**THE SERVICE FOR
PREVENTION AND CONTROL
OF MONEY LAUNDERING**

MD-2004, Chişinău, 198 Ştefan cel Mare şi Sfânt ave, www.spcsb.md, office@spcsb.gov.md Tel. (+373) 22-257-243

Unofficial translation

ORDER

23.08.2018 **no. 34**

Regarding the approval of the Regulation on prevention and control measures against money laundering and terrorist financing for reporting entities forseen by art. no. 4, par. (1), letter e) of the Law no. 308 of 22 December 2017 on prevention and combating money Laundering and terrorist financing

According to the provisions of art. 15, art. 22, par. (1), letter k) of the Law no. 308 of 22 December 2017 on the prevention and combating of money laundering and terrorist financing (Official Monitor of the Republica of Moldova, 2018, no. 58-66, art. 132),

I ORDER:

1. To approve the attached Regulation on the requirements for the prevention and combating of money laundering and terrorist financing for the reporting entities referred to in art. 4 par.(1) letter e) of the Law no. 308 of 22 December 2017 on the prevention and combating of money laundering and financing of terrorist.

2. Interaction with reporting entities and the control over the execution of this order is carried out by the Service for the Prevention and Combating of Money Laundering

3. This Order enters into force on August 23, 2018

Director **Vasile ŞARCO**

Annex
to the order no. 34 din 23.08.2018

REGULATION
on the requirements for the prevention and combating of money laundering and terrorist financing in the activity of real estate agents

Chapter I
GENERAL PROVISIONS

1. The present Regulation sets out the rules applicable to real estate agents (hereinafter reffered to as „Agents") in order to: identify assess the risks of money laundering and terrorist financing, applying the risk-based approach, developing internal policies and procedures, applying customer due diligence requirements, including simplified and enhanced precautionary measures, data retention, reporting of activities and transactions covered by the law on the prevention and combating of money laundering and terrosit financing, the organization and implementationof elements related to the internal control system, the implementation of the precautionary measures and the restrictive measures as well as other requirments for implementing measured top revent and combat money laundering and terrorist financing.
2. The present Regulation is developed based on the provisions of the Law no. 308 of 22 December 2017 „On the prevention and combating of money laundering and terrorist financing" (hereinafter - Law no. 308 of 22 December 2017), Methodology for the identification of suspicious money laundering activities and terrorist financing approved by the Government Decision no. 496 of 25 May 2018, Order no. 15 of 08 June 2018 on the approval of the Guide on the identification and reporting of suspicious money laundering activities or transactions, Order no. 16 of 08 June 2018 on the approval of the Guide on the identification and reporting of suspicious activities or transactions for terorism financing, Order no. 17 of 08 June 2018 on the approval of the Guide on the identification and monitoring of politically exposed persons, Order no. 18 of 08 June 2018 on the approval of the Instructions on the reporting of activities or transactions falling within the scope of the Law no. 308 of 22 December 2017 and other normative and legislative acts regulating the field of prevention and combating money laundering and terrorist financing.
3. In the context of this Regulation, **a real estate agent (hereinafter – agent)** represents a legal or physical person who provides brokerage services in real estate transaction, including the sale or purchase of real estate, and provides advice in this area in return for a pre-defined commision from transaction value.
4. The Service for the Prevention and Combating of Money Laundering (hereinafter - SPCSB) performs the function of the supervisory body of the real estate agents within the limits of the monitoring and verification compliance with the provisions of the Law no. 308 of 22 December 2017.

Chapter II
RESPONSABILITIES

5. The Agent shall have in place and implement an effective internal programme on the prevention and combating of money laundering and terrorist financing.
6. The Agent shall have in place an adequate internal control system to identify, assess, monitor and understand the risks of money laundering and terrorist financing. The Agent shall apply all necessary measures and use sufficient resources to minimize the identified risks.
7. The Agent shall be responsible for, approving and ensuring the implementation of the internal programme on the prevention and combating of money laundering and terrorist financing.
8. The Agent shall appoint persons entrusted with responsibilities to comply with those requirements with regard to the prevention and combating of money laundering and terrorist financing.

