurance and reinsurance activity, types of life insurance, number and/or amount of receipts/payments made (insurance/reinsurance premiums, insurance indemnity), number of clients (policyholders, insured, reinsured, insurance beneficiaries), information on previous compliance with legal provisions;

3) ensuring continuous training of its own staff and brokerage assistants on the applicable legal requirements in the field of prevention and combating of money laundering and terrorism financing, as well as the programme, internal policies and procedures of the insurance and/or reinsurance broker, in order to prevent and combat money laundering and terrorism financing through insurance or reinsurance activities;

4) providing guidance and assistance to the brokerage assistant to ensure compliance with the insurance and/or reinsurance broker's anti-money laundering and counter-terrorism financing programme.

65. The insurance and/or reinsurance broker monitors the activity of the brokerage assistant to ensure that the assistant properly implements the requirements of the insurance and/or reinsurance broker's anti-money laundering and combating the financing of terrorism programme. The extent and nature of the monitoring of the brokerage assistant depend on the volume of the brokerage assistant's operations, the monitoring method used (manual, automated or combined), the results of previous monitoring (if any), the types of clients and the type of life insurance offered to the clients. As part of monitoring the activity of the brokerage assistant and applying the risk-based approach, the insurance and/or reinsurance broker identifies the specific risk criteria for assigning a risk level to the brokerage assistant and reviews the assigned risk level if necessary. The specific criteria defined for this purpose must be periodically reviewed to determine whether they are appropriate for the established risk levels.

66. The insurance and/or reinsurance broker, in order to manage and minimize the specific risks arising from the activity of a brokerage assistant implements at least the following measures:

1) creation and maintenance of a register of high-risk brokerage assistants;

2) requirement to apply enhanced due diligence measures in appropriate cases;

3) application of limits on cash receipts/payments in respect of life insurance;

4) ensuring that brokerage assistants are trained on specific indicators of suspicious and reporting standards.

CHAPTER IX
ACTIVITY AND TRANSACTION REPORTING

67. The non-banking financial institution is obliged to report to the Office for Prevention and Fight against Money Laundering, in accordance with Article 11 of Law No 308/2017 on prevention and combating of money laundering and terrorism financing, about:

1) suspicious assets, activities or transactions suspicious of money laundering, predicate offences and terrorism financing, which are in preparation, attempted, in progress or already completed - immediately, and no later than 24 hours after the identification of the action or circumstances giving rise to suspicion;

2) activities or transactions of clients in cash in the amount of at least MDL 200 000, conducted in a single operation or in several related operations within a month, starting from the first day and ending on the last day of the month - until the 5th of the month following the month in which the activities or transactions were carried out;

3) customer transactions conducted through a single operation the value of which is at least MDL 200 000, and which do not fall under the provisions of subpoint 2) - by the 10th of the month following the month in which the transactions were carried out.

68. The non-bank financial institution will have:

1) written procedures, based on the provisions of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, communicated to all staff, which require staff to report all suspicious activities and transactions;

2) mechanisms for detecting suspicious activities and transactions according to established criteria, including by competent authorities;

3) procedures for informing the person responsible for ensuring the compliance of the non-bank financial institution's policies and procedures with the legal requirements on the prevention and combating of money laundering and terrorism financing, including senior management responsible for matters related to preventing and combating money laundering and terrorism financing.

69. The non-bank financial institution transmits, through a secure channel, to the Office for Prevention and Fight against Money Laundering, the special form for reporting the activities or transactions specified in point 67.

70. The form, structure, content, as well as the manner of reporting, receipt and confirmation of special forms are outlined in the instructions and procedures for reporting activities or transactions, developed and approved by the Office for Prevention and Fight against Money Laundering.

CHAPTER X
DATA RETENTION

71. The non-bank financial institution retains all documents and information necessary to comply with customer and beneficial owner due diligence measures, including, if available, information obtained through electronic means, relevant trust services or any other secure remote or electronic identification process, whether regulated, recognized, approved or accepted by national authorities empowered by law, and copies of identification documents, account records and primary documents, business correspondence, and the results of analysis and investigations, for a period of 5 years from the termination of the business relationship or the date of an occasional transaction. The data retained must be sufficient to enable the reconstruction of each transaction in such a way that it can be used, if necessary, as evidence in criminal, administrative and other legal proceedings.

72. The document and information retention procedures include at least the following:

1) maintaining a register of identified customers and beneficial owners, which will contain at least: customer's full name; IDNO/IDNP; account number, if any and or service/product provided; date of establishing the relationship or making the transaction;

2) keeping all records of transactions or activities, primary documents and business correspondence;

3) retaining records related to the identification and verification of customers, beneficial owners, monitoring of customer transactions and keeping supporting documents related to transactions;

4) storing information on operations carried out (type, volume, destination, etc.), including complex and unusual operations;

5) archiving records of customer and beneficial owner identity, transaction information and business correspondence in a secure and operationally accessible manner.

73. At the request of the Office for Prevention and Fight against Money Laundering or the National Bank of Moldova, in accordance with Article 9, paragraph (21) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, the non-bank financial institution extends the retention period for certain types of documents and information referred to in point 71, for a period not exceeding 5 additional years.

