Pursuant to Article 6 paragraph 1. Article 104 paragraph 1 item 5) and Article 114 of the Law on the Prevention of Money Laundering and Terrorism Financing (*Official Gazette of the Republic of Serbia* Nos. 113/201 7, 91/2019 and 153/2020, hereinafter referred to as the “Law”), the Minister of Trade, Tourism and Telecommunications passes these

GUIDELINES

ON THE ASSESSMENT OF MONEY LAUNDERING AND TERRORISM FINANCING RISK BY REAL ESTATE AGENTS

The Ministry in charge of supervision in the field of trade (hereinafter referred to as the “Ministry”), as the body responsible for supervising compliance with the Law by real estate agents (hereinafter referred to as the “Obliged Entity”), is authorized to, independently or in collaboration with other authorities, pass guidelines on risk assessment and application of the provisions of the Law in respect of these obliged entities.

The Law adopts an approach based on analysis and assessment of the risk of money laundering and terrorism financing, which Obliged Entities are required to perform in respect of each client and each commercial relationship. The Law also introduces risk assessment at the level of the Obliged Entity.

Furthermore, the government has developed the national assessment of the risk of money laundering and terrorism financing and has specified the measures and activities that need to be put in place to mitigate the identified risks.

The results of the national risk assessment provide Obliged Entities with the required information and serve as the mandatory baseline for the risk assessments they will conduct themselves at the level of their activities as economic operators. Obliged Entities must understand and apply the risks assessed at the national level.

A Obliged Entity is a legal entity or sole trader providing real estate agent services in accordance with the Law on Real Estate Brokerage and Leasing (*Official Gazette of the Republic of Serbia* Nos. 95/2013, 41/2018 and 91/2019) and other regulations.

The Ministry, as the national authority responsible for supervising compliance with the Law by Obliged Entities (legal entities and sole traders providing real estate brokerage and leasing services), adopts the Guidelines on the Assessment of Money Laundering and Terrorism Financing Risk (hereinafter referred to as the “Guidelines”) to clarify the procedures an Obliged Entity is required to apply in order to comply with its legal obligations.

The aim of the Guidelines is to define the foundations and/or assumptions on the basis of which a the Obliged Entity should assess the risk of money laundering and terrorism financing in relation to its operations, as well as the manner of conducting risk assessments/analyses in each specific case, i.e. at the level of an entity with which a commercial relationship is established (a client, a business associate, a contracting party etc.), to ensure uniform application of the Law and put in place an effective anti-money laundering and counter-financing of terrorism system by the Obliged Entities. Obliged Entities are required to use these Guidelines when developing and applying procedures based on risk analysis and assessment, in order to establish an effective anti-money laundering and counter-financing of terrorism system.

The Guidelines aim to raise the awareness of Obliged Entity on their role and place in the anti-money laundering and counter-financing of terrorism system and highlight the importance of compliance with all laws and secondary legislation in this area, because it is the only way to effectively counter money laundering and terrorism financing. Obliged Entities under the Law are not expected to determine whether the criminal offence of money laundering or terrorism financing has been committed. The primary goal is for the Obliged Entity gain access to all data required to know its clients’ operations, to assess whether certain behaviour patterns may be associated with a criminal offence and, if so, to what extent, and to undertake all measures in accordance with the Law and report suspicious activities. The Administration for the Prevention of Money Laundering (hereinafter referred to as the “Administration”) and investigation authorities will conduct further procedures in each specific case to determine whether a criminal offence exists or not.

The Obliged Entity is required to apply the General and Specific Sections of these Guidelines to ensure a consistent course of action when assessing risks. The economic operator/Obliged Entity, regardless of its size and complexity, is required to establish an appropriate money laundering and terrorism financing risk management system. Such system must enable comprehensive identification, assessment, monitoring, mitigation and management of risks. Obliged Entities may apply such measures to varying extents, depending on the type and level of risk and according to different risk factors.

Those in charge of developing and conducting the money laundering and terrorism financing risk assessment may gain further experience if they consult other printed materials, guidelines and publications issued by the relevant national and international institutions, including:

* The Ministry of Trade, Tourism and Telecommunications, www.nut.gov.rs
* The Ministry of Finance, www.mfn.gov.rs - the National Bank of Serbia, www.nbs.rs
* The Business Registers Agency, www.apr.gov.rs
* The Association of Serbian Banks, www.ubs-asb.com
* The Administration for the Prevention of Money Laundering, www.apml.gov.rs
* FATF www.fatf-gafl.org
* Moneyval www.coe.int/moneyval

**GENERAL SECTION**

# 1. **Money Laundering and Terrorism Financing** - *Concept*

Money laundering and terrorism financing are global phenomena with potential negative impact on the country’s economic, political, security and social structure. Consequences of money laundering and terrorism financing undermine the stability, transparency and effectiveness of the country’s financial system, cause economic disruption and instability and harm the country’s reputation and threaten its national security. The risks of money laundering and terrorism financing also arise as a result of omissions in the application of regulations, leaving the obliged entity significantly exposed to reputational risk if a supervisory authority imposes a fine on it.

Regarding money laundering, the initial assets always come from illegal activities, whereas in the case of terrorism financing the sources can be both legal and illegal. However, the main goal of persons engaging in terrorism financing is not necessarily to conceal the sources of their funding; instead, it is often to conceal the nature of the financed activity. when persons decide to invest money from legal activities in terrorism financing, it is more difficult to discover and trace the funds, because the transactions tend to involve lower amounts.

An effective anti-money laundering and counter-financing of terrorism system involves analysing the risk of money laundering and the risk of terrorism financing.

## 1.1. **Money Laundering** – *Definition and Phases*

Money laundering is the process of concealing the illegal origin of money or assets that are the proceeds of crime. Money laundering within the meaning of the Law is deemed to be:

1. conversion or transfer of property acquired through the commission of a criminal offence;
2. concealment or misrepresentation of the true nature, source, location, movement, disposition, ownership of or rights with respect to the property acquired through the commission of a criminal offence;
3. acquisition, possession or use of property acquired through the commission of a criminal offence.

