RS Official Gazette, Nos 13/2018, 103/2018, 57/2019, 137/2020 and 49/2021

Pursuant to Article 6, paragraph 1, Article 38, paragraph 1, Article 39, Section 5) and Article 114 of the Law on the Prevention of Money Laundering and Terrorism Financing (RS Official Gazette, No 113/2017) and Article 15, paragraph 1 of the Law on the National Bank of Serbia (RS Official Gazette, Nos 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015 and 40/2015 – decision of the Constitutional Court), the Executive Board of the National Bank of Serbia issues the following

DECISION
ON GUIDELINES FOR THE APPLICATION OF THE PROVISIONS OF THE LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR OBLIGORS SUPERVISED BY THE NATIONAL BANK OF SERBIA

1. The Guidelines for the Application of the Provisions of the Law on the Prevention of Money Laundering and Terrorism Financing for Obligors Supervised by the National Bank of Serbia are hereby issued and make an integral part of this Decision.

2. The obligors referred to in Section 1 of this Decision shall harmonise their internal acts with the Guidelines referred to in that Section by no later than 25 March 2018.

3. As of the date of the beginning of application of this Decision, the Decision on the Guidelines for Assessing the Risk of Money Laundering and Terrorism Financing (RS Official Gazette, Nos 46/2009 and 104/2009) and the Decision on Minimum Contents of the “Know Your Client” Procedure (RS Official Gazette, No 46/2009) shall cease to be valid.

4. This Decision comes into effect on the eighth day following its publication in the Official Gazette of the Republic of Serbia and applies as of 1 April 2018.

NBS Executive Board No 47
13 February 2018

Belgrade

Chairperson
of the Executive Board of the
National Bank of Serbia
Governor
National Bank of Serbia

Jorgovanka Tabaković, PhD

GUIDELINES FOR THE APPLICATION OF THE PROVISIONS OF THE LAW ON THE PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING FOR OBLIGORS SUPERVISED BY THE NATIONAL BANK OF SERBIA

1. These Guidelines regulate the manner in which an obligor supervised by the National Bank of Serbia carries out an analysis of the money laundering and terrorism financing risk, the procedure to determine whether the customer or the beneficial owner of the customer is an official, as well as the manner of applying other provisions of the law regulating the prevention money laundering and terrorism financing (hereinafter: the Law).

The obligor supervised by the National Bank of Serbia (hereinafter: the obligor) shall include: a bank, voluntary pension fund management company, financial lessor, insurance undertaking with a licence to perform life insurance business, insurance brokerage undertaking when it engages in life insurance brokerage, insurance agency undertaking and insurance agent with a licence to perform life insurance business – except for agency undertakings and insurance agents for whose work the responsibility shall be borne by the insurance undertaking in accordance with law, an electronic money institution, payment institution, public postal operator headquartered in the Republic of Serbia, incorporated in accordance with the law governing postal services and providing payment services in accordance with the law governing the provision of payment services, a digital asset service provider in the part of operation concerning virtual currencies (hereinafter: a virtual currency service provider).

The General Part of these Guidelines shall be applied by all obligors, while the Special Part shall be applied by those obligors that it relates to, taking into account specific circumstances concerning the product risk, customer risk, risk of the manner of establishing and carrying out a business relationship and geographic risk related only to such obligors.

GENERAL PART

2. The money laundering and terrorism financing risk is the risk of adverse effects on the financial result, capital or reputation of the obligor, due to the use of the obligor (direct or indirect use of a business relationship, transaction, service or product of the obligor) for the purpose of money laundering and/or terrorism financing.

The money laundering and terrorism financing risk arises in particular as a result of the failure to harmonise the obligor’s business with law, regulations and internal acts regulating the prevention of money laundering and terrorism financing, or as a result of the mutual incompatibility of internal acts regulating the behaviour of the obligor and its employees in relation to the prevention of money laundering and terrorism financing.

3. The management of the money laundering and terrorism financing risk shall include in particular:

– identification and assessment of the money laundering and terrorism financing risk in relation to the overall business of the obligor;
– adoption and implementation of internal acts for the timely and comprehensive identification, assessment, measurement, monitoring, control and mitigation of the money laundering and terrorism financing risk and reporting on that risk;
– establishment of an appropriate internal organisation and/or organisational structure of the obligor;
– continuous monitoring and supervision of this risk.

1. Identification and assessment of the money laundering and terrorism financing risk

Analysis of the money laundering and terrorism financing risk

4. The obligor shall develop and regularly update the analysis of the money laundering and terrorism financing risk (hereinafter: risk analysis) in accordance with the Law, these Guidelines and the assessment of the money laundering and terrorism financing risk developed at the national level. The risk analysis must be commensurate with the nature and scope of business, as well as the size of the obligor, and must also take into account the basic types of the risk (customer, geographic, transaction and product/service) and other types of the risk the obligor has identified based on the specific character of its business.

The obligor's approach to the risk analysis is based on the analysis of the money laundering and terrorism financing risk in relation to the overall operations of the obligor, as well as on the analysis of that risk for each group or type of customer, business relationship, product/service provided or transaction.

In the process of development of the risk analysis, the obligor shall assess the probability that its business will be used for the purpose of money laundering or terrorism financing. The risk analysis in relation to the overall operations of the obligor is aimed at identifying the exposure of the obligor to the money laundering and terrorism financing risk and segments of operations of obligors that should be given priority in implementing activities for efficient management of this type of risk.

The obligor shall identify each segment of its business (sources of risk), i.e. the type, scope and complexity of its business, all existing and new products/services, processes, activities and procedures in order to assess in

which business segment a threat from money laundering and terrorism financing may arise (probability of risk occurrence). After that, the obligor must adequately assess the adverse consequences that could arise from this source of risks, as well as their potential effect on the achievement of the business objectives (financial loss as a result of committing a criminal offence or imposed fines, negative consequences on the reputation of the obligor, etc.).

Based on the estimated likelihood of risk occurrence and estimated adverse consequences, the obligor shall determine the level of exposure to the money laundering and terrorism financing risk for each segment of its business (e.g. the size of the business network, because the number of branches of the business network can affect a higher likelihood of risk occurrence due to aggravated due diligence, which, as a consequence, may result in insufficient information about the customer, and therefore the level of risk is greater; entrusting the activities related to customer due diligence actions and measures to other parties can affect the likelihood of risk occurrence, especially if the debtor has only one branch and performs all business through these persons).

In the process of developing a risk analysis, the obligor shall also determine the characteristics of customers, products/services, transactions, ways of establishing a business relationship and location, and, by bringing into relation these specific characteristics, assess the likelihood that products/services, transactions, the way of establishing a business relationship and location will be used for the purpose of money laundering and terrorism financing, the consequences that may arise in a concrete situation, and the level of exposure to the money laundering and terrorism financing risk. The analysis of certain types of risks and their combinations is specific to each obligor, so the conclusion on the overall level of risk must be based on all relevant available data and information.

The risk analysis for each group or type of customer, business relationship, transaction, product/service that the obligor provides within its activity and the way of establishing a business relationship with the customer is aimed at determining the criteria based on which the obligor will classify a customer, business relationship, product/service or transaction into one of the risk categories in accordance with the Law. The classification of a customer into one of the risk categories shall be performed by analysing certain types of risks and their combination, depending on the specificity of each obligor. Customer due diligence actions and measures to be undertaken by the obligor in accordance with the Law (general, enhanced, simplified) will also depend on the category of risk of a customer, business relationship, product/service or transaction.

The obligor shall base the risk analysis in relation to its overall business and risk analysis aimed at classifying the customer into one of the risk categories according to all relevant information.

Risk assessment

5. The assessment of the money laundering and terrorism financing risk within the meaning of these Guidelines shall cover two phases:

- identification of the type of risk;
- risk assessment.

Identification of types of risk

6. The obligor shall identify the money laundering and terrorism financing risk to which it is exposed or will be exposed when establishing a business relationship with a customer or when performing a transaction. With this aim, the obligor shall consider all relevant types of risk, always taking into account the customer risk, geographic risk, transaction risk, product/service risk and risk concerning the manner of establishing and maintaining the business relationship.

Sources of information

In identifying the money laundering and terrorism financing risk, the obligor shall use the information it obtained by conducting customer due diligence actions and measures, as well as other different sources of information, including publicly available databases.

The obligor shall always take into account the assessment of the money laundering and terrorism financing risk developed at the national level, as well as other declarations and warnings issued by state authorities and authorities in charge of supervising the implementation of the Law.

The obligor may also consider other sources of information (own experience, information from civil society organisations – such as country reports, information from international standard-setting bodies, such as mutual evaluation reports or non-binding blacklists, statistics, information from the media, information from business units and subordinate companies of the legal person in the majority ownership of the obligor and members of the financial group within the meaning of Section 19a, paragraph 2 hereof, etc.).

Customer risk

7. In order to identify the customer risk, including the beneficial owner of the customer, the obligor shall consider the risks associated with the manner

of operation and type of professional activity, reputation, ownership and organisational structure, as well as the behaviour of the customer in relation to a business relationship or transaction.

In relation to the activity and/or profession of the customer, i.e. of the beneficial owner of the customer, the high money laundering and terrorism financing risk may be indicated by the following circumstances:

– the customer or the beneficial owner of the customer performs activities in the field of construction, arms trade and arms production, trade in high-value goods (such as precious metals, precious stones, cars, artwork, etc.);

– the customer or the beneficial owner of the customer performs activities featuring large turnover and cash payments (such as restaurants, petrol stations, exchange offices, casinos, shops, car washers, flower shops, goods and passenger carriers, etc.);

– the customer is a foreign bank or other similar financial institution of a state that does not apply standards in the field of the prevention of money laundering and terrorism financing;

– the customer or the beneficial owner of the customer is an official of the Republic of Serbia, another state or international organisation, or has been in the last four years, or a person who is a member of the immediate family of that official or his close associate (in this case, the obligor always conducts enhanced customer due diligence actions and measures in accordance with the Law);

– the customer, beneficial owner of the customer, subsidiary company of the customer or the controlling company of the customer is the person providing financial services, and/or digital asset services, for whose establishment and/or provision of those services, in accordance with regulations of the country in which it is established, it is not necessary to obtain the permission of the relevant supervisory body, and/or which is not subject to supervision over the application of actions and measures in the field of the prevention of money laundering and terrorism financing;

– the customer, beneficial owner of the customer, subsidiary company of the customer or the controlling company of the customer is founded by issuing bearer securities or by issuing digital assets which directly or indirectly enable the concealment of the identity of buyers/investors;

– the customer is a private investment fund.

In relation to the reputation of the customer, i.e. of the beneficial owner of the customer, the high money laundering and terrorism financing risk may be indicated by the following circumstances:

– information from reliable and relevant sources on the relationship of the customer or the beneficial owner of the customer with criminal offences of money laundering and terrorism financing;

– the customer, beneficial owner of the customer, representative or proxy of the customer is on the list of persons against whom sanctions, embargoes or other similar measures of the United Nations, Council of Europe or other international organisation are in force, or the customer or beneficial owner of the customer are persons closely related by personal or business relations to the persons on the list;

– there is knowledge that the customer or the beneficial owner of the customer was reported for suspicious transactions;

– the Administration for the Prevention of Money Laundering (hereinafter: the Administration) has requested over the past three years from the obligor in relation to that customer or the beneficial owner of the customer to submit data on persons and transactions for which there are grounds to suspect money laundering or terrorism financing;

− in the past three years, the Administration has issued a written order to the obligor, in relation to the customer, to temporarily suspend a transaction, or to temporarily suspend the access to the safe;

− in the past three years, the Administration has issued a written order to the obligor for monitoring the operations of that customer (all transactions or activities of that person carried out with the obligor).

In relation to the ownership or organisational structure of the customer or beneficial owner of the customer, the high money laundering and terrorism financing risk may be indicated by the following circumstances:

– due to the organisational structure, the legal form or complex and unclear proprietary relationships, it is difficult to determine the identity of the beneficial owners of the customer or persons who manage them;

– there are no grounded reasons for changing the ownership structure of the customer;

– the customer or the beneficial owner of the customer is a non-profit organisation that can be used for the purpose of financing terrorism;

– the customer or the beneficial owner of the customer is a person with a disproportionately small number of employees in relation to the volume of business and/or a person without its own infrastructure, business premises, etc.;

– the customer or the beneficial owner of the customer is an offshore legal person or a person under foreign law.

In relation to the behaviour of the customer, and/or beneficial owner of the customer regarding the business relationship or transaction, the high money laundering and terrorism financing risk may be indicated by the following circumstances:

– the customer does not submit all necessary evidence of identity, for which there are no objective reasons or there is suspicion as to the identity of the customer or beneficial owner of the customer;

– there are indications that the customer avoids establishing a business relationship with the obligor (e.g. requires the execution of one or several transactions, although the establishment of a business relationship would be economically more logical);

– business activity or transactions of the customer are carried out under unusual circumstances;

– the customer uses products or services in the way that is not expected when a business relationship is established;

– the customer is a non-resident and services would be more adequately provided to it in another country, or there is no economic logic for the type of service requested by the customer;

– there is suspicion that the customer does not act on its own account, or that it carries out instructions from a third party;

– the customer is not physically present with the obligor in determining and checking its identity (in this case, the obligor always implements enhanced customer due diligence actions and measures in accordance with the Law).