Chapter III
REQUIREMENTS REGARDING THE INTERNAL PROGRAMME ON THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORIST FINANCING

9. The internal programme on the prevention and combating of money laundering and terrorist financing represents a series of policies, procedures and internal controls including the customer due diligence procedures which promotes ethical and professional standards in the agent sector and prevents its use for the purposes of money laundering or terrosist financing by organised criminal groups or their associates. This programme must ensure that the agent operations are carried out in a safe and prudent way.

10. The Agent shall draw up the internal programme on the prevention and combating of money laundering and terrorist financing in accordance with the provisions of the Law no.308 of 22 December, 2017 on the Prevention and combating of money laundering and terrorist financing, the present Regulation, other regulatory acts of the Office for Prevention and Fight against Money Laundering, issued in the application of this law, taking into account the generally-accepted practices, including the documents issued by the Basel Committee and the international Financial Action Task Force (FATF).

11. The internal programme shall take into account the size, complexity, nature and volume of the agent's activities, identified risks of money laundering and terrorism financing, the types (categories) of customers, the products and services rendered, the geographical area covered by the Agent, the degree (level) of risk associated with different customers or customer categories as well as the customers' transactions.

12. Internal programme on the prevention and combating of money laundering and terrorist financing shall include, without being limited to, the following:

1) the responsibilities of the Agent shall include at least:

a) to determine the Agent's areas of activity exposed to the risk of money laundering and terrorist financing, with a precise delimitation of the competences of each subdivision responsible for the prevention and combating of money laundering and terrorist financing.

b) to determine the mechanism for identifying, evaluating and taking actions to control and minimize the risks of money laundering and terrorist financing;

c) to develop necessary measures to implement policies and procedures for knowing the actual clients and beneficiaries, including for high-risk customers;

d) to allocate sufficient resources for the effective performance of activities aiming to prevent and combat money laundering and terrorist financing;

e) to appoint persons responsible for the application of the provisions of the Law no. 308 of 22 December 2017;

f) to determine the lines of responsibilities of the Agents at different hierarchical levels;

g) to grant, within reasonable time limits, to the responsible persons, appointed in accordance with the provisions of point e), access to the information required for the application of the provisions of the Law no. 308 of 22 December 2017 and this Regulation;

h) to address the deficiencies identified in the field of the prevention and combating of money laundering and terrorist financing;

2) the procedures for identifying, assessing, controlling and undertaking measures to minimize the risk of money laundering and terrorist financing;

3) the methods to be used to identify, verify and monitor customers and beneficial owners according to the degree of associated risk (CDD procedures), the criteria and the procedure of moving customers from one risk category to another;

4) the CDD measures to be developed for each category of customers, products, services or transactions (operations) to be performed;

5) the procedures to be applied to monitor customer transactions for detecting significant, complex and unusual transactions, or suspicious activities and transactions;

6) the procedures and requirements set for the application of simplified customer/transaction due diligence measures when, by their very nature, they may present a lower-level risk of money laundering and terrorist financing;

7) the procedures and requirements set for the application of enhanced CDD measures in the cases of complex and unusual transactions performed without a clear legal or economic purpose, as well as significant and suspicious transactions, including politically exposed persons;

8) the procedures describing the collection and storage of information as well as the conditions of granting access to them;

9) the procedures describing the internal and external (to competent authorities) reporting on suspicious activities and transactions;

10) the procedures and measures aiming to ascertain compliance with relevant standards and to assess their effectiveness;

11) the standards developed for the personnel's recruitment, employment and training programmes in the CDD field;

13. Whenever required, but at least annually, the Agent shall review (update) its internal programme on the prevention and combating of money laundering and terrorist financing, taking into account relevant legal provisions in force.

Chapter IV
THE ASSESSMENT OF RISK OF MONEY LAUNDERING AND TERRORIST FINANCING. THE RISK-BASED APPROACH

14. The Agent commits to identify and evaluate the existing operational risk exposure to money laundering and terrorist financing, taking into account the threats and vulnerabilities identified in the national, regional and sectoral evaluation reports, as well as the criteria and risk factors elaborated for that purpose by the the Office for the Prevention and Fight against Money Laundering. The results of the assessment shall be approved by the designated person who is responsible for ensuring the compliance of policies and procedures with the legal requirements established for the prevention and combating of money laundering and terrorist financing.