CHAPTER XI
INTERNAL CONTROL SYSTEM REQUIREMENTS

74. The non-bank financial institution establishes policies, procedures and maintains an internal control system that ensures continuous compliance with normative acts, as well as an internal programme in the field of prevention and combating of money laundering and terrorism financing that will contribute to minimizing the associated risks.

75. The internal control system of a non-bank financial institution depends on a number of factors, including the nature, scale and complexity of the non-bank financial institution's business, the diversity of its operations, including its customer base, product and business profile, the level of risk associated with each jurisdiction of its operations and its distribution channels, i.e. the extent to which the non-bank financial institution interacts directly with its customer or through its agents.

76. The insurance and/or reinsurance broker, who conducts business through brokerage assistants, is required to include the brokerage assistants in the internal control system in order to verify their compliance with the provisions of the internal programme for the prevention and combating of money laundering and terrorism financing.

77. The internal control system of the non-bank financial institution will include the following elements:

1) conducting an audit by the staff of the non-bank financial institution or by an external audit entity/auditor to verify compliance with the internal programme for the prevention and combating of money laundering and terrorism financing. The audit functions for this purpose are:

a) independent assessment of the programme for the prevention and combating of money laundering and terrorism financing and compliance with legislative requirements;

b) monitoring staff activity through compliance testing;

c) testing the execution of transactions, where necessary;

d) informing senior management, responsible for ensuring compliance with policies and procedures about the audit results and recommending necessary actions to minimize risks and address identified weaknesses.

2) designation of persons responsible for ensuring the compliance of the non-banking financial institution with the normative acts in force on the prevention and combating of money laundering and terrorism financing. The person with senior management responsibilities, appointed from among the members of the Board of the non-banking financial institution and/or the executive body, has at least the following duties:

a) advises the employees of the non-bank financial institution on issues arising during the implementation of the programme for the prevention and combating of money laundering and terrorism financing, including the identification and examination of the non-bank financial institution's customers and the assessment of the risk of money laundering and terrorism financing;

b) takes decisions on the basis of the information received;

c) takes measures regarding the reporting of information to the Office for Prevention and Fight against Money Laundering in accordance with the legislation;

d) organizes the training of non-bank financial institution employees in the field of prevention and combating of money laundering and terrorism financing, including brokerage assistants by insurance and/or reinsurance brokers;

e) cooperates with the audit department in order to verify the compliance of the non-bank financial institution's activity with the legislation in the field of prevention and combating of money laundering and terrorism financing;

f) performs other functions in accordance with this Regulation and the internal documents of the non-bank financial institution.

78. The person conducting the audit of the non-bank financial institution reviews the implementation of the programme for the prevention and combating of money laundering and terrorism financing by the non-bank financial institution and submits a written report on the results of the analysis to the senior management of the non-bank financial institution.

79. The non-bank financial institution will have in place programs for the selection and continuous training of staff in the field of prevention and combating of money laundering and terrorism financing. The non-bank financial institution ensures that its staff have the appropriate knowledge, skills and abilities to effectively fulfil the responsibilities of compliance with the requirements for the prevention and combating of money laundering and terrorism financing.

80. The screening and training programs indicated in point 79 will cover various aspects of the process of preventing and combating money laundering and terrorism financing and the obligations under the relevant legislation, including:

1) training of newly hired staff regarding the importance and basic requirements of the respective programs;

2) annual training of "front-line" staff (employees who have direct contact with customers) regarding the verification of the identity of new customers, continuous monitoring of existing customers' accounts, detecting indicators and reporting suspicious activities and transactions, and those subject to reporting, etc.;

3) regular updating of staff responsibilities;

4) new techniques, methods and trends in money laundering and terrorism financing;

5) the level of staff involvement in the process of preventing and combating money laundering and terrorism financing.

The content and programme of the staff training must be adapted to the individual needs of the non-bank financial institution.

81. When establishing branches or representative offices in the territory of other countries, as well as during their activity, under the conditions of the legislation, the non-bank financial institution applies the requirements and measures to prevent and combat money laundering and terrorism financing in accordance with its own internal control system, internal policies and procedures and the regulatory acts of the Republic of Moldova, to the extent permitted by the legislation of the host country. If the requirements to prevent and combat money laundering and terrorism financing in the host country are insufficient, the non-bank financial institution must ensure the implementation of the requirements set forth in the regulatory acts of the Republic of Moldova, to the extent permitted by the host country's legislation. If the host country does not allow the proper application of the requirements of the regulatory acts of the Republic of Moldova, the non-bank financial institution applies appropriate additional measures to mitigate the risk of money laundering and terrorism financing and informs the National Bank of Moldova within two months. The National Bank of Moldova may apply supervisory measures in accordance with the legal framework to ensure that branches opened in other countries comply with the regulatory acts related to the given field. If non-compliance is found, the National Bank of Moldova may restrict the activity or withdraw the approval granted for opening branches in the territory of other countries. In application of this point, the National Bank of Moldova issues technical standards regarding the type of additional measures, as well as the minimum actions to be taken by the non-bank financial institution in case the legal requirements of another country (jurisdiction) do not permit the implementation of the measures outlined in this point.