The unusual circumstances within the meaning of paragraph 5, third indent of this Section shall include in particular:

– significant and unexpected distance between the location of the customer and the organisational unit of the obligor where the customer opens an account, establishes a business relationship or performs a transaction;

– frequent and unexpected establishment, without economic justification, business relationships of a similar kind with several banks, such as opening accounts in several banks, signing multiple membership contracts in a voluntary pension fund in a short period of time (regardless of whether they are concluded with one or several management companies) or several financial leasing agreements with several financial lessors, etc.;

− frequent and unexpected transfers, without any clear economic reason, of funds from an account with one bank to accounts with another bank, especially if banks are located in different locations, except in the case of multinational companies operating on multiple accounts, and frequent transfers of funds from one voluntary pension fund to another and frequent transfers of digital assets from one address of those assets to another;

− insisting on payment of a higher percentage of participation in the purchase of a lease asset than the one prescribed, which, in accordance with the general conditions of its business, the financial lessor requires during the conclusion of the financial leasing agreement;

− amendment of a membership contract in a voluntary pension fund for the purpose of an unusually high increase in the amount of the contribution;

− membership in a voluntary pension fund, i.e. payments of funds to the individual account of persons when due to age, there is no possibility of a significant period of accumulation,

− termination of the contract on pension plans and membership contracts in the voluntary pension fund shortly after their conclusion, especially in the case of high contributions;

− request that the funds accumulated in the individual account of a member of the voluntary pension fund be paid to the current account of a third person or to the account of a person in the territory of a country in which the standards in the field of money laundering and terrorism financing prevention are not applied;

– the conclusion of a large number of policies in various insurance undertakings, especially in the short term, frequent changes and cancellations of contracts, acceptance of unfavourable conditions in the insurance contract, insisting on secrecy of the transaction, etc.

The obligor shall take into account that certain circumstances in this Section will not be apparent at the very beginning of the establishment of a business relationship, and/or performance of a single transaction.

When assessing customer risk, the obligor shall use the results of the ML/TF risk assessment developed at the national level in the section pertaining to the activity and/or profession of the customer or to the ways in which economic entities – parties involved in money laundering can get organised.

Geographic risk

8. In order to identify the geographic risk, the obligor shall consider in particular the risk in relation to the country in which the customer or the beneficial owner of the customer is headquartered, performs activity or with which it is related in a relevant manner.

The importance of geographic risk factors often depends on the nature and purpose of the business relationship, and the obligor shall take into account the following:

− if the assets used in a business relationship are generated abroad, the obligor must determine the anti-money laundering and terrorism financing system established in that country;

– if the assets are received from a state where it is known that terrorist organisations operate or are sent to such state, the obligor must consider to what extent it could cause suspicion in relation to money laundering and terrorism financing, based on the information of the obligor about the purpose and nature of the business relationship;

– if the customer is a financial institution of another state or a digital asset service provider headquartered in another state, the obligor shall pay special attention to the adequacy and effectiveness of the system of that

country against money laundering and terrorism financing, particularly in relation to those institutions, and/or service providers;

– if the customer is a trust or a person under foreign law, the obligor shall, if applicable, consider the extent to which the country in which the customer or the beneficial owner of the customer is headquartered is aligned with international tax transparency standards.

In order to identify the effectiveness of the system against money laundering and terrorism financing of the state, the obligor must consider:

- whether the state has been identified to have strategic deficiencies in the system of the prevention of money laundering and terrorism financing;

– whether there is information from several credible and reliable sources on the quality of the anti-money laundering and terrorism financing system of that country, including information on the quality and effectiveness of the application of regulations and supervision of implementation (e.g. joint reports of relevant international bodies).

In order to identify the level of risk of terrorism financing for a particular country, the obligor must consider the following factors:

– whether there is information from bodies responsible for law enforcement or credible and reliable sources that indicate that the state finances or supports the activities of terrorist organisations or is known that terrorist organisations operate in that state;

– whether the United Nations, Council of Europe, OFAC or other international organisations have imposed sanctions, embargoes or similar measures against such state.

In identifying the level of tax transparency and compliance, the obligor shall take particular consideration of whether there is information from several credible and reliable sources that the state is considered to be in line with international standards of tax transparency. In assessing compliance with international standards of tax transparency, the obligor may use as the sources of information the reports of the Global Forum on Transparency and Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development, the EU list of non-cooperative jurisdictions adopted by the European Commission, estimates of the International Monetary Fund etc.

In order to identify the risks associated with predicate criminal offences related to money laundering, the obligor shall consider in particular the following circumstances:

- whether there is information from reliable and credible sources about the number of predicate criminal offences related to money laundering (e.g. criminal offences related to corruption, organised crime, tax evasion,

fraud and assets or other criminal offences for which the assessment of the ML/TF risk developed at the national level showed that these are criminal offences of a high or medium level of threat);

− whether there is information from several reliable and credible sources about the ability of the judiciary of a particular state to effectively process the acts referred to in the first indent of this paragraph.

Risk assessment also depends on the location of business of the obligor and/or its organisational units (e.g. for obligors operating in the area visited by many tourists, the risk is higher than for those operating in a rural area, where all customers know each other personally). Increased risks are possible especially at border crossings and airports, where there is a large concentration of foreigners or a large number of transactions with foreigners (e.g. fairs), at places where there is a high number of asylum seekers or refugees from countries identified as countries with strategic deficiencies in the system of the prevention of money laundering and terrorism financing or from countries in respect of which there is information from law enforcement authorities or credible and reliable sources which indicate that these countries finance or support the activities of terrorist organisations or it is known that terrorist organisations are active in those countries or that there is a high degree of corruption and crime in those countries etc., and countries where a disproportionately high number of persons providing virtual currency and/or digital asset services, and/or virtual currency and/or digital asset trading platforms operate, particularly in countries without any limitations on the performance of these activities.

An increased money laundering and terrorism financing risk also exists in transactions carried out with offshore destinations.

Customers from the region may be less risky than parties outside the region, i.e. customers from countries with which there are no business relationships or business relationships are present to a marginal degree.

Risk of product/service and transaction

9. In order to identify the risk of a product/service or a transaction, the obligor shall consider the risk that relates to: 1) the level of transparency of the product/service and/or transaction; 2) the complexity of the product/service and/or transaction; 3) the value of the product/service and/or transaction.

When considering the level of transparency of a product/service or transaction, the obligor shall particularly assess the extent to which the product or service or transaction enables or facilitates the anonymity of the customer, beneficial owner of the customer or the ownership structure (e.g. bearer shares, offshore legal entities, fiduciary deposits, virtual currencies, legal entities whose organisational structure is such that it allows them a high

degree of anonymity and transactions with fictitious companies), to what extent there is a possibility that a third person that is not part of the business relationship gives instructions with respect to this relationship (e.g. specific cases of correspondent banking).

When considering the complexity of a product/service or transaction, the obligor shall particularly assess the extent to which a transaction is complex and whether several parties or several different legal systems are involved in the relationship (e.g. in certain cases of financing trade), whether it is a direct transaction (e.g. whether regular payments to the pension fund are made), to what extent it is allowed that products or services are paid by third parties or excessive payments when this is unusual, if payment by a third party is expected and whether the obligor knows the identity of that person (e.g. whether it is a budget beneficiary or a guarantor), whether products or services are funded by transferring funds from a customer's account with another financial institution to which standards in the field of the prevention of money laundering and terrorism financing are applied which are at least at the level of European Union standards, whether the obligor understands the risks related to new products, especially those that involve the use of new technological achievements or payment methods.

When considering the value of products/services or transactions, the obligor shall in particular assess the extent to which products or services are provided primarily in cash, as is the case with individual payment services and certain current accounts, as well as with the provision of virtual currency services by means of crypto ATMs, to what extent products or services facilitate or encourage high-value transactions, whether there are limits to the value of a transaction or premium level in order to minimise the possibility of abuse of a product or service for the purpose of money laundering or terrorism financing.

In identifying and assessing the money laundering and terrorism financing risk, the obligor must include in a timely manner the money laundering and terrorism financing risk arising from the introduction of new products/services and activities related to the processes and systems of the obligor (hereinafter: a new product). The new product shall include significantly changed products, services and activities (hereinafter: significantly changed product).

The obligor, by means of appropriate internal acts, shall determine what it considers to be new products (including substantially altered products) and shall regulate the process of deciding on the introduction of these products.

Before introducing a new product, the obligor must perform an analysis:

– of the money laundering and terrorism financing risk that may occur as a result of such introduction;

– of the impact of such introduction on the exposure of the obligor to the money laundering and terrorism financing risk;

– of the impact of this introduction on the ability to adequately manage the money laundering and terrorism financing risk.

High-risk products/services may be:

– services that are new in the market, i.e. that have not been previously offered in the financial sector, which must be particularly monitored to determine the actual degree of risk;

– private banking, i.e. provision of private banking services and the management of funds of foreign nationals, which may be particularly risky as a customer with a significant amount of money is taken care of by one officer or a smaller group of officers who may be instructed by their superiors to accept everything that the customer requests, which the customer may abuse;

– electronic banking in cases envisaged by the obligor's own procedure;

– electronic issuance of orders for trade in securities in cases which the obligor foresees in its procedure;

– providing to persons with whom the business relationship has not been previously established, within the meaning of the Law, those types of services for which the employees in the obligor assessed on the basis of their experience that they bear a high degree of risk (one-off transactions, e.g. remittances);

– provision of services outside the business premises of a bank (e.g. approval of consumer loans in a point of sale of the merchant), insurance undertaking or other entity in the financial sector;

– providing services of opening the so-called joint accounts to which funds from different sources and from different customers are transferred and deposited in one account opened in one name;

– repurchase or payment of cheques or any other instrument or bearer securities;

– transferable bearer or fictitious recipient securities, instruments that provide the ability of endorsement without limitation or otherwise give the possibility of transfer after their surrender or other instruments that have been signed, but the name of the money recipient is not stated;

– the product enables the payment of a third person whose identity is not known, and such payments are not expected (e.g. in the case of housing loans);

– new products and new business practices, including new ways of establishing a business relationship, and the use of new technologies or technologies in development, both for existing and new products, including the use of smart contracts;

– financial derivatives and other financial instruments traded via electronic platforms when it is not possible to reliably determine that they are licensed, and/or registered by the authority responsible for the provision of those services;

– the granting of a loan secured by mortgage if the immovable property is located in another country, especially if it is difficult to determine whether the customer has the ownership right to the mortgaged asset or it is difficult to determine the identity of the beneficial owner of real estate.

High-risk transactions may be:

– transactions that significantly differ from the standard behaviour of the customer;

– transactions that do not have economic justification (e.g. frequent trading in securities when purchase is performed by placing cash in dedicated accounts, and soon afterwards they are sold below the price – the so-called trading in securities with a planned loss, unexpected loan repayment before the deadline or in the short period from the date of loan approval, unexpected repayment of the lease asset before the deadline or within a short period from the date of conclusion of the financial leasing agreement, withdrawal of funds from the individual account of a voluntary pension fund member in the short period after their payment);

– transactions conducted in the manner that avoids standard and usual methods of control (transactions in the amounts slightly lower than the amounts prescribed as limits below which the measures prescribed by the Law are not taken);

– complex transactions involving multiple participants without clear economic determination, several interconnected transactions that are performed in a short period or in several intervals consecutively in the amount below the limit for reporting to the Administration;

– loans to legal entities, in particular the loans of founders from abroad to a legal person in the country;

– transactions whose true grounds and reasons for implementation are obviously concealed by the customer;

– payment for consulting, management and marketing services, as well as other services for which there is no determinable value or price in the market;

– transactions for which the customer refuses to submit the documentation;

– transactions where the documentation does not correspond to the way the transaction is carried out;

– transactions in which the source of funds is not clear or their relationship with the customer’s business cannot be determined;

– transactions in which a disproportionately high amount of deposits (e.g. 100%) is deposited as loan collateral;

– the announced block trading in shares at prices that are clearly lower than market prices, when unknown or newly emerging companies appear as buyers, especially companies registered in offshore destinations;

– trading in shares on the stock exchange and over-the-counter, which were subject to pledge based on loans granted to holders of shares – the so-called “processing of shares through the stock market”;

– transactions of the payment of goods and services to partners of the customer that originate from offshore destinations, and it is clearly seen from the documentation that the goods originate from countries of the region;

– transactions of the payment of goods or services in countries that do not customarily produce the goods being paid or perform such type of service (e.g. import bananas from Siberia);

– frequency of transactions based on advance payment of import of goods or performance of services where it is not certain that goods will actually be imported or services performed;

– transactions intended for persons against whom measures of the United Nations or European Union are in force, as well as transactions performed by the customer in the name and on behalf of those persons;

– payment of funds from the customer’s account, i.e. the transfer of funds to the account of the customer, which is different from the account that the customer stated during identification, or through which it normally operates or operated (especially in the case of a cross-border transaction);

– transactions for persons that are residents or are headquartered in a country that is an offshore state or a tax haven;

– transactions for non-profit organisations headquartered in an offshore state or a tax haven, or a non-member state of the European Union;

– an unusually large volume or amount of transactions.