Any of the above activities committed outside of the territory of the Republic of Serbia is also deemed to constitute money laundering.

Money laundering includes numerous activities undertaken to conceal the origin of the proceeds of crime. The process of money laundering may involve a number of transactions in both informal and formal sectors, with proceeds of crime as the input and “legitimate” goods and services as the output of such transactions.

Anyone who provides services or supplies certain products can be abused as an instrument in the process of money laundering. Money may be laundered through operations in the financial or non-financial sectors. When proceeds are acquired through the commission of a criminal offence, the perpetrator attempts to find a way to use the money in ways which will not attract the attention of the authorities. He/she will therefore undertake a number of transactions intended to create an impression of legitimately obtained money.

Money laundering comprises three main phases:

1. The first phase: “**placement**” is breaking of the direct link between the money and the illegal activity by which it was obtained. It serves to introduce illegally obtained money into the financial system. money is paid to bank accounts, usually under the guise of a legal activity where payment is made in cash. One way is to form a shell company, which carries out no business operations and instead serves solely for the purpose of placing “dirty” money or breaking down large amounts of money and its subsequent depositing to accounts in amounts which are not suspicious and are not subject to reporting to the competent authorities.

1. The second phase: “**layering**” or “concealment”. Once money has entered the legal financial system, it is moved around from the account to which it was deposited to other corporate accounts, to create the impression of a business activity or conduct a legal operation (trade or service provision) with companies that operate legally. The main goal of such transactions is to conceal the link between the money and the criminal activity from which it originatewd.
2. The third phase: “**integration**”, where “dirty” money emerges as money earned from a legal activity. a frequent method of integration of “dirty” money into the legal financial system is the purchase of real estate or the purchase of controlling stakes in joint-stock companies, which is an example of large-scale concentration of “dirty” money, and this is in fact the goal of money “launderers”. Integration focuses on marketable commodities, i.e. items that can be bought and sold. Leasing of real estate is a legal operation and lease revenue is not suspicious. Money is also often invested in companies facing business difficulties, which then continue operating successfully, while their profits constitute legitimate income. Once money has reached this phase, it is very difficult to discover its illegal origin.

Illegal acquiring of asset is the main, but not the only motivation for the organised commission of criminal offences. In order to enjoy the proceeds of crime, they must be misrepresented as legally obtained assets.

## 1.2. **Terrorism Financing** – *Definition and Phases*

Within the meaning of the Law, terrorism financing means the providing or collecting of assets, or an attempt to do so, with the intention of using it, or in the knowledge that it may be used, in full or in part:

1. in order to carry out a terrorist act;
2. by terrorists;
3. by terrorist organisations.

Terrorism financing also means aiding and abetting in the provision and collection of assets, regardless of whether a terrorist act was committed or whether property was used for the commission of the terrorist act; the primary goal is not necessarily to conceal the source of the funds, but rather to conceal the nature of the activity which will be financed with those funds. There are four phases in the process of terrorism financing:

1. **Collecting** funds from legal operations or from criminal activities (e.g. donations, drug trafficking, extortion, embezzlement etc.);
2. **Keeping** or **holding** the collected funds (on accounts, either directly or on intermediary accounts);
3. **Transmitting** the collected funds to terrorists in order to use the money for terrorist acts (via money transfer systems or banking systems or using informal means of transmission);
4. **Using** the funds to purchase explosives, weapons and equipment, finance training camps, propaganda, political support, providing refuge etc.

## 1.3. **Suspicious Transaction** - *Concept*

A transaction may be flagged as suspicious if the obliged entity and/or the competent body believes there are reasonable grounds to suspect the transaction or the person executing the transaction of being involved in money laundering or terrorism financing or to suspect that the transaction involves the proceeds of illegal activities.

Transactions may also be treated as suspicious if they are unusual by their nature, scope, complexity, value or relatedness or have no clearly visible economic or legal rationale or are disproportionate to the client’s normal or expected operations, as well as other circumstances concerning the client’s status or other characteristics.

Both specific transactions carried out by clients and business relationships may be treated as suspicious. The assessment of the level of suspicion of a specific client, transaction or business relationship is based on the suspicion criteria set forth in the list of indicators (the Indicators Directive) for the identification of persons and transactions suspected of money laundering or terrorism financing. The indicator lists provide a baseline for the Obliged Entity’s employees and AML/CFT officers when identifying suspicious circumstances concerning a client, a transaction executed by a client or a business relationship entered into by a client; therefore, the Obliged Entity’s employees must be familiar with the indicators, so they could use them in their work. When assessing a suspicious transaction, the AML/CFT officer of the Obliged Entity mst provide the employees with any technical assistance they may require.

2. **Risk Assessment** – *Concept of Risk, Risk Assessment, Threat, Vulnerability and Consequences*

Risk assessment is the product resulting from or the process carried out on the basis of the methodology designed to determine, analyse and understand the risks of money laundering and terrorism financing and is the first step in their mitigation. Ideally, a risk assessment should include an assessment of threats, vulnerabilities (weaknesses) and consequences.

A **threat** is a person or group of persons, an object or an activity with the potential to cause harm (e.g. to the state, the society, the economy etc.) In the context of money laundering and terrorism financing, it includes persons engaging in criminal activity, terrorist groups and their abettors, the assets and property in the widest sense they have access to, as well as any part, current and future money laundering and terrorism financing activities (e.g. with obliged entities susceptible to harm to the institution, business or reputation, these could be clients identified or suspected of being connected to illegal activities, identified frauds, forged documents etc.).

**Vulnerability**, in the sense in which it used in risk assessment, includes all activities that could be exploited if a threat materialises. The focus is on those activities that are identified as weaknesses in the anti-money laundering and counter-financing of terrorism system and the control system. With regard to an obliged entity, a vulnerability is anything that makes it particularly susceptible to money laundering or terrorism financing (*e.g. a particular service provided by the obliged entity that has been identified as high risk at the national level, insufficient knowledge of the regulations governing this field, inadequate application of legislative provisions etc.*).