82. The non-bank financial institution communicates and implements the provisions of its own programmes for the prevention and combating of money laundering and terrorism financing within its branches, representative offices and other subdivisions, including those located in other countries. In order to prevent and combat money laundering and terrorism financing, the non-bank financial institution exchanges data with its branches, representative offices and other subdivisions, provided that the requirements of the normative acts are met.

83. In the case of opening branches in the territory of other countries, at the financial group level, the internal control system and the programme for the prevention and combating money laundering and terrorism financing will include, in addition to the elements established in points 77, 79, 80, the following additional elements:

1) policies and procedures on the exchange of information for the purposes of customer due diligence and effective management of money laundering and terrorism financing risks;

2) requirements for the provision of intra-group information concerning customers, accounts and transactions where this is necessary for the application of measures to prevent and combat money laundering and terrorism financing;

3) appropriate requirements for maintaining the confidentiality of information subject to exchange which constitutes professional secrecy and personal data, as well as the manner in which such information is processed.

CHAPTER XII
REQUIREMENTS FOR THE APPLICATION OF INTERNATIONAL RESTRICTIVE MEASURES

84. The non-bank financial institution immediately applies restrictive measures related to terrorist activities and the proliferation of weapons of mass destruction with respect to assets, including those obtained from or generated by assets owned or controlled, directly or indirectly, wholly or jointly, by persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, as well as by persons, groups and entities acting on behalf of, at the direction of, owned or controlled, directly or indirectly, by such persons, groups and entities.

85. For the application of restrictive measures in accordance with point 84, the non-bank financial institution develops internal rules and procedures which must include at least the following elements:

1) procedures for collecting, maintaining and updating the list of persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction, subject to international restrictive measures (including through the use of existing databases), as required by Law No 308/2017 on the prevention and combating of money laundering and terrorism financing and Law No 25/2016 on the application of international restrictive measures, including the use for this purpose of the Order of the Intelligence and Security Service No 14/2019 on the list of persons, groups and entities involved in terrorist activities and proliferation of weapons of mass destruction;

2) procedures for the screening/detection of designated persons or entities and transactions/payments involving assets, applicable to prospective customers, existing customers and applicants for life insurance and annuity transactions/policies;

3) competences of persons responsible for implementing internal rules and procedures for the application of international restrictive measures for the freezing of funds;

4) information/reporting procedures, internally and to the Office for Prevention and Fight against Money Laundering.

86. The non-bank financial institution, when identifying assets, including those derived from or generated by assets, owned or controlled, directly or indirectly, wholly or jointly, by persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, takes the following sequential steps:

1) by the decision (order) of the person with senior management functions of the non-banking financial institution, it refrains, for an indefinite period of time, from carrying out activities and transactions which are in preparation, attempted, in progress or already completed, for the benefit or in favour of, directly or indirectly, wholly or partially, of persons, groups/entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to the restrictive measures, as well as persons, groups and entities acting on behalf of or at the direction of such persons, groups and entities;

2) immediately informs, but not later than 24 hours from the moment of applying the restrictive measure, the Office for Prevention and Fight against Money Laundering about the indefinite abstention from the execution of activities and transactions. The information sent to the aforementioned authority includes at least the following elements:

a) data and information (name of individual/legal entity; IDNO/IDNP, if any; country of origin/residence; list of the competent authority/organization to which the restrictive measure applied refers, etc.) on the identified person, group or entity;

b) data and information (volume; currency; payee; destination, etc.) about the identified asset;

c) informing on the decision of the person responsible with senior management functions of the non-bank financial institution to refrain, for an indefinite period, from carrying out activities and transactions in relation to the identified asset;

3) if applicable, the non-bank financial institution accepts additional payments, made by a third party, or the increase in the value of assets on which the restrictive measures have been applied and extends the applicability of the restrictive measures to the additional assets, taking into account the requirements of point 86 subpoint 1), and also informs the Office for Prevention and Fight against Money Laundering thereof, taking into account the requirements of point 86 subpoint 2) (a) and (b);

4) informs the National Bank of Moldova about the restrictive measures applied, taking into account the requirements of point 86, subpoint 2) (a) and (b)."

87. In case of doubts or suspicions that do not allow for a firm belief as to the identity of the person, group or entity included in the list referred to in Article 34 paragraph (11) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing, the non-bank financial institution informs the Office for Prevention and Fight against Money Laundering without delay, no later than within 24 hours.

88. The non-bank financial institution continuously monitors the official websites of the United Nations, the European Union and the Intelligence and Security Service to ensure the proper application of restrictive measures on persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction.

CHAPTER XIII
OTHER PROVISIONS

89. In the event of a violation of the provisions of this Regulation, of the obligations set out by the legislation on the prevention and combating of money laundering and terrorism financing, the National Bank of Moldova applies sanctions in accordance with the legislation in force.

90. In the application of this Regulation, the non-bank financial institution informs the National Bank of Moldova about suspicious activities and fraud incidents that pose significant risks to the safety, sound operation or reputation of the non-bank financial institution.