15. For the purpose of implementing item 14 the Agent shall evaluate the risks of money laundering and terrorism financing in its own area of activity which shall include at least:

1) the preparation of a written report describing the countries or geographical areas, products, customers and transactions (operations) presenting a high degree of risk, their share and impact on the Agent's activity;

2) the drawing up of an action plan aiming to minimize the identified risks of money laundering and terrorist financing;

3) update the assessment under this item after each national risk assessment carried out by the Office for Prevention and Fight against Money Laundering and each update of the criteria and risk factors established by the Office for Prevention and Fight against Money Laundering.

16. The Agent shall identify and assess existing risks of money laundering and terrorist financing before:

1) it developes and launches new products and services;

2) it starts using new or developing technologies for both new and existing products and services.

17. In case of identifying systematic ML/TF risks, the agent immediately informs the Office for Prevention and Anti-Money Laundering.

18. While assessing its risk exposure to money laundering and terrorist financing, the Agent shall analyse different elements and characteristics of available variables, such as: the purpose of the business relationship, the volume of transacted assets or the number of transactions conducted, the frequency and duration of a business relationship, etc.

19. Following the assessment of its risk exposure to money laundering and terrorist financing, the Agent shall use the risk-based approach to determine and implement actions plan aiming to manage and minimize the identified risks, including through the allocation of appropriate technological, material and human resources.

20. In accordance with the requirements of the internal programme, the Agent shall retain and update statistical data, required to identify and assess the risk exposure to money laundering and terrorist financing.
21. The Agent shall apply simplified and enhanced CDD measures based on the degree of risk identified, taking into account the type of the customer, the identified degree of risk exposure to money laundering and terrorist financing, the country (jurisdiction), the type of business relationship, the product / service provided or the transaction performed etc.

Chapter V
CUSTOMER DUE DILIGENCE MEASURES

Section 1
Customer acceptance procedures

22. The customer acceptance procedures will contain provisions on customers who appear to expose the Agent to an increased risk of money laundering and terrorist financing. In order to minimize this risk, the customer information should be examined under a number of aspects, such as:

a) the customer's business experience;
b) the country of origin;
c) the activities run by the customer or other risk indicators set by the agent

23. The customer acceptance procedures will include several steps depending on the degree of the risk associated with each customer. The decision to start, continue or terminate a business relationship with a customer who is associated with an increased degree of risk shall be taken by the senior manager of the Agent by coordinating the decision with the designated person responsible for the implementation and compliance with the requirements for the prevention and combating of money laundering and terrorist financing.
24. The Agent shall not enter into business relations with persons, groups or entities involved in terrorist activities and the proliferation of weapons of mass destruction, specified in art. 34 par. (11) of the Law No 308 of 22 December 2017 on the prevention and combating of money laundering and terrorist financing. The Agent shall communicate immediately, but not later than within 24 hours, to the Office for the Prevention and Fight against Money Laundering its decision to refuse entering into business relationship with a customer, providing all supporting data.
25. The customer acceptance procedures should not hinder the public's access to Agent's services.

Section 2
Establishing the identity of the customer and the beneficial owner

26. The Agent shall take steps to establish the identity of the customer and the beneficial owner:
1) before it enters into a business relationship;
2) when there is a suspicion of money laundering or terrorist financing, regardless of any applicable derogation, exemption or threshold;
3) when there are suspicions regarding the veracity, sufficiency and accuracy of the previously obtained customer identification data;
27. While performing customer identification as laid down in item 25, the Agent shall obtain at least the following information:
1) when dealing with a customer who is a natural person:
a) a customer's full name;
b) the date and place of birth;
c) citizenship and the ID card data (IDNP, series and number, date of issue, code of the issuing body (if any) or other unique elements of an identity document containing the holder's photograph);
d) permanent and/or residence address;
e) the occupation, a public office held;
f) the source of income;
g) the financial product and service requested;

2) when dealing with a customer who is a legal person or an individual entrepreneur:

a) the name, the legal form of organisation, the articles of incorporation and the act on the state registration of the legal person;

b) the head office / business address;

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

d) the mailing address other than headquarters (if any);

e) the identity of the natural person authorised to manage the account, who exercises control over the legal entity based on the ownership rights held or through other means (in the absence of such person, the Agent shall indicate the senior manager of the legal person);