**Consequence** refers to the harm money laundering or terrorism financing may cause and includes illegal or terrorist activities and includes the impact of the underlying illegal or terrorist activity on financial systems and institutions, as well as more generally on the society and the economy as a whole. By the nature of their effects, consequences may be short-term or long-term and they affect the reputation and attractiveness of a country’s financial and non-financial sectors.

Regarding **risk assessment**, it should be noted that it covers inherent and residual risk. Inherent risk is the result of sector-specific threats and vulnerabilities. The level of this risk is impacted by various factors, in particular the quality and effectiveness of the repression measures applied by the competent authorities. These factors may mitigate the risk, if there is consistent and effective implementation of the law, developed supervision appropriate capacity etc., which ultimately result in lower residual risk. Lower residual risk (e.g. from the viewpoint of the obliged entity) can be brought about by a range of control mechanisms that contribute to lower risk of a specific product, service, business practice or the way in which a specific product or service is delivered.

Risk assessment is carried out at the level of:

1. The state (national risk assessment);
2. The obliged entity, and
3. Business relationship (client).

Obliged Entities are required under the Law to take into account the National Risk Assessment when performing risk analysis at the level of the obliged entity and risk analysis concerning their entire operations (*the so-called risk self-assessment*), as well as when performing risk analysis at the level of a business relationship (client).

While the process of risk assessment may be divided into a number of activities, its main stages are the following:

1. Risk identification
2. Risk analysis,
3. Risk evaluation and management.

When performing a risk analysis at the level of the Obliged Entity, i.e. a risk analysis concerning its entire operations, the Obliged Entity is required to take into consideration the threat level and the relevant sectoral vulnerability according to the results of the National Risk Assessment; furthermore, if a client is also an obliged entity under the Law, when performing a risk analysis at the level of the business relationship (client), the Obliged Entity is also required to take into consideration the threat level and the relevant sectoral vulnerability for the sector in which the client operates.

In particular, when performing a risk analysis at the level of the Obliged Entity, it must also take into consideration the risk level of the obliged entity’s organisational form, as determined by the National Risk Assessment, while when performing a risk analysis at the level of a business relationship (client) the obliged entity must take into consideration the risk level during the term of the business relationship.

Furthermore, the Obliged Entity must perform its risk assessment in compliance with the Law and these Guidelines, using the Indicators Directive.

Namely, if a client is considered high risk under the Law (*e.g. if the client or its beneficial owner is a public official or a legal entity whose ownership structure includes an off-shore leal entity or if the client is not physically present during the establishment of the business relationship*), the obliged entity is required to categorise such client as one with a high risk of money laundering and terrorism financing and subject it to increased KYC measures and actions. Therefore, when a risk analysis is performed, such client must be categorised as high risk under the Law.

Furthermore, when performing a risk analysis, the Obliged Entity is required to perform it in accordance with the National Risk Assessment and the Guidelines published by the supervisory authority, i.e. its risk self-assessment must take into account the risk analysis criteria at the level of the Obliged Entity set forth in these Guidelines. When performing a risk analysis at the level of a business relationship (client), the Obliged Entity is required to take into account the risk analysis criteria at the business relationship (client) level, i.e. it is required to assess geographic risk, client risk, service risk and transaction risk, as per the criteria set forth in the Specific Section of these Guidelines.

## **2.1. National Assessment of the Risk of Money Laundering and Terrorism Financing**

The state is required to perform the national assessment of the risk of money laundering and terrorism financing and specify the measures and activities that should be undertaken to mitigate the identified risks. The results of the money laundering and terrorism financing risk assessment provide Obliged Entities with the required information and serve as the mandatory baseline for the risk assessments they will perform on their own at the level of each institution.

The national assessment of the risk of money laundering and terrorism financing identifies which sectors and actions in a country’s system that carry a potentially higher risk of money laundering and terrorism financing and which carry a lower risk, so the state could respond properly to the identified risks with a range of measures and activities and, according to the assessed risks, make appropriate decisions on resource allocation, with the aim of directing more efforts and resources towards high-risk areas.

At its session held on 30 September 2021, the Government of the Republic of Serbia passed the Resolution adopting the National Assessment of the Risk of Money Laundering and the National Assessment of the Risk of Terrorism Financing, the Assessment of the Risk of Money Laundering in the Digital Assets Sector and the Assessment of the Risk of Financing the Proliferation of Weapons of Mass Destruction.

The national risk assessments[[1]](#footnote-1) cover a period of three years, from 1 January 2018 to 31 December 2020. A novelty in the current national risk assessment cycle is that the Republic of Serbia has for the first time conducted a risk assessment of money laundering and terrorism financing in the digital assets sector and an assessment of risk of financing the proliferation of weapons of mass destructions.

In view of the current issues of financing the proliferation of weapons of mass destruction and digital assets, in addition to the updated national money laundering and terrorism financing risk assessments, the risks to which Serbia’s system is exposed in these two areas has been examined for the first time.

1. National Assessment of the Risk of Money Laundering (*performed according to World Bank methodology*);
2. National Assessment of the Risk of Terrorism Financing and Assessment of the Risk in the Non-Profit Sector (*performed according to World Bank methodology*);
3. Assessment of the Risk of Money Laundering in the Digital Assets Sector (*performed according to Council of Europe methodology*);
4. Assessment of the Risk of Financing the Proliferation of Weapons of Mass Destruction (*performed according to the methodology of the* RUSl Institute for Defence and Security Studies (*RUSI), using the Guide to Conducting a National Proliferation Financing Risk Assessment, in consultation with US and EU experts)*.

### **2.1.1. Results of the 2021 National Risk Assessment**

Based on an analysis of predicate criminal offences, a review of threats by sectors and cross-border threats, the overall assessment of money laundering is “medium”, with a “no change” tendency.