When assessing the risk of a particular transaction, the obligor shall also take into account the analysis and the overview of the ways money laundering is done, presented in the ML/TF risk assessment developed at the national level.

Risk related to the manner in which a business relationship is established and carried out

10. In order to assess the risks related to the manner a business relationship is established or a transaction performed, the obligor shall particularly assess whether the customer is physically present in determining and checking the identity, and in case he is not physically present – to what extent it is certain that that the customer will not expose the obligor to an increased money laundering and terrorism financing risk.

If determination and verification of the identity of a customer is performed through a third party, the obligor shall assess in advance whether

such person is a financial institution, as well as what it has undertaken to ensure that the third party takes customer due diligence actions and measures and is subject to supervision of the implementation of obligations in relation to the prevention of money laundering and terrorism financing, and that immediately upon the request of the obligor, it will submit relevant copies of data on identification and verification of the customer. The obligor shall assess the reliability of the customer due diligence actions and measures conducted by a third party.

If, on behalf of the customer that is a natural person, a business relationship is established by a legal representative or proxy, or if, on behalf of a customer that is a legal person or a person under foreign law, a business relationship is established by a representative, proxy or procurator – it shall be analysed how the obligor can be convinced that this will be the person to collect sufficient information based on which the obligor will be informed about the customer and the level of risks related to the business relationship.

If the obligor entrusted the execution of some customer due diligence actions and measures to another person, it shall previously determine whether that person is an obligor or other regulated entity to whom the obligations related to the prevention of money laundering and terrorism financing are applied in accordance with the Law, and whether its business is subject to effective supervision, whether there are indications that the behaviour of such person in line with regulations relating to the prevention of money laundering and terrorism financing is inadequate (e.g. whether it was punished for not respecting these regulations) and whether there is an increased money laundering and terrorism financing risk in the country where its head office is located.

In order to identify the risks related to the way in which the business relationship is established and business conducted, the obligor shall consider whether and how the business relationship takes place without the physical presence of the customer, as well as the risk associated with representatives of customers or mediators that the obligor can engage, including the nature of their relationship with the obligor.

Risk assessment

11. The obligor shall comprehensively analyse all risk factors it has identified to determine the degree of the money laundering and terrorism financing risk related to a business relationship or transaction. As part of this assessment, the obligor may decide to weight risk factors differently, depending on their individual significance.

When weighting risk factors, the obligor shall determine the relevance of various risk factors in the context of a business relationship or transaction. This often results in the fact that the obligor assigns different assessments to

different factors (e.g. the obligor can estimate that the existence of a personal relationship with a country with an increased money laundering and terrorism financing risk is less relevant, given the characteristics of the product in question).

The weight assigned to each risk factor may vary depending on the particular product or customer, as well as on individual obligors. When weighting risk factors, the obligor shall ensure that:

– not only one risk factor is unjustifiably affected by weighting;
– economic considerations and examinations relating to the profit of obligors do not affect risk assessment;

– the weighting of risk factors does not lead to the situation that no business relationship can be classified into a high-risk category;
– the risk category determined by law cannot be changed;
– if necessary, an automatically generated risk assessment can be changed.

If the obligor automatically performs an overall risk assessment for the purposes of classifying a business relationship or transaction in a particular category, while the operating system is not developed by the obligor, but is provided by a third party – the obligor must understand how this system functions, including the way in which risk factors are combined in order to achieve overall risk assessment. The obligor must be sure that the assessment reflects its understanding of the money laundering and terrorism financing risk and that it can prove it.

Based on the performed risk analysis for each group or type of customer or business relationship, the services provided by the obligor within its activity, i.e. transaction – the obligor, in accordance with the Law, shall classify the customer into one of the following risk categories:

– low-risk category of money laundering and terrorism financing,
– medium-risk category of money laundering and terrorism financing,

– high-risk category of money laundering and terrorism financing.

The obligor may also envisage additional risk categories by its internal acts.

Customer due diligence actions and measures

12. International standards and the Law allow the obligor, depending on the degree of the money laundering and terrorism financing risk, to carry out

three types of customer due diligence actions and measures – general, simplified and enhanced. These measures should contribute to better understanding of risks of the obligor based on a business relationship and transaction.

General customer due diligence actions and measures shall include the determination and verification of the identity of the customer and beneficial owner of the customer, obtaining and assessing information about the intent and purpose of the business relationship or transaction of the customer and regular monitoring of the customer's operations, in the cases and in the manner prescribed by the Law. General actions and measures shall be applied to medium-risk customers.

Simplified customer due diligence actions and measures shall be implemented in cases and in the manner prescribed by the Law and shall be applied to customers with a low money laundering and terrorism financing risk. The obligor shall implement an adequate level of monitoring of business operations of the customer so as to be able to detect unusual and suspicious transactions. When there is suspicion of money laundering or terrorism financing in relation to the customer or transaction to which these actions and measures were applied, the obligor must carry out an additional assessment and possibly apply enhanced actions and measures (e.g. if the customer is a domestic company whose securities are admitted to the stock exchange, and during the establishment of a business relationship, it is classified into a low risk and simplified measures are applied, and the obligor suspects, in respect of a transaction of that customer, that it is a matter of money laundering or terrorism financing – such suspicion entails an obligation to apply enhanced actions and measures to that customer).

Enhanced customer due diligence actions and measures shall include, in addition to general customer due diligence actions and measures, additional actions and measures to be taken by the obligor in the cases prescribed by the Law and other cases, when it assesses that due to the nature of the business relationship, manner of execution of transaction, type of transaction, ownership structure of the customer, or other circumstances related to the customer or transaction, there is or might be a high level of the money laundering and terrorism financing risk. By its internal act, the obligor shall define which enhanced measures it will undertake in each particular case and to what extent.

The nature of additional measures to be implemented by the obligor when it classifies a customer as high-risk based on its own risk assessment, shall depend on a concrete situation (e.g. if the customer is assessed as high-risk due to its ownership structure, the obligor may include a provision in its procedures specifying the need for additional data provision and further verification of the documents submitted).

Risk assessment shall be conducted not only when establishing cooperation with the customer but also during cooperation in the frequency and at the intensity corresponding to the estimated risk and changed circumstances concerning the customer (due diligence), which means that one and the same customer may initially be classified as high-risk whereas later on, during the business relationship, the obligor may decide to apply general or simplified customer due diligence actions and measures and vice versa. This does not apply to cases that are classified as high-risk by the Law and to which enhanced customer due diligence actions and measures must be applied as specified in the Law.

If an employee in an obligor that is in direct contact with the customer suspects that there is a money laundering and terrorism financing risk in relation to that customer or its transaction, such employee must make an internal written report thereon and, within the deadline and in the manner determined by the internal act of that obligor, submit it to the person in charge exclusively for the fulfilment of obligations under the Law and other regulations governing the prevention of money laundering and terrorism financing (hereinafter: compliance officer). This report shall include the information on that customer and transactions that enable the compliance officer to assess whether the customer or the transaction are suspicious.

If, on the basis of the report referred to in paragraph 7 of this Section or on the basis of directly learned information on the existence of the money laundering and terrorism financing risk, the compliance officer assesses a transaction as suspicious – such officer shall act in accordance with the Law, and if he does not assess so – he must make a note on that assessment.

If the implementation of due diligence actions and measures would cause suspicion of the customer that the obligor implements actions and measures for the purpose of submitting data to the Administration, the obligor shall suspend the undertaking of such actions and measures, and make an official note thereon in writing, which it shall submit to the Administration.

Reports and notes referred to in paragraphs 8 to 10 of this Section shall be kept by the obligor for at least five years from the date of their preparation.

Central records of beneficial owners and other registers and records of beneficial owners in foreign countries

12a. In the procedure of identifying and verifying the identity of the beneficial owner of the customer in accordance with the Law, the obligor who obtains data on the beneficial owner of the customer from the records established based on a separate law governing the central records of beneficial owners or from other records or register established for those purposes in a foreign country – shall not be exempted from the obligation to

undertake actions and measures to determine the beneficial owner which it is obliged to undertake based on the assessment of the customer risk. The obligor shall undertake additional measures to verify the data recorded in such records/registers, particularly in the case of increased risk of money laundering and terrorism financing in relation to the established business relationship or in the case it assesses that there is suspicion that the person recorded in the records/register is not the beneficial owner of the customer.

In case that in the due diligence procedure the obligor determines that the beneficial owner of the customer is the person not recorded as the beneficial owner in the records/register referred to in paragraph 1 hereof – it shall act in accordance with the guidelines for the establishment of the beneficial owner of the customer and the guidelines for recording the beneficial owner of the registered entity in the central records adopted by the Administration.

If the obligor, in accordance with the guidelines referred to in paragraph 2 hereof, referred the customer to correct the recorded data on the beneficial owner within a given deadline, and the customer failed to do so within the deadline – the obligor, based on the estimated risk of the customer, shall inform the Administration thereof.

In the case referred to in Article 25, paragraph 5 of the Law, when after undertaking all actions prescribed by that Article, the obligor is not able to determine the beneficial owner, it shall determine the identity of one or several natural persons discharging the function of the top management in the customer, and shall assess whether the impossibility to determine the beneficial owner of the customer constitutes the grounds for suspicion concerning money laundering or terrorism financing, and whether the reasons specified by the customer as the reasons why it is not able to determine the identity of the beneficial owner are credible and justified.

When determining one or several natural persons discharging the function of the top management in the customer referred to in paragraph 4 hereof as the beneficial owner of the customer, the obligor shall also take into account who of these persons has the ultimate and comprehensive control of the operations of the customer and who adopts the binding decisions on behalf of the customer.

Correspondent relationship with banks and other similar institutions from foreign countries

13. In establishing a correspondent relationship with banks and other similar institutions of foreign states, the obligor shall, in addition to customer due diligence actions and measures in accordance with the risk assessment, obtain additional data, information and documentation prescribed by the Law.

The obligor cannot establish a correspondent relationship with a bank or other similar institution of a foreign country operating as a quasi-bank, nor a business relationship based on which such institution may use the account with the obligor by enabling its customers to directly use this account.

The obligor must document the processes of decision-making and implementation of enhanced actions and measures prescribed by the Law.

New technological achievements and services

14. The obligor must recognise and understand the risks associated with a new or innovative product or service, especially when it involves the use of new technologies or payment methods. The new products and new business practices, including new modes of product delivery and the use of new developing technologies (both for new and existing products), especially if there is no clear understanding in respect of them, may contribute to an increased money laundering and terrorism financing risk.

In applying new technological achievements and new products or services, in accordance with the Law, the obligor shall, in addition to general customer due diligence actions and measures, apply additional measures that reduce the risks and manage the money laundering and terrorism financing risk (e.g. more frequent monitoring of the customer for the purpose of determining whether its business is expected, bearing in mind knowledge of the customer, its income, etc.).

Official

15. The obligor shall determine the procedure establishing whether the customer or beneficial owner of the customer is an official, a member of the close family of the official or his close associate.

Customer due diligence actions and measures shall be the key source of information about whether the customer is an official (e.g. information on the basic occupation or employment of the customer). The obligor shall also use other sources of information that may be useful to identify the official.

To obtain relevant information for identification of an official, the obligor shall undertake the following activities:

– obtain a written statement of the customer on whether it is an official, a member of the close family of the official or his close associate.

– use electronic commercial databases containing lists of officials (e.g. World-Check, Factiva, LexisNexis);

– search publicly available data and information (e.g. the register of officials in the Anti-Corruption Agency or the list of holders of prominent public functions adopted by the European Commission, which contains the list of officials in member states;

– create and use an internal database of officials (e.g. larger financial groups have their own lists of officials).

The number and the sequence of activities from paragraph 3 of this Section, which the obligor undertakes, should enable the obligor to determine in a valid manner whether the customer or the beneficial owner of the customer is an official, a member of the close family of the official or his close associate.

The written statement referred to in paragraph 3, first indent of this Section shall contain the following information:

- name and surname, date and place of birth, permanent or temporary residence and personal ID number of the official establishing a business relationship or performing a transaction, and/or for whom a business relationship is established or a transaction performed, as well as the type and number of his personal document, name of the issuer, date and place of issue;
- the statement on whether a customer is an official according to the criteria set out in the Law (it is necessary to specify in the statement all cases stipulated by the Law);
- data on whether the official is a natural person performing or has performed over the past four years a high-ranking public office in the state or other state or international organisation, whether he is a member of the family of the official or his close associate;
- data on the period of performing this function;
- data on the type of public office that the official performs or has performed in the last four years;
- data on family relations, if the customer is a member of the close family of the official;
- data on the type of business cooperation, if the customer is a close associate of the official.