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

g) the rights and obligations of the management body of the company arising from the primary registration documents or its constitutive act;

h) the nature and the purpose of the activity, their legitimacy;

3) when dealing with customers who are legal entities providing fiduciary asset management services (trusts, investment funds, etc.) irrespective of ownership and country of registration:

a) the name and the proof of incorporation / registration;

b) the headquarters / business address and the country of registration;

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

d) full names of the founder, the administrator, the protector (if any), the beneficiaries or classes of beneficiaries, and any other person who ultimately exercises effective control over the entity;

e) the description of the purpose / activity;

28. While performing identification of high-risk customers, the Agent shall obtain the following additional information:

1) when dealing with natural persons:

a) any other name used (the married name, previously-held name or nickname);

b) business address, postal code, email address, mobile phone number;

c) the status of resident / non-resident;

d) gender;

e) the name of the employer, if any;

f) the information on the source of the customer's wealth;

g) certificate of residence.

2) when dealing with legal persons and individual entrepreneurs:

a) unique company identifier, if any;

b) email, telephone and fax numbers;

c) information on the identity of persons holding senior management positions;

d) the financial situation;

e) VAT registration number and / or tax payer in the state of residence.

3) when dealing with legal entities providing fiduciary asset management services (trusts, investment funds, etc.) irrespective of ownership and country of registration:

a) email, telephone and fax numbers;

b) information on the identity of the persons holding senior management positions, if any;

c) the source of funds;

29. The Agent shall identify the customer's beneficial owner and apply reasonable risk-based measures to verify his identity to be sure that it knows the ultimate beneficial owner and understands the property and control structures of the customer. In order to identify the beneficial owner, the agent applie the requirements specified in item 27 sub-item 1) letter a)-f) and, additionally, depending on the risk identified, in item 28 sub-item 1) letter. a)-f). The Agent will not identify the beneficial owner in the case of business relationships with international organizations and institutions established in accordance with international treaties and / or intergovernmental agreements between countries.

30. The agent will establish internal procedures for identifying the beneficial owner using the guides and instructions approved for this purpose by the Office for Prevention and Fight against Money Laundering.

31. When identifying the beneficial owner for the customer who is a legal person, including entities with complex ownership structure (a legal person whose direct owners are not natural persons), the Agent shall determine the beneficial owner on the basis of the appropriate registration documents and if, after having exhausted all possible measures and that there are no grounds for suspicion, no person has been identified as the beneficial owner, the natural person acting as the administrator of the customer shall be deemed to be the beneficial owner. The agent keeps all the information and documents accumulated in the process of determining the beneficiary's effective legal status in order to confirm to the supervisory authorities the exhaustion of all possible means of identifying the actual beneficiary.

32. The Agent shall determine whether the natural or legal person who opens the payment account or initiates a business relationship acts on his behalf (the person's statement of the beneficial owner) and, where an account is opened or a business relationship is initiated by the authorised representative, the Agent shall request the Power of Attorney to be submitted, certified in the manner prescribed by the law. The Agent shall apply CDD measures to establish the identity of the authorised representative in accordance with the provisions of this Regulation. The statement of the beneficial owner shall be completed by the beneficial owner or by his authorised representative and shall contain information specified under item 27 sub-item 1) (a)-(f) and, additionally, depending on the risk identified, in item 28 sub-item 1) (a)-(f) of this Regulation.

33. When performing the customer identification, the Agent shall verify the submitted information that relates to both the customer and the beneficial owner.

34. In order to verify the identification information provided for the customer and the beneficial owner, the Agent shall use documents, data and information obtained from reliable and independent sources. Verification effort must be proportionate to the risk associated with the customer and the types of submitted documents. For this purpose, the Agent shall use documentary and non-documentary verification procedures:

1) when dealing with customers who are natural persons:

a) to confirm the identity of a customer or a beneficial owner by using a legal valid document, containing a photograph of the holder, such as an identity card, passport, residence permit, etc.

b) to confirm the date and place of birth by using any legal documents, such as the birth certificate, ID card, passport, residence permit, etc.;

c) to confirm the validity of the presented identity documents by requesting an expert advice of competent persons, such as notaries, embassies, etc.;

d) to confirm the residence address by requesting the invoices for public utility services, tax payment documents, information provided by public authorities or other persons;

e) to confirm the information submitted after the account has been opened - by contacting the customer by telephone, fax, e-mail (if any) or by sending a letter by post;

f) to verify information by using public or private databases, or any other safe and independent sources (for example, references provided by credit history offices / agencies).