National vulnerability to money laundering has been assessed as “medium”, on the basis of an analysis of the state’s ability to defend against money laundering and an analysis of sectoral vulnerabilities.

The **national money laundering risk assessment** is the result of an assessment of money laundering threats and national vulnerability to money laundering. The analysis conducted to that end in respect of the Republic of Serbia has identified that **the level of comprehensive risk of money laundering is MEDIUM**.

# *2.1.1.1.* ***National money laundering threat assessment***

The data collected, protected and analysed to determine the frequency of predicate criminal offences indicate that, apart from property-related criminal offences, the most common criminal offences still include unauthorised production and circulation of narcotics referred to in Article 246 of the CC[[2]](#footnote-2), tax criminal offences, abuse of position of a responsible person referred to in Article 227 of the CC and the criminal offence abuse of office referred to in Article 359 of the CC, and criminal offences against legal transactions, including forging a document referred to in Article 355 of the CC and forging an official document referred to in Article 357 of the CC.

In the preparation of the 2021 National Risk Assessment, a list was made of 15 criminal offences that may be identified as predicate criminal offences, i.e. criminal offences that precede money laundering and through the commission of which the perpetrator directly or indirectly gains illegal proceeds – illegal assets that can subsequently be subject to money laundering, regardless whether the perpetrators are also being prosecuted for money laundering in connection with those criminal offences or not.

Predicate criminal offences associated with a high risk of money laundering include: abuse of position of a responsible person, tax criminal offences, unauthorised production and circulation of narcotics, abuse of office, illegal crossing of state border and criminal offences committed by organised criminal groups.

Predicate criminal offences with a medium risk of money laundering include fraud, forging (documents and official documents), human trafficking, mediation in prostitution, illicit trade and illicit storage of goods.

Criminal offences associated with a low risk of money laundering are other criminal offences. All other criminal offences are identified as offences with a low risk of money laundering, because the perpetrators of such criminal offences do not seek to “launder” illegally obtained proceeds by concealing their illegal origin; instead, they as a rule spend them on daily needs.

**A growing threat** with regard to money laundering is posed by **environmental criminal offences, smuggling of protected plants and animals and abuse of the farm industry**.

Based on the established criteria and analyses of the data collected, it has been determined that limited liability companies and sole traders are the forms of legal entities with a high risk of money laundering, while joint-stock companies and cooperatives carry a medium risk and other forms (limited partnerships and partnerships) carry a low risk. On the other hand, the legal form of registered farms has been identified as a growing threat.

The analysis of individual cases in which persons were prosecuted for the criminal offence money laundering has revealed that the perpetrators of this criminal offence are commonly persons who own registered farms, as well as natural persons who hold special-purpose accounts with commercial banks.

A majority of the predicate criminal offences were committed in the national jurisdiction, which is why the level of threat has been assessed as high.

The 2021 National Money Laundering and Terrorism Financing Risk Assessment included also an assessment of cross-border money laundering threats.

The assessment of cross-border money laundering threats covered 164 countries. On the basis of the conducted analyses, a list was made of 29 countries identified as relevant in terms of cross-border money laundering threats (with 11 countries identified as high risk for money laundering, 15 countries identified as medium risk and 3 countries identified as low risk).

Sectors that are most exposed to **high risk** of money laundering, include **the real estate sector** (*residential and commercial property developers, direct real estate purchases*), the sector of organisers of online games of chance and the banking sector.

These are followed by the accounting sector, as the sector exposed to a medium-high risk with a tendency towards high risk. Sector exposed to a medium-high risk of money laundering include exchange offices and casinos.

Sectors exposed to a medium risk of money laundering include real estate agents, attorneys, virtual asset service providers (hereinafter referred to as “VASPs”), the automobile sales sectors, postal service operators and factoring companies. Sectors associated with a medium risk level with a tendency towards medium-low risk include life insurance companies, while sectors with a medium-low risk level include the capital market sector, payment institutions and electronic money institutions, auditors and public notaries. Sectors with a low risk of money laundering include financial lease providers and voluntary pension funds.

|  |  |
| --- | --- |
| High | Real estate sector |
| Organisers of online games of chance |
| Banks |
| Medium-high/high | Accountants |
| Medium-high | Exchange offices |
| Casinos |
| Medium | Real estate agents |
| Attorneys |
| VASPs |
| Automobile sales |
| Postal service operators |
| Factoring companies |
| Medium/medium-low | Insurance companies |
| Capital market |
| Payment institutions and electronic money institutions |
| Auditors |
| Public notaries |
| Low | Financial lease providers |
| Voluntary pension funds |

# Table 1: Money laundering risk levels

Residential and non-residential property developers in the real estate sector[[3]](#footnote-3) and the automobile sales sector, although not obliged entities under the Law, were subject to the money laundering risk assessment. According to the results of the 2021 National Risk Assessment, the real estate sector is the most exposed to the risk of money laundering, while the automobile sales sector is exposed to a medium level of money laundering risk.

It is also noteworthy that the largest contributors to the financial segment of Serbia’s system are banks, whose balance sheet total accounts for approx. 90% of the balance sheet total of the entire financial sector, while insurance companies, lease companies and voluntary pension funds account for approx. 9%. Of all the sectors in the non-financial segment of the system, by far the largest market share is that of the real estate sector, followed by games of chance, attorneys, accountants, postal service operators, public notaries and auditors.



Figure 1: Money laundering risk assessment map

## 2.1.1.2. ***National Vulnerability to Money Laundering***

National vulnerability was analysed through strategic framework quality, comprehensiveness of the normative framework, effectiveness of compliance with the Law, the capacities, resources, independence and integrity of key participants in the prevention and repression system, effectiveness of internal and international cooperation and the level of financial integrity, formalisation of the national economy and other relevant parameters.