When establishing a business relationship or performing a transaction (in the amount of EUR 15,000 or more in the dinar equivalent, regardless of whether it is one or several interrelated transactions, in the event that a business relationship is not established) with a customer that is an official, a member of the close family of the official or his close associate, or whose beneficial owner is one of these persons – the obligor shall apply enhanced customer due diligence actions and measures against this customer as well.

Such actions and measures shall be undertaken by the obligor even when the natural person stops discharging the public function (former official) over as much time as necessary to conclude that this person did not abuse his former position, at least four years after the day of termination of the function.

The procedure referred to in paragraph 1 hereof shall be undertaken also during a business relationship with the customer, within regular monitoring of its operations. The following factors may be particularly important:

– official's country of origin (risk related to dealing with the official is higher if the official comes from the country with a high degree of corruption and crime);
– official's title, responsibility and authorisations (a higher degree of title or responsibility indicates a higher risk given a greater possibility of use and allocation of public funds);
– scope and complexity of the business relationship (a higher degree and greater complexity of the established business relationship between the official and the obligor are indicative of a higher degree of risk regarding this person);
– type of product or service offered to an official (some categories of services imply a higher risk, e.g. private banking);
– third parties doing business with the official (officials often rely on offshore companies and banks, i.e. entities located in areas or countries not applying adequate measures and standards regulating the prevention money laundering and terrorism financing).

The data and documentation obtained under the procedure from this Section shall be kept in the customer's file, within the deadline regulated by the Law.

Determination and verification of identity without the customer's physical presence

16. If in determining and verifying the identity, the customer or legal representative, and/or a person authorised to represent a legal person or a person under foreign law, is not physically present with the obligor – in accordance with the Law, the obligor shall, in addition to general customer due diligence actions and measures, apply additional measures prescribed by Article 39 of the Law, which refer to obtaining additional documents, data or information, based on which it shall verify the identity of the customer; conducting additional inspection of submitted identity documents or additional verification of customer data; ensuring that the first payment shall be carried out to the account opened by the customer with the obligor from the account

of the customer opened with the bank or a similar institution, before the execution of other transactions of the customer with the obligor; obtaining data on the reasons for the customer's absence.

In the event from paragraph 1 of this Section, the obligor shall in particular take into account the application of the provisions of Section 9 of these Guidelines.

Offshore legal person

17. In accordance with the Law, the obligor shall set out the procedure for establishing whether the customer or a legal person that appears in its ownership structure is an offshore legal person. To that end, the obligor may use the list of states which is an integral part of the rulebook governing the list of states with a preferential tax system as defined by the minister in charge of finance and the list of relevant international institutions (such as the International Monetary Fund, World Bank, etc.).

If, on the basis of the conducted procedure, it established that the customer or legal person that appears in the ownership structure of the customer is an offshore legal person, the obligor shall, in addition to general customer due diligence actions and measures, take additional measures in accordance with the Law.

Countries which do not implement international standards in the area of the prevention of money laundering and terrorism financing

18. In accordance with the Law, strategic deficiencies in the anti-money laundering and terrorism financing system of the state relate in particular to 1) the legal and institutional framework of the state, in particular the criminalisation of criminal offences of money laundering and terrorism financing, customer due diligence measures, provisions concerning the keeping of data, provisions governing the reporting of suspicious transactions, authorisations and procedures of relevant bodies of these countries in relation to money laundering and terrorism financing; 2) effectiveness of the system for combating money laundering and terrorism financing in eliminating the money laundering and terrorism financing risk.

When establishing a business relationship with a customer from the country with strategic deficiencies in the system of fighting against money laundering and terrorism financing or carrying out a transaction with that customer without an established business relationship – the obligor shall apply enhanced due diligence actions and measures prescribed by the Law.

2. Internal acts

19. In accordance with the Law, the obligor shall adopt and apply appropriate internal acts that will, in order to effectively manage the money laundering and terrorism financing risk, include all actions and measures for the prevention and detection of money laundering and terrorism financing defined by the Law, by-laws adopted based on the Law and these Guidelines. By the internal acts, the obligor must take into account the identified money laundering and terrorism financing risks, whereby internal acts must be proportionate to the nature, scope of operation and size of the obligor and must be approved by the top management. The obligor must ensure the application of the internal acts by determining relevant internal control procedures and mechanisms.

The obligor must in particular regulate by its internal acts:

– the process of drafting analyses of the money laundering and terrorism financing risk, including the manner in which such analysis is taken into account when deciding on taking other risks, or the introduction of new products of the obligor;

– procedures and mechanisms for detecting suspicious transactions and/or customers, as well as the manner in which employees will behave after identifying such transactions and procedures for providing information, data and documentation at the level of the obligor;

– determining the customer's admissibility according to the degree of the money laundering and terrorism financing risk in establishing a business relationship and over its duration;

– establishing the risk category of the customer, services, products and transactions according to risk factors relative to the money laundering and terrorism financing risk;

– the procedure for conducting customer due diligence actions and measures, which also includes the procedure of determining and verifying the identity of the customer and the procedure of determining the beneficial owner of the customer, regular monitoring of its operations in accordance with the established risk category, including the verification of compliance of the activities with the nature of the business relationship and the usual scope and type of its business, monitoring and updating, and/or periodical verification of the obtained information, data and documentation on the customer and its operations, and a potential change in its risk category;

– the procedure for the implementation of enhanced customer due diligence actions and measures, especially in cases referred to in Sections 13 to 18 of these Guidelines;

– determination of the products or services that the obligor will not provide to the customers of a particular risk category;

– compliance management procedures relating to these risks, including compliance management in all its business units, and the procedure for appointing a compliance officer and his deputy, as well as providing conditions for their work in accordance with the Law;

– the relevant procedure of determining and verifying the conditions for entering into employment and engaging persons outside employment with the obligor, so as to ensure high standards of employment and/or engagement of persons with the obligor, and the procedure of further verification of these conditions during employment and/or engagement;

– the procedure of regular internal control of the fulfilment of obligations under the Law, as well as internal audit, in accordance with the Law and Section 23 of these Guidelines;

– the procedure of conducting regular professional education, training and development of employees, in accordance with the programme of annual professional education, training and development of employees in the field of the prevention of money laundering and terrorism financing;

– record keeping, protection and storing of data from such records;

– the procedure for verifying the completeness of the data on the payer and the payee in the form of a payment order or an electronic message accompanying the transfer of funds, in accordance with the Law;

– the procedure in case that the transfer of funds or an electronic message on funds transfer does not contain complete data, in accordance with the Law;

– the procedure for verifying the completeness of data on all persons participating in the digital asset transaction, in accordance with the Law;

– the procedure in the case of non-submission of accurate and complete data on all persons participating in the digital asset transaction, in accordance with the Law;

– the procedure of implementing measures under the Law in branches and other business units and subsidiaries of a legal person in the majority ownership of the obligor, regardless of whether their place of operation is in the Republic of Serbia or in foreign countries;

– control of the application of procedures for the prevention of money laundering and terrorism financing at the group level, in accordance with the Law;

– the procedure for internal reporting on the violation of provisions of the Law.

The obligor shall also regulate by its internal acts:

– that the file on the opening of the account or the establishment of another form of a business relationship contains all necessary documentation prescribed by the Law, regardless of the organisational unit where the account is opened or a business relationship established;

– what actions will be performed and measures taken against the customers with whom it has not established a business relationship, but for which it performs occasional transactions (payment of bills, exchange transactions etc., from the scope of the obligor);

– measures and actions for monitoring the operations of the customer that it will, in accordance with the risk category of the customer, take or perform over the duration of the business relationship, as well as the conditions for changing its status according to the degree of exposure to the money laundering and terrorism financing risk.

If the obligor is a bank, it shall be bound by its internal acts to regulate the following:

– acting in the establishment of correspondent relationships with other banks and similar institutions, especially foreign banks and other similar institutions headquartered in a foreign country;

– monitoring the customer's transactions performed through all its accounts, regardless of the type of the account or the organisational unit of the bank where those accounts are opened, in accordance with the risk categorisation of the customer;

– the method of monitoring the customer's transaction based on the concluded contract if the customer's transaction is executed on the basis of a concluded business contract with a third party (e.g. the bank may obtain a copy of that contract, certified by the employee's signature and the date of receipt, kept for ten years).

An integral part of the internal acts shall also be a list of indicators for identifying persons and transactions for which there are grounds to suspect money laundering or terrorism financing, which obligors are required to supplement according to trends and typologies of money laundering that are known to them, as well as according to circumstances arising from the obligor's operations.

In order for the obligor to ensure adequate application of the provisions of its internal acts, it is particularly important that the relevant employees are familiar with the said provisions and with their obligations and responsibilities arising from these acts.

The obligor's top management must ensure that risk assessment and risk resolving processes are carried out in a professional manner, in accordance with the management's responsibility as to the obligor's legality of operations established by law.

19a. The obligor who is a member of a financial group shall implement the programme for efficient management of the money laundering and terrorism financing risk at the group level. The obligor who is a member of an

international financial group whose ultimate parent company is headquartered abroad can apply the group's programme only if the programme ensures the fulfilment of all its obligations in accordance with the Law, other regulations and international standards in the field of the prevention of money laundering and terrorism financing, provided the programme is not contrary to the regulations of the Republic of Serbia. The obligor shall ensure effective implementation of this programme at the level of the financial group in all branches and other business units of the obligor and majority-owned subordinated companies of the obligor.

The financial group referred to in paragraph 1 hereof means a group of companies consisting of financial sector persons, where at least one member of the group has the status of the ultimate parent company, and/or company that effectively controls the operation of the group or has a dominant influence on its operation.

In determining the programme referred to in paragraph 1 hereof, account shall be taken of the nature and scope of operation, and the size of the financial group, so as to ensure efficient and appropriate application of the programme in all branches and other business units of members of the group, and in the majority-owned subordinated companies of group members.

The provisions of Section 19 of these Guidelines, particularly provisions of paragraph 2, subparagraphs 8–11 of that Section shall apply accordingly to the contents of the programme, which also includes the appointment of the compliance officer at the level of the financial group.

The programme referred to in paragraph 1 hereof, as a single and comprehensive act that is efficiently applied in practice, shall contain in particular:

– policies and procedures for the exchange of information and data relating to customer due diligence and managing the money laundering and terrorism financing risk;

– procedures for obtaining information and data on clients, accounts and transactions from members of the financial group, branches and other business units of members of the group and majority-owned subordinated companies of members of the group, in relation to the performance of the compliance function, internal audit and the prevention of money laundering and terrorism financing at the group level, when this is necessary for the purpose of performing activities relating to the prevention of money laundering and terrorism financing;

– the procedure for the submission of information and data from subparagraph 2 hereof to members of the financial group, and branches and

other business units of members of the group and majority-owned subordinated companies of members of the group, when the holders of functions referred to in that subparagraph submit such information and data, on condition this is, in the concrete case, important for adequate management of the money laundering and terrorism financing risk, unless the Administration or the competent authority in a foreign country required different action;

– appropriate mechanisms to protect the confidentiality of information and data exchanged and used at the level of the group of companies, including the mechanisms to prevent tipping off, in accordance with regulations.

The data and information referred to in paragraph 5, subparagraph 2 hereof shall include information, data and analyses on transactions or activities that seem unusual (if analyses were prepared), the reporting on suspicious transactions, information and data that form the basis for the reporting of suspicious transactions and information on whether the transaction was already reported to the competent authority as suspicious.

19b. The obligor shall ensure that the activities and measures for the prevention and detection of money laundering and terrorism financing that are at least equal to those prescribed by the Law and these Guidelines are implemented in the same scope in its branches and business units operating abroad, and in majority-owned subordinated companies which operate abroad, unless this is explicitly contrary to the regulations of the country where business activities of these branches and business units and/or subordinated companies are carried out.

In the event that regulations of the country where business activities are carried out, including regulations governing the banking secret and personal data protection, do not allow for the application of the prescribed activities and measures for the prevention and detection of money laundering and terrorism financing at least at the equal level and in the same scope as in the Republic of Serbia, the obligor shall in the branch, business unit or subordinated company which operate abroad apply appropriate additional measures for the management of the money laundering and terrorism financing risk, and shall inform the National Bank of Serbia thereof without delay.

If it assesses that the additional measures referred to in paragraph 2 hereof are not sufficient, the National Bank of Serbia may order to the obligor to implement supplementary measures, including additional controls of branches, other business units and majority-owned subordinated

companies which operate abroad, as well as partial or complete cessation of activities through that branch, other business unit or subordinated company.

3. Internal organisation and/or organisational structure of the obligor

20. The obligor shall establish such internal organisation or organisational structure that will enable it to efficiently manage the money laundering and terrorism financing risk, taking into account:

- the nature, scope and complexity of operations;
- the diversity of operations and geographic distribution;
- the profile of customers, products/services;
- the volume and value of transactions;
- the level of risk associated with each area of operations;
- the extent to which the obligor has direct contact with customers, operates through intermediaries, third parties or correspondents, or there is access without direct contact.