2) when dealing with customers who are legal persons and individual entrepreneurs - by any appropriate method depending on the degree of associated risk, so that the Agent can assure the veracity of the information, such as:

a) to verify a legal existence of the legal person, the individual entrepreneur or the individual performing other type of activity by checking the records made in the State Register of legal persons or, as the case may be, in another public or private register or other independent safe source, such as legal firms, accountants, etc.;

b) to obtain a copy of the articles of incorporation or the memorandum of association, a partnership contract;

c) to verify in public or private databases information on the customer’s existing business relationships;

d) to conduct a research / investigation, either individually or through another person, aiming to determine whether there is any evidence that the person is insolvent, filed for liquidation, intends to sell the entity or there are other potential financial problems which have to be taken care of;

g) to contact the customer by telephone or fax, by post or email, to check the information placed on the customer's website, if any, or to make a field visit to the headquarters or other business address indicated by the legal entity, the individual entrepreneur or an individual performing other type of activity;

h) to verify the company's unique identifier and the related data, which can be accessed through a public database;

35. Documents submitted in order to identify the customer and the beneficial owner as well as to verify their identity must be valid on the date of their presentation and their copies shall be stored / archived by the agent in accordance with the established internal procedures. The documents shall be submitted individually by each person (the customer, the administrator, the beneficial owner, etc.) or by their authorised representatives.

36. Throughout its business relationship, the Agent shall review and update the identification information for customers and beneficial owners, depending on associated risk. It can update the information whenever it deems necessary, but at least annually - for high-risk customers, and once in every three years - for low- and medium-risk customers.

Chapter VI
SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

37. The Agent shall apply simplified CDD measures when, by their very nature, they present a lower degree of risk of money laundering or terrorist financing.

38. Simplified CDD measures represent CDD measures referred to in par. 38.1-38.4. under a simplified procedure corresponding to the low degree of risk of money laundering and terrorist financing, which include:

38.1. verifying the identity of the customer and the beneficial owner after establishing a business relationship with the customer;

38.2. a less frequent updating of the identification data;

38.3. a reduced degree of ongoing monitoring of transactions or the business relationship;

38.4. obtaining of a limited amount of information on the purpose and nature of a business relationship.

39. Based on its own assessment, the Agent shall set out the factors that generate lower risk of money laundering and terrorist financing and which determine the application of simplified CDD measures using for this purpose indicators specified in art. 7 par.(3) of the Law no. 308 of 22 December 2017.

40. The simplified CDD measures can not be applied if there is a suspicion of money laundering or terrorist financing.

41. On the basis of risk-assessment of the money laundering and terrorist financing at national level and on the basis of the criteria and factors established by the authorities with supervisory functions, the Agent shall accumulate sufficient information to determine whether the customer, transactions or business relationships meet the conditions specified in art. 7 par.(3) of the Law no. 308 of 22 December 2017.

Chapter VII
ENHANCED CUSTOMER DUE DILIGENCE MEASURES

42. If the risk of money laundering or terroist financing is increased, the agent applies enhaced CDD measures proportionate to the risk identified, increasing the degree of business relationship monitoring in order to determine whether the activity or transaction is unusual or suspicious.

43. Agents shall apply enhanced CDD, in addition to those set out in paragraphs 5 to 7, where they are likely to present a high risk of money laundering or terrorist financing, as well as in other situations, according to the criteria and factors established by the Office for Preventind and Fighting against

Money Laundering, including by applying the measures provided by art. 8 par. (2) of the Law no. 308 of 22 December 2017.

44. Based on its own assessment, the Agent shall set out the factors that generate an increased degree of risk of money laundering or terrorist financing and which determine the application of enhanced CDD measures. For this purpose, the Agent will use the factors that generate increased risks as described in art. 8 par. (3) of the Law no. 308 of 22 December 2017.