A comprehensive analysis of money laundering threats constitutes the first step of national money laundering risk assessment. In the light of the results of such analysis, national vulnerability should be examined and assessed, since risk is a function of threats and vulnerabilities. Thus, an assessment of national vulnerability to money laundering is the next step in the National Money Laundering Risk Assessment.

As already stated, **national vulnerability to money laundering** has been assessed as **medium**, based on an analysis of the state’s ability to defend against money laundering and an analysis of sectoral vulnerability.

2.1.1.2.1. ***Sectoral vulnerability***

As national vulnerability is determined both by the country’s ability to defend against money laundering and the vulnerability of specific sectors which may be abused for money laundering, the analysis covered the financial and non-financial segments of the system.

Serbia’s financial sector comprises the banking sector, the insurance sector[[4]](#footnote-4), financial lease providers, voluntary pension funds, other payment service providers and electronic money issuers – payment and electronic money institutions, capital market (broker-dealer companies, authorised banks, investment fund management companies and custody banks), authorised exchange offices and factoring companies.

In the financial segment of the system, the most vulnerable institutions are banks, payment institutions, the public postal service operator and electronic money institutions, followed by exchange offices, factoring companies and the capital market sector, and then life insurance companies, financial lease companies and voluntary pension funds.

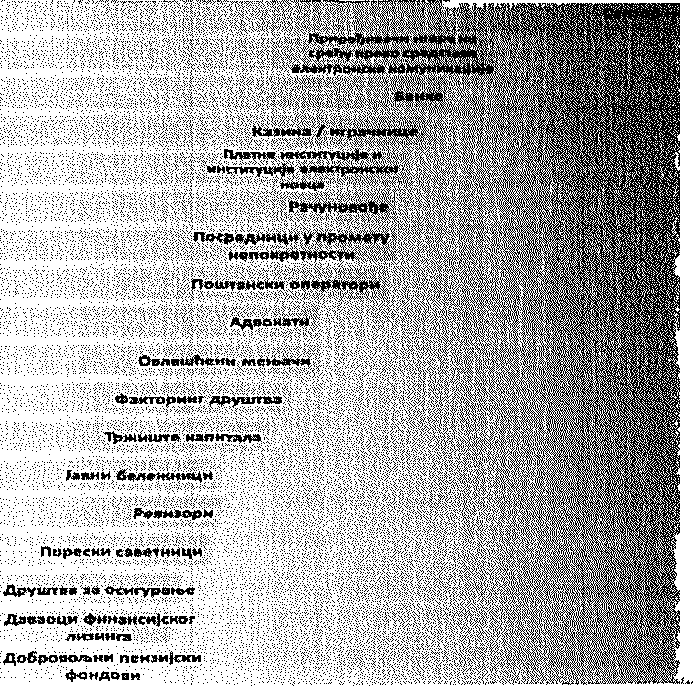


Figure 2: Table overview of vulnerability assessment by sectors

|  |  |
| --- | --- |
| Financial sector | Vulnerability |
| Banks | medium |
| Payment institutions, public postal service operator and electronic money issuers | medium |
| Exchange offices | medium-low |
| Factoring companies | medium-low |
| Capital market | medium-low |
| Life insurance | low |
| Financial lease providers | low |
| Voluntary pension funds | low |

Table 2: Overview of vulnerability assessment – financial sector

Serbia’s non-financial sector includes the following types of obliged entities under the Law: real estate agents, organisers of online games of chance, casinos and postal operators, as well as the so-called “gatekeepers”, including auditors, accountants, attorneys and public notaries.

Furthermore, the non-financial segment also includes residential and non-residential real estate developers and automobile dealerships, which are not obliged entities under this Law.

The most vulnerable sectors identified in the non-financial segment include the **real estate sector**, games of chance, accounting agencies and postal operators, followed by attorneys, public notaries and audit firms.

|  |  |
| --- | --- |
| Non-financial sector | Vulnerability |
| Real estate agents | medium |
| Organisers of special games of chance at gaming establishments (casinos) | medium |
| Organisers of special games of chance via means electronic communication (online) | medium |
| Accountants | medium |
| Postal service operators | medium |
| Attorneys | medium-low |
| Public notaries | medium-low |
| Audit firms | medium-low |

Table З: Overview of vulnerability assessment – non-financial sector

### *2.1.1.2.2.* ***Results of the 2021 National Money Laundering Risk Assessment regarding real estate agents***

**Real estate agents**, as Obliged Entities in the non-financial segment, **have been assessed to have a medium level of vulnerability, with medium exposure to the risk of money laundering**.

The results of the data obtained, their cross-referencing and analyses between the Ministry as the supervisory authority for the one part and the private sector for the other part, have produced a more comprehensive analysis of the state of play.

The 2018 National Risk Assessment separated real estate agents from real estate developers, as it was determined that these constituted two entirely different business activities, although parts of the same real estate sector. Real estate agents provide a service, while real estate developers produce and sell real estate across all stages of construction.

Supervision of real estate agents has revealed that their principals in 90% of the cases are persons selling/buying existing (used) real estate.

The number of economic operators registered with the Register of Real Estate Agents at 2020 year-end was 1278, which was a significant increase over the previous period. The Register of Real Estate Agents is publicly available on the Ministry’s website at www.mtt.gov.rs and all interested persons may access the data kept in the Register free of charge and without any restrictions. Real estate agents account for a mere 0.7% of total sales in the Republic of Serbia, which is indicative of the low awareness of this type of activity, although a mild increase has been observed over the previous period.

From 2018 to 2020, the normative framework was improved through the enactment of amendments to the Law on Real Estate Sale and Lease Brokerage, aimed at mitigating the risk of money laundering and financing of terrorism. Under the amendments to the Law, an entity applying for registration with the Register of Real Estate Agents must enclose a certificate of no criminal conviction issued by the competent public authority verifying that the applicant (founding member or owner, beneficial owner, associate, managing body member etc.). Another step to reduce vulnerability is the fact that the Ministry may demand of a real estate agent at any time to present proof of no criminal conviction. These amendments to the Law were made to ensure direct compliance with FATF recommendation 28, which concerns in particular preventing persons with a criminal background, specifically persons convicted of criminal offences and grave violations of anti-money laundering and counter-financing of terrorism regulations, from participating in the ownership and management structure.