The obligor shall in particular provide:

– the conditions and process of appointing a compliance officer and his deputy, who are also responsible for submitting reports to the top management of the obligor, as well as for initiating and proposing appropriate measures for the improvement of the system for the prevention and detection of money laundering and/or terrorism financing;

– the obligation of all organisational units of the obligor to provide assistance and support to persons referred to in indent 1 of this paragraph when performing the tasks referred to in this indent;

– establishing an appropriate reporting system that will enable adequate communication, information exchange and cooperation at all organisational levels and relevant employees at all levels with the obligor to provide timely, accurate and sufficiently detailed information necessary for the efficient management of the money laundering and terrorism financing risk; in addition to regular reporting, this system should also enable timely information of all relevant levels about identified deficiencies in the system for the prevention of money laundering and terrorism financing, the corrective measures taken and persons and deadlines established for their correction;

– protection against unauthorised disclosure of data on persons referred to in indent 1 of this paragraph and other procedures that may affect uninterrupted performance of their duties.

Due to the permanently increased volume of activities related to the prevention and detection of money laundering and terrorism financing, the nature and scope, type and complexity of the activities it performs, as well as

the risk profile of the obligor and the level of its exposure to the money laundering and terrorism financing risk, the obligor may enable the compliance officer and his deputy to perform the tasks within a separate organisational unit, which is functionally separate from other organisational units of the obligor and which is directly accountable to the top management.

If the compliance officer performs tasks within the other organisational unit of the obligor, this cannot affect his autonomy in the performance of tasks and direct accountability to the top management of the obligor in relation to the prevention of money laundering and terrorism financing.

The obligor must ensure that the compliance officer is in a classified job position that enables him to perform the obligations prescribed by the Law and regulations adopted based on the Law in a fast, high-quality and timely manner, and that enables independence in work and direct communication with the top management of the obligor.

4. Assessment, monitoring and surveillance in relation to the money laundering and terrorism financing risk

Annual assessment of exposure to the money laundering and terrorism financing risk

21. For the purpose of adequate risk management, the obligor shall at least once a year assess its overall exposure to the money laundering and terrorism financing risk. In making this assessment, the obligor shall in particular include the size of the obligor's network, number of employees directly responsible for performing activities related to the prevention of money laundering and terrorism financing in relation to the total number of employees, the number of employees who are in direct contact with customers, manner of organisation of activities and responsibilities, the dynamics of recruiting new staff, quality of training, etc.

In addition to the factors referred to in paragraph 1 of this Section, the obligor must include at least the following when making the annual assessment under that paragraph:

- the structure and number of customers according to the determined categories of the money laundering and terrorism financing risk and their percentage share in the total number of customers,
- the structure and number of high-risk customers by residence, country of origin, types of products and services they use, and the method of establishing a business relationship, as well as their percentage share in the total number of customers,

- the structure and number of customers in respect of which the performance of customer due diligence actions and measures is entrusted to a third party and their percentage share in the total number of customers,
- the structure and number of customers with whom correspondent relations are established and their percentage share in the total number of customers,
- representation and types of products and services with an increased money laundering and terrorism financing risk,
- the structure, number and value of transactions executed according to the determined categories of the money laundering and terrorism financing risk,
- the structure, number and value of transactions executed with an increased money laundering and terrorism financing risk and their percentage share in the total number and value of executed transactions,
- the structure, number and value of executed cash transactions and their percentage share in the total number and value of executed transactions,
- the structure, number and value of executed cash transactions reported to the Administration and their percentage share in the total volume of executed cash transactions,
- the structure, number and value of transactions reported to the Administration where there are grounds to suspect money laundering or terrorism financing and their percentage share in the total number and value of executed transactions,
- the structure, number and value of executed international transactions and their percentage share in the total number and value of executed transactions,
- the structure, number and value of executed transactions with high-risk countries and their percentage share in the total number and value of international transactions executed, as well as in the total number and value of transactions executed,
- the structure, number and value of transactions executed by using new technological achievements.

Based on the factors under this Section, as well as the measures it takes to mitigate the money laundering and terrorism financing risk, the obligor shall assess the overall exposure to the money laundering and terrorism financing risk as low-risk, medium-risk or high-risk.

The obligor shall ensure that, at least once a year, the relevant obligor's body receives the report on the overall exposure to the money laundering and terrorism financing risk, and the report on activities in the area of anti-money laundering and terrorism financing, which in particular contains an analysis of whether the measures taken are applicable and effective, what

shortcomings of the system for the prevention of money laundering and terrorism financing were discovered during the previous year and to what risks they can expose the obligor, as well as the proposed measures for their elimination and improvement of the system of money laundering and terrorism financing risk management.

Continuous monitoring and supervision

22. The obligor shall update the risk assessments of money laundering and terrorism financing based on business relationships and transactions, as well as the risk factors on which these assessments are based, in order to ensure the reliability, credibility and relevance of these assessments. The obligor shall evaluate the collected information within continuous supervision of the business relationship, and analyse whether changes affect the risk assessment.

The obligor shall establish the systems for identifying the emerging risks of money laundering and terrorism financing, and timely include them, as necessary, in its assessments, both at the individual level and at the level of the obligor.

The systems and controls that the obligor must establish to identify the emerging risks of money laundering and terrorism financing include:

- procedures ensuring a regular review of internal information in order to identify trends and new controversial issues regarding individual business relationships, as well as business operations of the obligor;
- procedures that provide a regular review of sources of information, which in particular includes a regular review of media reports that are relevant to particular sectors or countries where the obligor is active, a regular overview of warnings and reports from the bodies responsible for implementation of the Law, ensuring that the obligor is aware of changes in warnings about terrorist activities and sanction regimes immediately after their emergence, and regular review of publications issued by competent bodies;
- processes for collecting and reviewing information on new products/services;
- cooperation with representatives of other sectors and competent bodies;
- establishing awareness about the need for adequate information exchange within the obligor, as well as appropriate practices.

The systems and controls referred to in paragraph 3 hereof shall also include an effective and adequate system of monitoring transactions. The

effectiveness of the system enables the obligor to reliably recognise at any moment a suspicious or unusual transaction, and to carry out further assessment of such transaction without delay. The adequacy of the system depends on the nature, size and complexity of operations of the obligor, and on the assessed risk to which the obligor is exposed in its operations. In this regard, the obligor must determine:

1) what transactions to follow in real time, which can be subject to ex-post monitoring, and shall also determine the circumstances indicating a high risk, which it shall apply when determining the transactions to be followed in real time;
2) whether it will monitor transactions automatically or manually;
3) frequency of ex-post monitoring of transactions.

In addition to the obligations referred to in paragraph 4 hereof, the obligor shall also regularly check the executed transactions based on random sample, irrespective of whether they are followed in real time or ex-post, in order to make sure that the established system of transaction monitoring is reliable and adequate.

Internal control and internal audit

23. The obligor shall ensure adequate regular internal control of the performance of tasks for the prevention and detection of money laundering and terrorism financing, within the scope of the activities undertaken for the purpose of efficient management of the money laundering and terrorism financing risk. The obligor shall carry out internal control in line with the established money laundering and terrorism financing risk.

The scope of regular internal control shall be in line with the estimated level of the money laundering and terrorism financing risk.

The obligor shall organise independent internal audit whose scope includes regular assessment of the adequacy, reliability and efficiency of the system of money laundering and terrorism financing risk management when the law governing the activity of the obligor prescribes the obligation of having independent internal audit, or when the obligor assesses that, given the size and nature of activity, it is necessary to have independent internal audit.

The obligor shall ensure that internal audit is carried out in accordance with the size and scope of the obligor’s business, its risk profile and exposure to the money laundering and terrorism financing risk, and in the manner adapted to the specificities of the system for the prevention of money

laundering and terrorism financing established with the obligor. The subject of internal audit shall be in particular the following:

– adequacy of all processes related to the prevention of money laundering and terrorism financing;

- procedure of assessing the risk of a particular customer, business relationship, product/service or transaction in accordance with the policy of money laundering and terrorism financing risk management and risk analysis;
- adequacy of the protection of collected data available to the obligor in relation to the prevention of money laundering and terrorism financing;
- adequacy of professional education, training and development of employees in relation to the prevention and detection of money laundering and terrorism financing;

– adequacy and reliability of the procedures for submitting data on transactions and persons in respect of whom there are grounds to suspect money laundering or terrorism financing.

SPECIAL PART

1. Correspondent relationship with a bank or other similar institution of a foreign state

24. In establishing a correspondent relationship, the obligor must take into account that correspondent services enable banks and other similar institutions of other countries (including credit institutions and other financial institutions) to operate and provide different kinds of services (e.g. international payment operations, cash management – accounts that yield interest on deposits in different currencies, purchase of securities, cash flow management, cheque clearing, FX transactions and transactions with financial instruments), which they would not be able to provide otherwise (due to the impossibility of doing business outside the borders of the home country, as well as due to the absence of payment systems for international payments), and that in executing transactions for customers of banks and other similar institutions of other countries, the obligor does not have a direct business relationship with these customers (they may be natural persons, legal persons and persons under foreign law that are not established in the same country as the correspondent bank). Consequently, the customers of banks and other similar institutions of other countries are at the same time the correspondent bank’s customers. Due to the structure of these activities and the limited availability of information on the nature and purpose of the transactions being carried out, correspondent banks may be exposed to the money laundering and terrorism financing risk, and are therefore obliged to

apply enhanced customer due diligence actions and measures to banks and other similar institutions of other countries.

Risk factors that a correspondent bank shall consider when assessing risks include:

1) the nature and purpose of the correspondent relationship being established, in particular:

– the purpose of services provided to banks and other similar institutions of a foreign country,

– whether the establishment of the correspondent relationship enables direct provision of services to other banks and similar institutions, and/or whether the account and other correspondent services will be used by other banks and similar institutions with a direct relationship with the respondent and not the correspondent;

– whether the provided banking services will be used by third parties to which due diligence measures are not applied (including members of a group of companies that include the bank or other similar institution of a foreign country), as well as various risks arising from those third parties and parts of the group of companies that include the bank or other similar institution of a foreign country;

2) characteristics of operations of the bank and other similar institution of a foreign country and information about them, in particular:

– basic business activities of banks and other similar institutions of a foreign country, including target markets and all types of customers of the bank and these institutions in key business lines (the correspondent bank should have adequate knowledge of products and services that a bank or other similar institution of a foreign country offers to its parties, as well as the types of customers to whom it provides services and whether it operates with persons whose activity poses a high money laundering and terrorism financing risk),

– who are members of governing bodies and owners of the bank or other similar institution of a foreign country (including beneficial owners), and whether they (members of governing bodies, owners and beneficial owners) pose a special money laundering and terrorism financing risk (e.g. officials from a country that is associated with a higher money laundering and terrorism financing risk),

– policies and procedures for the detection and prevention of money laundering and terrorism financing, including controls for the prevention of money laundering and terrorism financing, and the description of customer due diligence actions and measures applied by a bank or other similar

institution of a foreign country to its customers, as well as the possibility for a correspondent bank to obtain information about a concrete transaction,

– whether court or administrative proceedings have been instituted against a bank or other similar institution of a foreign country, and whether irregularities have been determined and sanctions imposed in these proceedings, particularly in the field of the prevention of money laundering and terrorism financing, with information on the gravity of the irregularity, the manner in which a bank or other similar institution of a foreign state acts after having identified such irregularity, the gravity of the sanction, and the time that elapsed since the end of these proceedings and/or the imposition of sanctions;

3) the environment in which a bank or other similar institution of a foreign country operates, in particular:

– the country in which it operates, and the state of its parent company, if it is different from the country in which the bank or other institution of a foreign country operates (e.g. it comes from a country that is associated with a higher money laundering and terrorism financing risk),

– the quality and efficiency of regulations and supervision of banks / other similar institutions in the country where the bank or other similar institution of a foreign country and the state of its parent company operates, if the bank or other similar institution of a foreign country is a part of a group (in particular regulations governing the area of the prevention of money laundering and terrorism financing).

The obligor must assess previous experience in dealing with the bank or other similar institution of a foreign state.

The obligor must establish policies, procedures and systems for disclosing financial activities that are not in accordance with the purpose and aim of the services provided or for disclosing any financial activity that is contrary to the contractual obligations that the correspondent and the bank or other similar institution under foreign law assumed when establishing correspondent relationships. Continuous monitoring shall be performed at the level that corresponds to the risk profile of a bank or other similar institution of a foreign country.

The correspondent bank shall ensure from a bank or other similar institution of a foreign state that the message about the transaction to be delivered to the correspondent contains complete and accurate information about the principal and the payment beneficiary, and ensure that it is enabled to monitor transactions. The obligor shall prepare procedures for checking the

completeness and accuracy of the data contained in the transaction message.

Factors that can contribute to mitigating the money laundering and terrorism financing risk are that the obligor is assured on the basis of credible and reliable sources that:

– the controls for the prevention of money laundering and terrorism financing in a bank or other similar institution of a foreign state are no less effective than those prescribed by the Law;
– the bank or other similar institution of a foreign country is not headquartered in a country with an increased money laundering and terrorism financing risk;
– the bank or other similar institution of a foreign state is part of the same group of companies to which the obligor (correspondent) belongs and successfully applies standards in the field of money laundering prevention that are no less effective than those prescribed by the Law;
– the bank or other similar institution of a foreign country operates in a member state of the European Union in accordance with regulations of the European Union.