45. In case of business relationships or transactions with politically exposed persons, their family members or persons associated with politically exposed persons, the reporting entities, in addition to the enhaced measures provided for in paragraph (5) to (7), shall apply the following measures:

45.1. Developing and implementing appropriate risk management systems, including risk based procedures, to determine whether a customer, potential customer or the actual beneficiary of a customer is a politically exposed person;

45.2. Obtaining the approval of a person with senior management positions in establishing or continuing business relationships with such customer;

45.3. Adopting appropriate measures to determine the source of the goods involved in the business relationship or the transaction with such customers;

45.4. Performing increased and continuous monitoring of the business relationship if the customer is permanent.

46. In the case of activities, transactions or business relationships with politically exposed persons, family members of politically exposed persons and persons associated with politically exposed persons, the agent applies the provisions of the Guidance on the identification and monitoring of politically exposed persons approved by the Order of the OPCML Director no. 17 of 08 June 2018.

Chapter VIII
Monitoring of the customer's activity and transactions

47. The Agent shall continuously monitor the customer's activities, transactions (bank operations), or its business relationship with the customer. The ongoing monitoring process shall include:

1) determining the customer's ordinary (specific) transactions;

2) an extensive examination of transactions conducted during its business relationship with the customer, to ensure that they are in line with the information held by the Agent, the customer's declared activity and the risk level associated with the customer. The examination of transactions requires, at least, the Agent to have in those mechanisms / IT solutions, including the automated ones, which would enable the Agent to detect suspicious activities, transactions or people.

3) verifying whether documents and information gathered during the customer / transaction monitoring are up-to-date and relevant, including for high-risk customers or business relationships;

4) drawing up a transaction monitoring protocol that will reflect all transactions (type, volume, currency, destination of funds, etc.) and all supporting documents submitted or related to those transactions, whenever deemed necessary depending on the associated level of risk. The monitoring protocol shall be kept in the customer's file and upon request, shall be submitted to the Office for Prevention and Fight against Money Laundering.

5) identificarea activităţilor, tranzacţiilor suspecte, inclusiv a celor potenţiale, precum şi a surselor mijloacelor băneşti utilizate în aceste activităţi şi tranzacţii;

6) reporting to the responsible person of the information on risks identified with respect to the customers' accounts and transactions, including for high-risk customers;

7) a real-time monitoring of all transactions conducted by customers or potential customers, to identify persons, groups or entities involved in terrorist activities and the proliferation of weapons of mass destruction, including to identify and prevent any payments made by them in violation of the sanctions, prohibitions or other restrictions imposed.

48. The Agent shall pay particular attention to all significant, complex and unusual transactions that do not appear to have a clear economic or legal purpose. The Agent shall examine the nature and the purpose of such transactions, document the findings and take enhanced CDD measures in accordance with the requirements of this Regulation. Besides, the Agent shall obtain supporting documents for

such transactions and determine the source of the funds (contracts, tax invoices / invoices, shipping documents, customs declarations, salary certificates, tax reports, activity reports, other documents).
49. If the risk of money laundering or terrorist financing is increased, the agent applies enhaced CDD measures to customers proportionate to the risk identified, increasing the degree of business relationship monitoring to determine whether the activity or transaction is unusual or suspicious.
50. The Agent shall apply enhaced CDD measure, in addition to those set out in par. (5)-(7), where they are likely to present a high risk of money laundering or terrorist financing, as well as in other situations, according to the criteria and factors established by OPCML, including by applying the measures provided by art. 8 par. (2) of the Law no. 308 of 22 December 2017.
51. On the basis of its own assessment, the agent determines the factors that generate increased risks and determines the need to apply enhanced CDD measures. For this purpose, the agent will use the factors that generate increased risks as described in art. 8 par. (3) of the Law no. 308 of 22 December 2017.
52. In case of business relationships or transactions with politically exposed persons, their family members or persons associated with politically exposed persons, the reporting entities, in addition to the enhaced measures provided for in paragraph (5) to (7), shall apply the following measures
52.1. Developing and implementing appropriate risk management systems, including risk based procedures, to determine whether a customer, potential customer or the actual beneficiary of a customer is a politically exposed person;
52.2. Obtaining the approval of a person with senior management positions in establishing or continuing business relationships with such customer;
52.3. Adopting appropriate measures to determine the source of the goods involved in the business relationship or the transaction with such customers;
52.4. Performing increased and continuous monitoring of the business relationship if the customer is permanent.
53. In the case of activities, transactions or business relationships with politically exposed persons, family members of politically exposed persons and persons associated with politically exposed persons, the agent applies the provisions of the Guidance on the identification and monitoring of politically exposed persons approved by the Order of the OPCML Director no. 17 of 08 June 2018.