Under the amendments to the Law, an Obliged Entity is to be expunged from the Register of Real Estate Agents if it no longer complies with the registration requirements. Accordingly, relevant secondary legislation was passed as well, including: the Bylaw on the Register of Real Estate Agents[[5]](#footnote-5), the Bylaw on the State Qualifying Examination for Real Estate Agents[[6]](#footnote-6), the Bylaw on the Commercial Space and Equipment of Real Estate Agents[[7]](#footnote-7) and the Bylaw on Records of Real Estate Sale and Lease Brokerage[[8]](#footnote-8), thus eliminating the risk of persons convicted of business crimes engaging in real estate sale and lease brokerage.

After amending these regulations, the Ministry passed the Directive on Issuing of Indicators for Recognising Cases of Suspected Money Laundering and Terrorism Financing[[9]](#footnote-9) by Obliged Entities and issued new Guidelines on Money Laundering and Terrorism Financing Risk Assessment[[10]](#footnote-10).

These regulations aim to instruct real estate agents how to implement an approach based on risk assessment, how to conduct and regularly update a risk analysis and how to effectively manage risk through the application of appropriate actions and measures aimed at detecting and countering money laundering and financing of terrorism.

The line Ministry had carried out direct and indirect supervision and preventive action (official advisory visits) through market inspectors.

The most common irregularities identified by inspection include failure to conduct a risk analysis in accordance with the Guidelines, which should be passed by the responsible body of the Obliged Entity, or failure to designate an AML/CFT officer and his/her deputy; failure to determine a client’s identity as required by law; insufficient cooperation with the Administration, usually by failing to comply with the duty to provide information on the personal name and name of the post of the AML/CFT officer and his/her deputy; and failure to compile an annual report on internal controls.

During the observed period, the Register of Real Estate Agents was updated through expunging of agents exclusively on the request of the Obliged Entity concerned and in case of expiry of the insurance policy, i.e. there have been no instances of expungement of real estate agents who had been found by inspection to be non-compliant with the anti-money laundering and counter-financing of terrorism legislation.

Professional qualifications of an Obliged Entity to perform real estate sale and lease brokerage operations is determined in a state qualifying examination, in accordance with the Bylaw on the State Qualifying Examination for Real Estate Agents.

A certificate of passed state qualifying examination issued to natural persons (agent) is a condition for legally engaging in real estate sale and lease brokerage operations, the primary goal of this arrangement being to strengthen legal certainty for customers by significantly reducing the possibilities of illegal pursuit of real estate sale and lease brokerage operations; another requirement is that a person taking the state qualifying examination must not be sentenced to imprisonment for a criminal offence in the future, whether in Serbia or in a foreign country.

To clarify the obligations imposed by the Law, the Ministry has cooperated with the Administration, the Chamber of Commerce and Industry of Serbia, the Real Estate Association and the Real Estate Cluster to organise and deliver 22 trainings in Serbia’s largest cities, while also conducting 156 official advisory visits to real estate agents.

However, even with all these efforts of the line Ministry, real estate agents have not been brought to comply with their statutory obligations as required by the law and report suspicious transactions to the Administration; indeed, the number of reported suspicious transactions during the observed period was negligible, which shows that these Obliged Entities still lack sufficient awareness and knowledge of the importance of these activities.

The vulnerability of real estate agents can be addressed and reduced in the coming period through intensified trainings, round tables and panels for the obliged entities, which would highlight the importance of and the need for stepping up compliance with those obligations and performance of those activities through case studies and clarifications of money laundering typologies in real estate sale and lease operations.

Obliged Entities and their employees have access to all information regarding money laundering typologies and all novelties concerning anti-money laundering and counter-financing of terrorism activities, which are posted on the Administration’s website.

2.1.2. ***Assessment of Terrorism Financing Risk*** *and Sectoral Risk Assessment for Non-profit Organisations*

а) The 2018-2020 **National Terrorism Financing Risk Assessment** is based on the assessed terrorism threat, the threat of terrorism financing at the national level, the sectoral risk of terrorism financing and the country’s vulnerability to terrorism financing.

The overall terrorism financing risk assessment for the Republic of Serbia is **MEDIUM LOW**, taking into account the following:

* The assessed threat of terrorism financing posed by terrorists and terrorist organisations is low;
* The assessed threat of terrorism financing at the national level is medium to low;
* The sectoral risk of terrorism financing is low;
* The country’s assessed vulnerability to terrorism financing is low.

As there were no criminal prosecutions during the observed period for the criminal offence of terrorism and other related criminal offences, including terrorism financing, the threat of terrorism financing is **low**.

The Republic of Serbia strongly condemns terrorism in all its forms, as well as all types of extremism and radicalism, fully aware that the complexity and transnational nature of these phenomena calls for coordinated efforts at the widest global front and for addressing all their aspects in order to provide a comprehensive response.

Regarding threats of terrorism financing, it is paramount to examine how the internal risks correlate with the external ones, given that the amounts involved in terrorism financing are disproportionate to the damage they may cause, whether through the perpetration of a terrorist act or through other activities executed by terrorists and their sympathisers.

Terrorism financing may have consequences for the system, unless all public authorities and institutions continue with their efforts to combat terrorism and its financing and there are no disruptions in the continuity of efforts to harmonise the normative framework with the recommendations of relevant international organisations tasked with combating terrorism and its financing. As the legislative framework governing this area is relatively sound, efforts should be focused more on defining the criteria and standards that would contribute to early detection an identification of such transactions, in full compliance with all principles of a democratic society.