The obligors that, for the purposes of carrying out the analysis of a bank or other similar institution of a foreign country, use questionnaires drawn up for these purposes by international organisations (e.g. the Wolfsberg Group Anti-Money Laundering Questionnaire) shall assess whether the information obtained by using these questionnaires is sufficient to fulfil their legal obligations.

2. Electronic money issuers

25. The level of the money laundering and terrorism financing risk associated with electronic money largely depends on the characteristics of certain electronic money products, as well as the scope in which electronic money issuers distribute and purchase electronic money through third parties.

In addition to the application of the General Part of these Guidelines, electronic money issuers, within the meaning of the law governing payment services, shall apply the provisions of Sections 25 to 29 of these Guidelines, taking into account the following risk factors:

– product risk;
– risk of the customer (holder of electronic money);
– risk related to the distribution of electronic money;
– geographic risk.

Product risk

26. The assessment of risk with the issuer of electronic money may be indicated by the following circumstances in relation to the product:

– limits related to the issuance and use of electronic money;
– method of financing (redeeming or recharging) of electronic money;
– usable value and transferability.

The following factors may contribute to increasing the risks associated with the issuer of electronic money in relation to the product:

– the product allows for the payment with electric money, recharging or redeeming that money (e.g. cash withdrawal) in large and/or unlimited amounts;
– the product allows for large or unlimited amounts of money to be deposited in the electronic money account or the appropriate instrument;
– the product can be financed (purchased or recharged) anonymously or through another electronic money product, especially if that money is anonymous;
– the product allows person-to-person (P2P) transfers;
– electronic money in relation to that product is accepted as a means of payment with a large number of merchants or at a large number of points of sale;
– the product is intended to be accepted as a means of payment by merchants who sell goods and services that are associated with a high risk of financial crime (e.g. betting on the internet);
– the product can be used for cross-border transactions or transactions in another country;
– the product may be used by persons who are not the customer, e.g. partner cards, but not gift cards of small value;
– the product enables the purchase of electronic money by cash withdrawal.

The following factors may contribute to the mitigation of risks associated with the issuer of electronic money in relation to the product:

– low limits have been established for the payment, recharging or redemption of electronic money (including cash withdrawal) over a period of time (although obligors must bear in mind that this limitation does not in itself have to be sufficient to represent a circumstance that can reduce the money laundering and terrorism financing risk);

– the number of payments, recharges or redemptions of electronic money (including cash withdrawal) in a given period is limited;

– the product allows only for small amounts of money to be deposited in an electronic money account or in an appropriate instrument, at any time;

– the product allows for the means for redemption or recharge, with verification, to be transferred from an independent or joint account which the customer opened with a financial institution of a resident of the Republic of Serbia or a resident of the European Economic Area (hereinafter: EEA);

– the product does not allow or strictly limits cash withdrawal;

– the product can be used only within one country;

– electronic money in relation to the product as a means of payment is accepted by a small number of merchants or points of sale, whose operations are known to the issuer of electronic money;

– the product cannot be used or its use is restricted to merchants that sell goods and services that are associated with a high risk of financial crime;

– the product is accepted as a means of payment only for certain types of low-risk services or products.

Customer risk

27. The following factors may contribute to increasing the risks associated with the issuer of electronic money in relation to the customer:

– the customer buys electronic money based on several products from the same issuer of electronic money, frequently recharges or redeems the product (withdraws cash) at short intervals without economic justification, and if distributors (or agents acting as distributors) are at the same time obligors, this also applies to electronic money products of different issuers purchased from the same distributor;

– the values of transactions performed by the customer are always slightly lower compared to any limitation of the value (limits);

– there are circumstances indicating that the product is used by several persons whose identity is not known to the issuer (e.g. the product is simultaneously used with several internet protocol addresses (hereinafter: IP address));

– there are frequent changes in customer identification data, such as the address of the place of residence or IP address or related accounts in the bank;

– the product is not used for the intended purpose (e.g. it is used globally, and is intended for use as a gift card only at certain points of sale).

A low risk may be indicated by the fact that the product is available only to certain categories of customers, e.g. socially vulnerable persons or employees in the legal person that issues them for the purpose of covering the costs.

Distribution risk

28. The following factors may contribute to increasing the risks associated with the issuer of electronic money in relation to the distribution of electronic money:

– the issuance and distribution of electronic money via the internet or otherwise without the physical presence of the customer, without proper identification, such as electronic signatures, electronic identification documents, and other measures aimed at preventing abuse or concealment of genuine identity;

– distribution of electronic money through third parties that are not obligors within the meaning of the Law, when the issuer of electronic money is aware that some of the measures that the obligor must implement to prevent money laundering and terrorism financing will be carried out by the distributor, and it has not reliably established that the distributor has appropriate systems and controls established to adequately take these measures;

– separation of services, which means the provision of services relating to electronic money by several operatively independent providers of such services without proper supervision and coordination.

When concluding the agreement on distribution of electronic money through third parties, the obligor should understand the nature and purpose of activities performed by the third party, in order to make sure that the goods and services sold and/or provided by this person are compliant with regulations. The obligor should also assess the risks of money laundering and terrorism financing relating to the activity performed by the third party. If the third party operates online, the obligor should also understand the structure of customers that such person has or will have, and should determine the expected volume and value of transactions to be carried out through the third party for the purpose of recognising suspicious or unusual transactions.

Geographic risk

29. The following factors may contribute to increasing the risks associated with the issuer of electronic money in relation to the geographic risk:

– the fact that the payee is located in a country that is associated with a higher money laundering and terrorism financing risk;

– the fact that the product is financed from a country that is associated with a higher money laundering and terrorism financing risk.

The obligor must pay particular attention to those legal systems that are known for providing funds or supporting terrorist activities or that are known to have operational terrorist groups, as well as legal systems where financial sanctions, embargoes or other penal measures are imposed as a consequence of connection with terrorism, terrorism financing or proliferation of weapons of mass destruction.

3. Payment service providers

30. In addition to the application of the General Part of these Guidelines, payment service providers, within the meaning of the law governing payment services, shall apply the provisions of this Section, given the need to take into account the circumstances of payment services provision during risk analysis, particularly payment services which due to simplicity and speed, the possibility of cross-border provision, and the nature of these services conditioning more frequent one-time (sporadic) payment transactions compared to transactions based on business relationships with the customer, lead to the fact that the perception of a relevant risk associated with the customer may be limited (e.g. execution of a remittance).

Product risk

31. A high risk may be indicated by the following circumstances:

– the payment service enables payment transactions in large or unlimited amounts;

– the payment service has a global reach;

– the payment transaction is cash-based or financed by anonymous electronic money or electronic money products, which are an exception to the obligation to perform customer due diligence actions and measures, in accordance with Article 16 of the Law;

– transfer is effected by payments of one or more payers from different countries to the local payee.

A low risk can be indicated by the circumstance that the transfer is made by using funds from the payment account that is in the name of the payer with a financial institution of a resident of the Republic of Serbia, or a resident of an EEA state, and the payee is a resident of the Republic of Serbia or a resident of an EEA state.

Customer risk

32. A high risk may be indicated by the following circumstances relating to the behaviour of the customer:

– the needs of the customer may be met elsewhere in a faster and/or simpler manner;

– the customer leaves the impression that it acts on someone's behalf, e.g. when it is visible that other persons monitor the customer inside or outside the premises in which the transaction is performed or the customer acts by reading an instruction note, the customer's behaviour does not have economic justification, the customer unquestionably accepts an unfavourable exchange rate or a high fee, requires a transaction in a currency that is not an official means of payment or is unusual in the legal system of the country where the customer or the payee is located, or asks for or gives significant amounts of currency in large or small denominations;

– payment transactions of the customer are always slightly below the appropriate limits;

– the customer uses the service in an unusual way, e.g. sends money to himself or receives the money it sent to himself or sends money immediately upon receipt;

– the customer leaves the impression that he does not know much about the payee or is cautious when providing information about the payee;

– several customers make the transfer of funds to the same payee or leave the impression that they have the same identification data, e.g. address or phone number;

– the payment transaction is not accompanied with the requested data on the payer or the payee;

– the amount sent or received does not correspond to the income of the customer (if known).

A low risk may be indicated by the following circumstances:

– the previous behaviour of the customer that is a long-term customer of the service provider does not cause suspicion or indicate the existence of the money laundering and terrorism financing risk;

– the amount of transfers is low (however, obligors have to bear in mind that small-scale transactions do not necessarily represent a circumstance that indicates a lower money laundering and terrorism financing risk).

Risk of establishing a business relationship

33. A high risk may be indicated by the following circumstances:

1) there are no restrictions concerning the payment instrument, e.g. payment by cash or payment by electronic money products which constitute an exception to the obligation to perform customer due diligence actions and measures, in accordance with Article 16 of the Law;

2) the manner of establishing a business relationship provides a certain degree of anonymity;

3) the payment service is fully provided via the internet without proper identification;

4) the payment service is provided through the agent:

– representing several payment service providers,

– whose turnover, in comparison with other agents in similar locations, is unusual (e.g. unusually large or small amounts of transactions, unusually large cash transactions, a large number of transactions slightly below the limit prescribed for the implementation of enhanced customer due diligence actions and measures, or business operations of the agent outside of working hours),

– where a large part of business operations is related to payers and payees from countries where the legal and institutional framework is such that there is a high level of the money laundering and terrorism financing risk,

– in relation to which there is suspicion regarding the manner and consistent application of policies for the prevention of money laundering and terrorism financing at the group level,

– that is not from the financial sector, or does not perform financial activity as core activity;

5) the payment service is provided through a complex network of agents in different countries;

6) a complex service chain (e.g. a large number of intermediaries operating in different countries or a service chain is such as to prevent the monitoring of payment transactions).

A low risk may be indicated by the following circumstances:

– agents are regulated financial institutions;

– payment services consist of transfer from an account in the name of the customer with a financial institution – resident of the Republic of Serbia or an EEA resident, or the customer has proven that it is authorised to dispose of funds in that account, and the payee is a resident of the Republic of Serbia or an EEA resident.

Geographic risk

34. A high risk may be indicated by the following circumstances:

– the payer or the payee is a permanent or temporary resident, or has a head office or permanent activity in a country whose legal and institutional framework is such that there is a high degree of the money laundering and terrorism financing risk;

– the payee is a permanent or temporary resident, or has a head office or permanently performs activity in a country in which the regulated banking sector is underdeveloped, which means that for payments it is possible to use the services of the transfer of funds provided by unregulated entities (e.g. hawala, a traditional money transfer system used in Arab countries and South Asia, whereby money is paid to an agent who then instructs his associate in the respective country or region of that country to pay money to the final payee).

Measures undertaken by the payment service provider licensed to provide the payment service of remittances execution

34a. The obligor that is a payment service provider licensed to provide the payment service of remittances execution shall establish the system for the monitoring of transactions, which enables detecting the attempts of money laundering or terrorism financing also in the cases when the information and data based on customer due diligence actions and measures are insufficient or incomplete because the business relationship is not established.

When deciding on the adequate system for the monitoring of transactions, the obligor referred to in paragraph 1 hereof shall take into account the size and complexity of the business network (including representatives), and the scope of transactions performed.

34b. The obligor shall establish the following procedures and technical solutions:

– for the recognition of connected transactions, including those indicating the existence of a business relationship between the payer and the payee, such as the system recognising transactions below EUR 1,000 in the dinar equivalent, when the payer and the payee are the same persons carrying out transactions over a longer period;

– for the recognition of transactions when different payers transfer funds to the same payee;

– for detecting the origin of funds to be subject to the transaction, and the destination of those funds, to the extent possible;

– which enable complete following of both transactions and the number of intermediaries in remittances execution;

– which enable determining whether the transaction originates from or is carried out in the country with strategic deficiencies in the system for the prevention of money laundering and terrorism financing;

– which prevent that unauthorised persons influence the process of remittances execution from the receipt until the payment of funds.

4. Insurance undertakings and insurance brokerage undertakings

35. Insurance undertakings with a licence to perform life insurance business and insurance brokerage undertakings when they engage in life insurance brokerage must, in order to prevent money laundering and terrorism financing, particularly identify risks that indicate suspicious transactions and manage those risks so as to prevent activities that could be characterised as money laundering and terrorism financing.

Customer risk

36. The customer risk involves assessing whether the customer with which the insurance undertaking and/or brokerage undertaking cooperates is associated with a higher money laundering and terrorism financing risk. The customer means a policyholder and an insured in the procedure of payments of life insurance policies in accordance with Article 26 of the Law.