Chapter X
APPLICATION OF INSURANCE MEASURES

54. The Agent shall refrain from executing any operations and transactions in goods, including in financial assets, for up to 5 business days, once it gained pertinent suspicions of money laundering or related offenses, terrorist financing, or the proliferation of weapons of mass destruction, whether these are at the stage of preparation, attempt, are in process or have been already completed.
55. The Agent shall apply the provisions specified under item 54 at the request of the Office for the Prevention and Fight against Money Laundering or on its own initiative. When applying the provisions of item 54 on its own initiative. The Agent shall inform immediately, but not later than within 24 hours, the Office for the Prevention and Fight against Money Laundering of the decision taken.
56. When applying the provisions of item 54, the Agent, where applicable, shall ask the customer to provide additional data and information, including any confirmatory documents for the transactions conducted, in order to apply proper CDD measures and, in particular, to understand the purpose and the nature of the business relationship, as well as the source of the transacted assets.
57. The measures applied according to the provisions of item 42 shall cease ex officio based on the written permission and confirmation of the Office for the Prevention and Fight against Money Laundering. In the event that the suspected nature of the goods and / or transaction can not be established with certainty, including for the purposes of understanding the purpose and nature of the business relationship, the agent applies enhanced precaution measures.

Chapter X
ACTIVITY AND TRANSACTION REPORTING

58. The Agent commits to inform the Office for the Prevention and Fight against Money Laundering of:

1) any suspicious goods, activities or transactions suspicious to be related to money laundering, to associated offences and to terrorism financing that are in course of preparation, attempting, accomplishment, or are already performed – immediately or, latest, within 24 hours after identification of the action or circumstances that raise suspicions;

2) any cash transactions or bank operations, whether they are carried out in a single transaction with value exceeding 200000 MDL (or its equivalent) or through a series of cash transactions that appear to be linked - within 10 calendar days;

3) any transactions conducted through bank transfer with a value exceeding 500000 MDL (or equivalent) - not later than the 15th of the month following the reporting month;

59. The Agent shall have in place:

1) clear procedures, developed in compliance with the provisions of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing, which were made known to the entire staff and which provide for the reporting by personnel of all suspicious assets, any activities or transactions that raise suspicions of money laundering, any related offence or terrorist financing;

2) systems including software that allows identification and reporting of the activities and transactions referred to in point 85 as required and in the form established by the Office for Preventing and Fight against Money Laundering.

Chapter XI
DATA STORAGE

60. The Agent shall retain all records and information on customers and beneficial owners, collected for CDD purposes, including copies of identification documents, archive of primary documents, business correspondence, the results of researches conducted to identify any complex or unusual transactions, throughout the entire period of its business relationship with a customer and for a period of 5 years after its termination or after the date of each occasional transaction and transfer of funds, and, subsequently, for up to 5 years in electronic format.

61. The procedures of records and information storage shall include at least the following, as appropriate:

1) keeping a register of all customers and identified beneficial owners, which shall contain at least: the full name of the customer; IDNO / IDNP;

2) keeping all primary documents, including business correspondence;

3) keeping files containing records regarding the identification and verification conducted on customers and beneficial owners; files containing records of the monitored customer transaction and the transaction supporting documents;

4) keeping records of all conducted transactions and related monitoring protocols, including for complex and unusual transactions;

5) archiving information on conducted transactions and related business correspondence in IT systems and ensuring that the archived data are safe and quickly accessible for operational purposes.

62. The Agent shall ensure that any document and information obtained as a result of the customer (beneficial owner) identification and verification procedures, any data related to transaction monitoring, including transaction supporting documents, are available to the Office for the Prevention and Fight against Money Laundering, upon request. Based on the request of the competent authorities, in accordance with item 9 sec. (2) of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing, the record storage period established for the information related to customers and their transactions may be extended for a period specified in the request but not more than 5 years.