Regarding terrorism financing, increased attention is required both of obliged entities, whose duty and interest it is to prevent the use of their systems to transfer assets intended for terrorism financing, and of the competent authorities, whose duty it is to prevent abuses and activities carried out by legal entities to collect funds for terrorism financing. Accordingly, to avert the consequences of terrorism financing, it is necessary to maintain the effective capacity of the system to combat terrorism and financing of terrorism, analyse the normative framework with regard to the effectiveness of certain legislative arrangements and their implementation, continually improve and upgrade human resources and renew technical capacities of the enforcement agencies (*police, prosecution offices, security services*) and the administration and prevention authorities (*different segments of the Ministry of Finance* - *Administration* *for the Prevention of Money Laundering*, *Customs Administration*, *Tax Administration*) to counter the financing of terrorism and raise awareness of the dangers of terrorism and all of its manifestations, as well as of the risk exposure of the so-called vulnerable categories of persons and organisations.

With regard to abuse for terrorism financing purposes, the sectoral risk assessment has revealed that the financial sector is more susceptible to abuse than the non-financial one. Sectoral analyses have shown that risk levels are not identical across all sectors, with the following sectors identified as the most susceptible to abuse for terrorism financing purposes:

* Electronic money issuers;
* Payment institutions;
* Public postal service operator;
* Authorised exchange offices;
* Digital asset service providers;
* Real estate agents; and
* Banks.



Figure З: Overview of sectoral risks

The Administration has cooperated with the “Mihajlo Pupin – Computing Systems” Institute to develop a Search Engine for the lists of persons subject to UN sanctions, the “flagged persons” (http://www.unsearch.apml.gov.rs/). This Search Engine enables all natural persons and legal entities to quickly and simply check whether they have contacts or business cooperation with this category of persons, in order to timely undertake the measures and actions provided for by the Law on the Freezing of Assets with the Aim of Preventing Terrorism and Proliferation of Weapons of Mass Destruction[[11]](#footnote-11).

# **b) Sectoral Risk Assessment for Non-profit Organisations**

The exposure of non-profit organisations to the risk of abuse for terrorism financing in the Republic of Serbia in 2018-2020 was low to medium, i.e. it was lower than in the period covered by the previous national risk assessment, which had been conducted in 2018.

During the reporting period, Obliged Entities reported no suspicious activities by associations with regard to suspected terrorism financing.

## *2.1.2.* ***Money laundering and terrorism financing risk assessment in the digital assets sector***

Persons providing the services of virtual currency purchase, sale or transfer or exchange of virtual currencies for cash or other assets using online platforms, physical devices or otherwise or persons acting as intermediaries in the provision of these services have been included among the obliged entities under the Law. Accordingly, a separate law has been passed to govern the digital assets market and the procedure for licensing and supervising the providers of digital asset services (the supervision is carried out by the National Bank of Serbia and the Securities Commission).

In the Republic of Serbia, digital assets services may be provided solely by a company headquartered in the Republic of Serbia and licensed to provide digital assets services. All obliged entities under the Law, as well as the general public, have access to the register of licensed VASPs in the Republic of Serbia, which is available on the website of the National Bank of Serbia. Thus, financial institutions and other obliged entities under the Law have no difficulties when identifying VASPs that are authorised/unauthorised to provide digital assets services.

Due to the numerous regulatory restrictions, as well as the materiality of the digital assets sector in the Republic of Serbia, it has been assessed that virtual currency transactions are associated with **medium risk** of money laundering and terrorism financing, while investment and user tokens carry a **low risk**.

As regards VASPs, the risk level has been assessed as **MEDIUM** due to regulations which are more stringent than the global standards of anti-money laundering and counter-financing of terrorism, the materiality of this sector and the fact that most banks in the Republic of Serbia have disabled cross-border transactions involving digital assets.

## *2.1.3.* ***National Assessment of the Risk of Financing the Proliferation of Weapons of Mass Destruction (WMD)***

A high level of threat of WMD proliferation exists when opaque entities and corporations are used to support WMD proliferation or when “shell corporations” do so on behalf of persons under the sanction regimes of the UN and the international organisations of which the Republic of Serbia is a member.

The National Proliferation Risk Assessment is a strategic document which presents an analysis of the current situation in the country in order to identify potential risks of WMD proliferation financing, so the state could timely recognise threats and vulnerabilities in this regard, with the aim of focusing the country’s resources on those activities that may help to at least mitigate, if not eliminate, certain risks.

# *2.1.3.1.* ***Serbia’s security environment and risks determining its geopolitical position***

Serbia, as a responsible UN and OSCE member state committed to strengthening regional and international peace and security, makes efforts to prevent WMD proliferation in our country using all available mechanisms, including arms control and disarmament.

The most significant trends which, according to most serious international analytical institutes, influence the outlook of international security and potential WMD proliferation, include: continual increase in military spending, chronic crisis of the arms control system, growing serious global and regional geopolitical rivalries, numerous armed conflicts around the world, as well as activities of various non-state actors and terrorist groups, which seek to achieve their goals by violent means.

## *2.1.3.2.* ***States under UNSC sanctions***

The following member states are currently under the UN sanctions system: Central African Republic (2013), Guinea-Bissau (2012), DR Congo (2003), Iran (2006), Iraq (2004), Lebanon (2006), Sudan/Darfur (2006), Mali (2017), Libya (2011), DPR Korea (2006), Somalia (1992), Yemen (2015) and South Sudan (2015), as well as Afghanistan/the Taliban and Al-Qaeda, on the individuals list (2002).

# *2.1.3.3.* ***Non-state actors as a threat - Terrorism***

The development of modern communication and information technologies has increased the risk of their abuse by terrorists, not only for communication, financing, propaganda, recruitment or terrorist training, but also for cyberterrorist attacks, where information resources are the means, rather than the object of the attack. An additional threat with regard to terrorism financing is the proliferation of weapons of mass destruction and illegal trafficking in all kinds of weapons, since this increases the risk of weapons, including WMD, falling into the hands of structures over which the state has no control, including in particular terrorist groups and individuals.