A high risk may be indicated by the following circumstances:

1) nature of the customer:

– the customer, beneficial owner of the customer, insurance beneficiary or beneficial owner of the insurance beneficiary is an official,

– the age of the customer (in this case, of the insured) is unusual for the type of the requested product (e.g. the buyer is very young or very old),

– the contract does not correspond to the customer's financial capacity;

2) Customer's behaviour:

– in relation to the contract (e.g. the customer often transfers the contract to another insurer, there are frequent and inexplicable redemptions, especially when the refund is made to different bank accounts; the customer bears high costs, requesting premature termination of the contract; the customer transfers the contract to an unrelated third party; the customer's

request for change or increase of the insured sum and/or premium is unusual or excessive),

– in relation to the insurance beneficiary (e.g. the insurer is familiar with the change of the insurance beneficiary only after filing a claim for damages; the customer changes the insurance beneficiary and appoints an unrelated third party; the insurer, customer, beneficial owner of the customer, insurance beneficiary or beneficial owner of the insurance beneficiary are in different jurisdictions),

– in connection with payments (e.g. the customer uses unusual payment methods or means enabling anonymity; payments from different accounts without explanation; payments from banks / financial institutions that are not established or do not operate in the country of residence of the customer; the customer makes frequent or high-value payments where this is unexpected; payments received from unrelated third parties).

Product risk

37. A high risk may be indicated by the following circumstances:

1) insurance products that are new in the market, i.e. not previously offered and must be especially monitored in order to determine the actual degree of risk;

2) an insurance product that enables:

– payments from third parties whose identity has not been established,

– payment of a premium of high or unlimited value, excessive payments or a large volume of payments for low-value premiums,

– cash payments;

3) easy access to accumulated assets, e.g. the product allows partial withdrawal or early redemption of an insurance policy at any time, with limited fees or expenses;

4) the insurance product used:

– for trading in the secondary market,

– as a means of securing loan repayment;

5) anonymity, e.g. the product facilitates or allows the anonymity of the customer or insurance beneficiary.

A low risk may be indicated by the following circumstances:

– the insured sum is paid only for a predefined event, e.g. death or at a certain date, as is the case with a life insurance policy for debt repayment, which covers consumer and mortgage loans and where payment is made only in the event of death of the insured person;

– the policy does not have a redemption value;

– the product does not have an investment component;

– there is no possibility of paying insurance premiums by third parties;

– the product requires that total investment be limited to a low value;
– life insurance policy is with a low premium;
– the product only allows regular payments of a low-value premium, e.g. does not allow overpayment;
– no policy redemption can be made in the short or medium term;
– the policy cannot be used as a means of security;
– cash payments are not allowed.

Business relationship risk

38. A high risk may be indicated by the following circumstances regarding insurance distribution channels:

– sale of insurance without the physical presence of the customer (e.g. online sale) without adequate safeguards, such as electronic signatures or electronic identification documents;
– long chains of insurance agents;
– the insurance broker is used in unusual circumstances (e.g. inexplicable geographical distance).

A low risk may be indicated by the following circumstances:

– brokers are well known to the insurer, which is convinced that the broker applies customer due diligence actions and measures, in proportion to the risk associated with the business relationship;
– the product is available only to the employees of certain companies that have a contract with a life insurer for their employees, e.g. as part of the benefits package.

Geographic risk

39. The geographic risk exists if the transaction related to the insurance product is carried out through a risky state, or if the person involved in the transaction is a resident of a risky state.

A high risk may be indicated by the following circumstances:

– the insurer, customer, beneficial owner of the customer, insurance beneficiary or beneficial owner of the insurance beneficiary are headquartered and/or have residence in a country that is associated with a higher money laundering and terrorism financing risk;

– premiums are paid through accounts opened with financial institutions established in a country that is associated with a higher money laundering and terrorism financing risk;

– the broker is headquartered in or connected with a country that is associated with a higher money laundering and terrorism financing risk.

A low risk may be indicated by the following circumstances:

– states are identified from credible sources, such as mutual evaluations or detailed assessment reports, in terms of the presence of effective systems for the prevention of money laundering and terrorism financing;

– states are identified from credible sources, in terms of a low level of corruption and other criminal activities.

5. Voluntary pension fund management companies

Customer risk

40. A higher risk may be indicated by activities performed by the following customers:

1) the customer carrying out business activity or transaction under unusual circumstances, such as:

– frequently and unexpectedly establishes, without economic justification, business relationships, such as signing multiple membership contracts in a voluntary pension fund in a short period of time (regardless of whether they are concluded with one or several management companies);

– frequent transfers of funds from one voluntary pension fund to another;

− amending the membership contract in a voluntary pension fund for the purpose of an unusually high increase in the amount of the contribution;

− membership in a voluntary pension fund, i.e. payments of funds to the individual account of persons in which due to age, there is no possibility of a significant period of accumulation,

− termination of the contract on pension plans and membership contracts in the voluntary pension fund shortly after their conclusion, especially in the case of high contributions;

− request that the funds accumulated in the individual account of a member of the voluntary pension fund be paid to the current account of a third person or to the account of a person in the territory of a country in which

the standards in the field of money laundering and terrorism financing prevention are not applied;

2) the customer where due to the structure, legal form or complex and unclear relationships, it is difficult to determine the identity of the beneficial owner of the customer or persons managing it;

3) the person whose offer to establish a business relationship was rejected by another management company, regardless of the way in which this fact became known, and/or the person with a bad reputation;

4) the customer whose sources of funds are unknown or unclear, and/or cannot be proven by the customer,

5) the customer that establishes business cooperation without physical presence;

6) the customer in respect of which customer due diligence activities are entrusted to a third party;

7) the customer participates in a voluntary pension fund which is intended for a smaller number of persons with higher income or persons closely related by family links or otherwise.

Transaction risk

41. The transaction risk in management companies concerns transactions without economic justification, such as withdrawals of funds from an individual account of a voluntary pension fund member in the short period after their payment.

5a. **Financial lessors**

Customer risk

41a. The following factors may contribute to the increase in customer risk in the financial lessor:

– a customer concludes several lease agreements in a short period without a clear economic justification;

– a customer that is a natural person and does not have the status of an entrepreneur requests the conclusion of the lease agreement for the purpose of procuring machinery and other equipment used in the production process;

– a customer that has the status of an entrepreneur or company requests the conclusion of the lease agreement to procure assets not related to the performance of the prevalent activity of the customer;

– a customer that rescinded the lease agreement relatively quickly after its conclusion soon appears with the intention to conclude a new lease agreement concerning the subject which is the same or similar to the subject of lease in the rescinded agreement;

– a customer establishes business cooperation without physical presence.

5b. Virtual currency service providers

41b. In addition to applying the general part of these Guidelines, virtual currency service providers, within the meaning of the law governing digital assets, shall also apply the provisions of this section bearing in mind the following risk factors:

– product risk (services connected with virtual currencies);
– customer risk;
– geographic risk.

Product risk

41c. The following circumstances may indicate a high product risk:

– the virtual currency service enables the execution of virtual currency transactions of high or unlimited value;
– the virtual currency service is provided exclusively by means of a crypto ATM or the purchase and/or sale of virtual currencies is carried out exclusively for cash or anonymous e-money or e-money products which are an exception from the obligation of customer due diligence in accordance with Article 16 of the Law.

The provision of virtual currency services which indirectly or directly enable the concealment of the customer's identity and the performance of transactions with such virtual currencies shall be prohibited. A virtual currency service provider shall refuse the establishment of a business relationship with a customer with a view to providing such virtual currency services, and/or shall refuse the execution of such transaction.

A virtual currency service provider may not use the information system resources (software components, hardware components and information goods) which enable and/or facilitate the concealment of the customer's identity and/or disable and/or aggravate the monitoring of virtual currency transactions.

Customer risk

41d. The following circumstances may indicate a high customer risk:

– the customer behaves in a suspicious or unusual way, avoids to give data or gives incomplete or insufficient data or data which seem to be false or inconsistent, including data on the person in whose favour he initiates the virtual currency transaction;

– the customer often changes identification data (e.g. the business name, permanent residence, and/or head office, representative etc.), including data relating to business activities and financial status of the customer;

– the customer refuses to submit a personal document or submits a personal document suspected of being falsified and/or modified;

– due to the structure, legal form, or complex and unclear relations, it is hard to determine the identity of the customer's beneficial owner or persons managing the customer;

– the customer performs virtual currency transactions in values slightly smaller compared to any value limits;

– the customer performs virtual currency transactions in values significantly higher than its actual financial capacity (according to the available data on the customer's financial status);

– the customer continuously buys high-risk (highly volatile) digital assets;

– there are circumstances indicating that the product is used by one or several persons whose identity is not known to the virtual currency service provider (e.g. the product is simultaneously used from several IP addresses);

– the customer performs virtual currency transactions which include several different types of virtual currencies or several money accounts or uses a crypto ATM for the execution of several low-value transactions, when there is no economic justification for it (e.g. regardless of higher fees for such transactions);

– the customer performs one or several virtual currency transactions successively, and/or frequently in a short period (24–72 hours);

– the customer has a proxy through which he performs virtual currency transactions;

– the customer is obviously not familiar with the manner of performing virtual currency transactions and the underlying technology or is a financially vulnerable person (e.g. a student, an unemployed person) or performs high-value transactions which are not in line with his financial status, or the customer's behaviour is economically unjustified (e.g. he unconditionally accepts an exceptionally high fee), which is why there is a justified suspicion that the customer is not performing the transaction in his name and for his account;

– the customer is associated with criminal activities based on publicly available information;

– customer due diligence actions and measures are outsourced to a third party;

– the customer performs virtual currency transactions in relation to services connected with a high risk of financial crime (e.g. online betting).

Geographic risk

41e. The following circumstances may indicate a high geographic risk:

– the customer or the person in whose favour the customer initiates the execution of a virtual currency transaction has a permanent or temporary residence, and/or head office, or performs a business activity in the state whose legal and institutional framework is such that there is a high money laundering and terrorism financing risk;

– the customer is a virtual currency or other digital asset service provider from the state whose regulations do not regulate digital asset operations and licensing or registration of digital asset service providers, and there is no supervision of digital asset service providers, or the state whose legal and institutional framework is such that there is a high money laundering and terrorism financing risk, or such virtual currency or other digital asset service provider participates in the execution of the virtual currency transaction;

– a virtual currency or other digital asset service provider from another state participates in the execution of the virtual currency transaction and it provides to its customers virtual currency services which indirectly or directly enable the concealment of the customer's identity, and/or who performs transactions with such virtual currencies.

6. Obligor performing exchange operations

42. Authorised exchange dealers, as well as the economic entity performing exchange operations based on a separate law governing its activity (hereinafter: public postal operator), within the meaning of the law governing foreign exchange operations, shall implement the approach based on ML/TF risk assessment, i.e. to develop and regularly update the analysis of the risk and to efficiently manage the risk by carrying out appropriate activities and measures with the aim of detecting and preventing ML/TF risk and establishing efficient systems for combating money laundering and terrorism financing.

Authorised exchange dealers, as well as the public postal operator and a bank when performing exchange operations (hereinafter collectively termed: exchange dealer or obligor), shall apply the provisions in the General Part of these Guidelines accordingly, unless otherwise stipulated by the provisions in this part, bearing in mind that these are specific foreign cash purchase and sale operations with natural persons in the country.

Customer risk

43. Customer risk shall imply an assessment of whether the customer is associated with a higher risk of money laundering and terrorism financing and how likely it is that customers in a certain category would abuse obligors for the purpose of money laundering and terrorism financing.

A higher risk may be indicated by the following activities:

– the customer is behaving in a suspicious or unusual manner, avoiding his obligations or hesitating to continue with the transaction after being informed that he needs to identify himself;

– the customer seeks to provide as little information as possible or provides information that appears false or inconsistent;

– the customer keeps changing the information he has provided as soon as he is asked to provide more details;

– the customer refuses to present his personal documents;

– the customer questions the requirement to identify himself or to submit data to the Administration with an evident intention to avoid this requirement;

– the customer resorts to threats in an effort to prevent being identified or submitting data to the Administration;

– the customer voices concern over the obligor's intention to submit data to the Administration;

– the customer discontinues the transaction after being told that he must identify himself;

– the customer attempts to reduce the transaction amount after learning that he must identify himself;

– the customer wants to buy/sell a larger amount of money or to perform a considerable number of transactions;

– the customer brings money in currency straps with different bank stamps or markings;

– the customer is controlled by another person, especially when it appears that the customer is unaware of that or if he is an elderly person accompanied by someone who is not a relation;

– the customer is a person with a criminal history who wants to buy/sell a larger amount of money or to perform a considerable number of transactions;

– the customer is a student, an unemployed person or a low-income person, and wants to exchange large amounts of money;

– the customer is selling faded or damaged banknotes in a considerable amount;

– the customer is buying/selling banknotes which are wrapped or packaged, which is unusual for that customer;

– the customer is delivering uncounted money, and after counting it, he is lowering the transaction to the amount slightly below the legal limit subject to reporting;

– the customer is buying/selling a larger amount of money and is asking the exchange dealer to split the transaction into amounts not subject to reporting under the Law;

– the customer is buying/selling a larger amount of money and is not interested in the exchange rate used by the exchange dealer or in the amount of the commission charged by the exchange dealer;

– the customer or his family members perform purchase/sale transactions in larger amounts rather frequently or cyclically, i.e. in the same intervals (on the same day of the week, month or similar);

– the customer or his family members perform frequent purchase/sale transactions in identical or rounded amounts, or in amounts slightly lower than the ones that are subject to reporting according to the Law;

– when buying a larger amount of US dollars, the customer insists on denominations for which customer identification is not required by regulations governing exchange operations (this is obligatory when buying denominations of USD 50 and USD 100);

– the exchange dealer learns that the customer has already performed purchase/sale transactions of larger amounts of money on the same day and at other exchange offices;

– the customer is offering money, gifts or services to the exchange dealer in return for providing exchange services;

– the customer has an unusually good knowledge of legal regulations regarding the reporting of suspicious transactions, is quick to confirm to the exchange dealer that the money is “clean”, etc.;

– the customer is very “chatty” about topics regarding money laundering and terrorism financing;

– the customer is performing the transaction accompanied by a person who is evidently monitoring the customer’s behaviour or insisting that the transaction be carried out quickly;

– for identification purpose, the customer presents documents that appear to be forged, altered or incorrect;

– the customer is showing interest in the way in which he could buy/sell a larger amount of money without having to present a personal document for identification purposes;

– the customer presents only copies of personal identification documents;

– the customer is trying to prove his identity in another manner, instead of by presenting a personal document;

– for identification purposes, the customer presents documents issued abroad whose authenticity cannot be verified;

– the customer is an official;

– the customer tries to sell a larger amount of money in the currency which is not convertible and is not on the foreign exchange list in accordance with the decision determining the types of foreign exchange and foreign cash purchased and sold in the FX market or the currency is unusual.