Chapter XII
INTERNAL CONTROL SYSTEM REQUIREMENTS

63. The Agents will develop and implement internal control policies and procedures to effectively mitigate and manage the risks of money laundering and terrorist financing identified in their own field of activity, as well as directly in the activities of Agents.
64. Internal control policies and procedures must be proportionate to the risk of money laundering and terrorist financing, as well as the specificity of the activities and the size of the agent.
65. The Agents approve their own programs for the prevention and combating of money laundering and terrorist financing, including the recommendations and normative acts approved by the OPCML.
66. Internal control procedures will include at least the following:
66.1. Policies, methods, practices, written procedures, internal control measures and strict rules for preventing money laundering and terrorist financing, including customer precautions, identification of complex and unusual transactions, reporting, risk assessment and risk management procedures and other relevant measures in the field;
66.2. The names of the persons, including senior officials, responsible for ensuring compliance of policies and procedures with legal requirements on preventing and combating money laundering and terrorist financing;
66.3. Measures to promote ethical and professional standards in the supervised sector and to prevent the use of the reporting entity, intentionally or otherwise, by organized criminal groups or their associates;
66.4. A continuous training program for employees, selection of staff based on the high professionalism criterion for their employment;
66.5. Conduct independent audit to test compliance of the reporting entity with policies, internal controls and procedures.
67. Agents designate the persons entrusted with the enforcement of Law no. 308 of 22 December 2017, including senior management positions whose name is communicated within 5 working days to the OPCML, together with the nature and limits of their responsibilities. The indicated persons as well as other responsible employees must have access to the results of the CDD measures, including identification data and transactions and activities, and other relevant information required. If the person in charge of ensuring compliance with policies and procedures with legal requirements on preventing and combating money laundering and terrorist financing has not been appointed, the responsibilities in the field are taken over by the leader, and in the absence thereof by the person who replaces it.

Chapter XIII
CERINȚE PRIVIND APLICAREA MĂSURILOR RESTRICTIVE INTERNAȚIONALE

68. The Agent will be required to verify whether his clients and their beneficial owners are included in the lists of persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction referred to in paragraph 73.
69. The Agent shall immediately apply restrictive measures to assets, including those obtained from or generated by assets owned, held or controlled, directly or indirectly, by persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, and by legal persons who make part of or are controlled, directly or indirectly, by such persons, groups and entities.
70. The restrictive measures provided for in par. (69) are binding, apply immediately and remain indefinite. This is only the date indicated in the decision on the lifting of the restrictive measure, communicated by the OPCML.
71. The Agents do not establish business relationships with persons, groups or entities involved in terrorist activities and the proliferation of weapons of mass destruction included in the list referred to

in paragraph (73). For the refusal to establish business relationships with them, the reporting entities shall promptly inform the OPCML, within 24 hours at the latest, of all data held in relation to this case.
72. For the application of restrictive measures under par. (69), the Agent shall develop internal rules and procedures that shall include at least the following elements:
72.1. procedures for keeping 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), in compliance with the provisions of the Law no. 308 of 22 December 2017.
72.2. procedures for screening/detection of designated individuals or entities and of transactions/payments involving goods, applicable to prospective customers, existing customers and occasional service seekers;
72.3. competences of persons responsible for the implementation of internal rules and procedures for the application of international restrictive measures to block funds;
72.4. procedures for internal information dissemination / reporting as well as for reporting to the Office for the Prevention and Fight against Money Laundering.
73. The list of persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures shall include:
73.1. The United Nations Security Council's list of persons, groups and entities involved in terrorist activities;
73.2. The United Nations Security Council's list of persons, groups and entities involved in proliferation of weapons of mass destruction;
73.3. The European Union's list of persons, groups and entities involved in terrorist activities;
73.4. The Information and Security Service's supplementary list of persons, groups and entities involved in terrorist activities.
74. The Information and Security Service elaborates, updates and publishes in the Official Monitor of the Republic of Moldova the consolidated list of persons, groups and entities that includes all the categories of the lists mentioned in par. (73.1)-(73.4).
75. The Agents permanently monitor the official web pages of the United Nations, the European Union and the Information and Security Service to ensure direct application and immediate legal effect of the lists mentioned in par. (73.1)-per(73.4).