Geographic risk

44. Geographic risk implies the assessment of exposure to ML/TF risk depending on the customer’s country of origin or the person performing the transaction and the area or territory where the obligor is located.

A higher ML/TF risk is associated with customers whose country of origin:

– has been the subject of sanctions, embargoes or similar measures imposed by the United Nations, Council of Europe, OFAC or other international organisations;

– has been designated by credible organisations and institutions (FATF, Council of Europe, IMF, World Bank, etc.) as a country that does not apply adequate measures for the prevention of money laundering and terrorism financing;

– has been designated by credible organisations and institutions (FATF, United Nations, etc.) as a country that supports or finances terrorist activities or organisations;

– has been designated by credible organisations (IMF, World Bank, etc.) as a country with a high degree of corruption and crime.

Transaction and service risk

45. A comprehensive ML/TF risk assessment must take into account the potential risks arising from foreign cash purchase and sale transactions to natural persons. The obligor has to assess the likelihood that the customer would abuse the obligor or the transaction for the purpose of money laundering and terrorism financing, as well as to assess the impact of such event in the same manner it assesses customer risk.

A higher risk may be indicated by the following activities:

– transactions in the amount slightly lower than EUR 5,000 in the dinar equivalent;

– several interconnected transactions in the amount slightly lower than EUR 5,000 in the dinar equivalent;

– transactions in the amount of EUR 15,000 or more in the dinar equivalent;

– several interconnected transactions in amounts lower than EUR 15,000 in the dinar equivalent whose sum exceeds EUR 15,000 in the dinar equivalent;

– the customer is selling large amounts of foreign cash in higher denominations and is afterwards buying smaller denominations in the same currency (practically, he is changing large banknotes for smaller ones), or he is selling foreign cash in smaller denominations and afterwards buying foreign cash in larger denominations in the same currency (practically, he is changing smaller banknotes for larger ones);

– unusually frequent transactions, with faded or damaged banknotes, or banknotes wrapped in currency straps of different banks, etc.;

– frequent purchase/sale transactions in identical or rounded amounts, or in amounts slightly lower than the ones that are subject to reporting to the Administration;

– purchase/sale transactions of a larger amount of money, where the exchange dealer is asked to split the transaction into amounts not subject to reporting under the Law;

– purchase/sale transactions in larger amounts performed rather frequently or cyclically, i.e. in the same intervals (on the same day of the week, month or similar).

Customer due diligence actions and measures

46. The obligor shall carry out customer due diligence actions and measures, determination and verification of the customer's identity based on documents, data and information obtained from reliable and credible sources when:

1) executing a transaction worth EUR 5,000 or more in the dinar equivalent, regardless of whether it is one or several interconnected transactions. This shall be carried out before executing the transaction;

2) there are grounds to suspect money laundering or terrorism financing in relation to the customer or the transaction;

3) there are doubts as to the veracity or credibility of the obtained data about a customer.

The obligor establishes and verifies the customer's identity by obtaining the prescribed data. When identifying a natural person, his legal representative or proxy, the obligor shall obtain a photocopy or the scan reading of that person's identity document, on which the date, time and personal name of the person who inspected the document are written. The photocopy and/or the scan reading of the personal document shall also be considered the digitalised document referred to in Article 17, paragraphs 2 and 4 of the Law. The photocopy and/or the scan reading of the personal document in electronic form shall contain the qualified electronic stamp and/or qualified electronic signature, in accordance with the law governing electronic signature, with a timestamp. The photocopy and/or the scan reading of the personal document referred to in this paragraph shall be kept by the obligor in hardcopy or electronic form in accordance with law. If, during the establishment and verification of the customer's identity, the obligor suspects the veracity or credibility of the documents, it shall obtain a written statement about the veracity and credibility of data and documents from the customer.

The obligor shall refuse to execute a transaction if he cannot establish and verify the customer's identity. The obligor shall prepare an official note about this in writing, as well as consider whether there are grounds to suspect money laundering or terrorism financing, and to notify the Administration thereof. The obligor shall keep the official note and the photocopy of the personal document in accordance with the Law.

The obligor shall take enhanced customer due diligence actions and measures when:

1) executing a transaction worth EUR 5,000 or more in the dinar equivalent, regardless of whether it is one or several interconnected

transactions with a customer who is an official. This shall be carried out before executing the transaction;

2) executing a transaction with a customer from a state that has strategic deficiencies in the system for the prevention of money laundering and terrorism financing;

3) it assesses that due to the manner of performing the transaction, the customer's profile and/or other circumstances associated with the customer, there is or there might be a high ML/TF risk.

Pursuant to the provisions of the Law, the obligor must carry out risk assessment in all cases when the customer is an official, before executing a transaction.

According to law, in its internal act the obligor shall define which enhanced actions and measures it will carry out and in which scope, for each individual case, as well as to define the process for determining whether a customer is an official, a member of the immediate family of the official or a close associate of the official.

Notwithstanding Section 15 of these Guidelines, in its internal act the authorised exchange dealer shall also define the procedure for determining whether a customer is an official, a member of the immediate family of the official or a close associate of the official.

Submitting information, data and documents to the Administration

47. The obligor shall submit to the Administration data about every cash transaction equalling or in excess of EUR 15,000 in the dinar equivalent, as soon as the transaction has been executed and no later than three days from the execution day.

The obligor shall submit data to the Administration in all cases where there are reasons to suspect money laundering or terrorism financing in relation to a transaction or customer. This shall be done before executing the transaction, and with the stated deadline for the execution of the transaction. In case of urgency, such report may also be delivered by phone, while a written report shall be submitted to the Administration by no later than the following business day. The obligation to report on these transactions applies to scheduled transactions as well, regardless of whether they have already been executed.

The data shall be submitted to the Administration on the Form for reporting cash and suspicious transactions and suspicious activities (Form 1). Together with Instructions for filling it in, the Form is integral to the Rulebook on Methodology for the Performance of Tasks in Accordance with the AML/CFT Law and is available on the Administration's website. The obligor

shall specify whether it is a suspicious transaction/customer, as well as the reasons for suspecting money laundering or terrorism financing.

Appointing the compliance officer and his deputy

48. The obligor shall appoint a compliance officer and his deputy immediately upon obtaining the authorisation to perform exchange operations, i.e. before executing the first transaction. If the obligor has only one employee, then this employee shall be considered the compliance officer.

The obligor shall submit to the Administration data about the personal name and job position of the compliance officer and his deputy, as well as data about the personal name and job position of the member of the top management, responsible for the implementation of the Law, as well as any change in those data within 15 days of appointment.

The obligor shall provide conditions for work to the compliance officer and his deputy, as well as assistance and support in their tasks; it shall also regularly notify them about the facts that are or might be associated with money laundering and terrorism financing. The obligor shall prescribe the manner of cooperation between the compliance officer and other organisational units.

Mandatory regular professional education, training and development for employees

49. The obligor shall ensure regular professional education, training and development for employees tasked with the detection and prevention of money laundering and terrorism financing. Professional education, training and development means being acquainted with provisions of the Law, these Guidelines, regulations governing the limitation of the use of assets to prevent terrorism and proliferation of weapons of mass destruction, regulations governing personal data protection, other regulations, internal acts, scholarly literature in this area and the indicator list, as well as being continuously informed via the websites of the Administration and the National Bank of Serbia.

The obligor shall develop an annual professional education, training and development programme for employees in the area of the prevention and detection of ML/TF by no later than the end of March for the current year.

The programme from paragraph 2 of this Section shall contain as a minimum:

1) the planned number of training sessions in one year;
2) the planned number of employees who will attend the training, as well as the profile of employees to whom the training is intended;
3) topics relating to the prevention of money laundering and terrorism financing that will be covered during the training;

4) manner in which the training will be carried out (seminars, workshops, etc.).

In the year for which the programme has been adopted, and no later than end-March the following year, the obligor shall carry out the training sessions and make an official note thereof. The official note must include the time and place of the training, the number of employees in attendance, the name and surname of the person providing the training and a brief description of the topic covered in the training session.

Ensuring regular internal control

50. The obligor is required to ensure regular internal control of operations of detecting and preventing money laundering and terrorism financing. Internal control is carried out in line with the established ML/TF risk.

The aim of internal control is to detect and eliminate the identified shortcomings, as well as to improve the internal system for detecting persons and transactions suspected to be associated with money laundering or terrorism financing.

During internal control, and using the random sampling method or in another appropriate manner, the obligor shall test the implementation of the system for the prevention of money laundering and terrorism financing and the adopted procedures.

In case of changes in the business process (e.g. organisational changes or changes in business procedures), the obligor shall verify and align his procedures within its internal control, to make sure they are adequate for carrying out obligations under the Law.

Once a year, as well as every time a change occurs, and no later than the day of the introduction of that change, the obligor shall verify the alignment of the system and procedures for implementing the Law and internal procedures.

The obligor shall compose an annual report on the conducted internal control and measures taken following the control, by no later than 15 March of the current year for the prior year, and submit it to the NBS, at its request, within three days of receiving the request.

The obligor shall organise independent internal audit whose scope includes regular assessment of the adequacy, reliability and efficiency of the system of money laundering and terrorism financing risk management when the law governing the activity of the obligor prescribes the obligation of having independent internal audit, or when the obligor assesses that, given the size

and nature of activity, it is necessary to have independent internal audit within the meaning of the Law.

Composing the indicator list

51. The obligor shall develop a list of indicators for identifying persons and transactions in respect of which there are reasons to suspect money laundering or terrorism financing. When composing the indicator list, the obligor shall also enter the indicators developed by a competent authority, which are published on the Administration's website.

When establishing the reasons to suspect money laundering or terrorism financing, the obligor shall apply the indicator list and take into account other circumstances as well. It is particularly important that all employees be familiar with the indicators and apply them when executing transactions and/or before their execution, in accordance with the Law and these Guidelines.

Keeping records, protecting and keeping data in those records

52. The obligor shall keep records of the following data:

1) about customers and transactions in the amount of EUR 5,000 or more in the dinar equivalent;
2) submitted to the Administration (cash transactions in the amount of EUR 15,000 or more in the dinar equivalent and when there are reasons to suspect money laundering or terrorism financing in relation to a transaction or customer).

The contents of the data records in this Section are stipulated in Article 99 of the Law.

The obligor shall keep the data and documents about the customer and the performed risk analysis, as well as the executed transaction, for at least ten years after the day of the transaction.

The obligor shall keep data and documents about the compliance officer, the compliance officer's deputy, professional training of employees and the performed internal controls for at least five years after the day of the compliance officer's termination of duty, the performed professional training or the performed internal control. After the expiry of deadlines for keeping these data, the obligor shall handle them in accordance with the law governing personal data protection, on the condition these are not data used by competent government authorities for special purposes.

When the obligor submits data, information and documents to the Administration, this shall not be deemed as breaching the obligation of keeping a business, banking or professional secret.

The obligor shall undertake the necessary measures to protect the compliance officer and the employees implementing the provisions of the Law from any violent acts against their physical or psychological integrity.

The obligor or persons having access to data from Article 99 of the Law may not reveal the following to a customer or a third person:

– that data, information and documents about a customer or a transaction in respect of which there are reasons to suspect money laundering or terrorism financing, have been submitted or are being submitted to the Administration;

– that the Administration has issued an order to temporarily suspend the transaction;

– that the Administration has issued an order to monitor the customer's financial operations;

– that a procedure in relation to money laundering or terrorism financing has been or might be launched against a customer or a third party.