According to this assessment, threats of WMD proliferation financing may be recognised using the indicators associated with the risk of abuse of:

* Shell corporations;
* Off-shore corporations and complex ownership structures;
* Foreign politically exposed persons;
* Re-export of transactions;
* Forged official documents and documentation etc.

# *2.1.3.4.* ***International and national legal framework***

The Republic of Serbia continually complies with its obligations arising from UNSCR 1540 to prevent the proliferation of WMD and their means of delivery (reaffirmed by UNSCR 2572 of 2021). State authorities have undertaken a number of activities; at the national level, the Strategy for the Prevention of Proliferation of Weapons of Mass Destruction of the Republic of Serbia 2021-2025 was adopted and Instructions on Application of the Law on the Freezing of Assets with the Aim of Preventing Terrorism and Proliferation of Weapons of Mass Destruction were passed, which concern prevention of financing WMD proliferation. The latter aims not only to raise public awareness of the importance of taking preventive actions and measures to identify, detect and prevent financing of WMD proliferation, but also to help the obliged entities under the Law, as well as the supervisory authorities, in establishing appropriate policies and procedures necessary to apply its provisions.

Following a comprehensive analysis of relevant factors, the national risk of WMD proliferation financing has been assessed as **low to medium**.

A higher degree of threat is associated with trading with high-risk countries, where the risk of potential redirection of goods is particularly relevant. This aspect is a continual threat and, in this context, additional checks under the export regime and regular exchange of information are activities that must be continued.

## *2.1.4.* ***Consequences for the System***

Apart from the assessed threats and vulnerabilities, the national money laundering and terrorism financing risk assessment also took into account the assessed consequences for the system. These should be understood as the **harm** money laundering might cause and include the impact of criminal activity on the obliged entity, the financial system, the society and the economy as a whole.

Given that the assessed level of threats and vulnerabilities is **medium**, the **consequences** for the system should have the same ranking. The “path” of dirty money is not easy to identify and recognise, which certainly makes it harder to timely undertake effective measures to detect, prevent and counter it.

New forms of money laundering emerge on a daily basis, as money launderers resort to different methods and means. The largest and gravest adverse effects of money laundering are evident in particular in the economic sphere, through reduced government revenue, transparency and efficiency of the financial system and increased informal economy; at this point, Serbia’s track record in this regard is not sufficiently low, so any increase is bound to trigger negative effects throughout the entire economic and financial system.

Money laundering, as a rule, leads to lower budget revenues as a result of tax avoidance. This is one of the most common types of illegal income subject to money laundering. Such situations often further deteriorate the tax system, as they trigger an increase in tax rates and tax burden for those entities that pay their liabilities. All this puts them at a competitive disadvantage and makes their business operations more difficult.

# *2.1.4.1.* ***Consequences for real estate agents***

Real estate sale and lease operations provide a major avenue for criminal structures to introduce the proceeds of crime into legal flows. Using real estate sale and lease services creates scope for concealing and covering the trace of illegal money, while agents may be abused to that end through a quick, efficient real estate transaction, often with an unrealistically high or low value. When they provide also other services (*real estate appraisal, obtaining of documentation pertaining to a property, real estate supply and demand analysis in a given territory or area, real estate price analysis for a given area etc.*), real estate agents can be an attractive target for “Money launderers”, who may pay for such services using dirty money (*cash or electronic currency etc.*).

Real estate sale and lease brokerage operations that are of greatest interest to “money launderers” include:

1. Financial or other advisory services – criminals may pose as individuals seeking financial or other advice how to put their assets outside the reach of others, to avoid future liabilities;
2. Purchase or sale of real estate – criminals may exploit asset transfers as a cover for transferring illegal funds (layering phase) or as the final investment of those proceeds after they have gone through the laundering process (integration phase);
3. Executing financial transactions – criminals may use real estate agents to execute or facilitate various financial operations on their behalf;
4. Introduction to financial institutions – criminals may use agents as someone to represent them vis-à-vis an institution. The same is also true *vice versa*, i.e. criminals may use financial institutions to introduce them to agents.

Services considered particularly vulnerable include:

a) Commercial space lease services

Criminals may seek opportunities to retain control of illegal proceeds, while also making it more difficult for law enforcement to trace the origin and ownership of their assets. Leasing commercial space on an attractive location may be a handy tool for achieving this aim, i.e. for “laundering” dirty money, because it creates an impression of being used for legal operations and in the normal course of business, since it exists for years on the same location.

b) |Other services

Criminals may also abuse other real estate sale and lease services provided by agents to create an impression of genuine interest in property or location, in order to conceal the source of the funds used in the transaction (*e.g. the real estate agent may provide such service and charge it in cash, which comes from an unknown source*).

# 2.1.4.2. ***Risk-based approach***

The risk of money laundering and terrorism financing is the risk of negative effects for the financial result, capital or reputation of the Obliged Entity stemming from the use of the Obliged Entity (*direct or indirect use of a business relationship, transaction or service*) for money laundering and/or terrorism financing purposes.

The risk of money laundering and terrorism financing arises in particular as a failure of the obliged entity to bring its operations in compliance with the Law, the regulations and the internal bylaws on anti-money laundering and counter-financing of terrorism, i.e. as a consequence of incompatibility of internal bylaws governing the course of action to be taken by the obliged entity and its employees to counter money laundering and terrorism financing.

Money laundering and terrorism financing are real and serious issues which Obliged Entities must face, to avoid actually encouraging it, whether inadvertently or otherwise.

Obliged Entities need to adopt a risk-based approach in order to identify, assess and understand the risks of money laundering and terrorism financing, so they could direct their resources where the risks are greatest and thus put in place appropriate risk mitigation measures.

Key elements of a risk-based approach:

|  |  |
| --- | --- |
| **Risk identification and assessment** | Identification of money laundering and terrorism financing risks faced by the obliged entity, taking into account its clients, services and countries of operation, and also taking into account publicly available information on money laundering and terrorism financing risks and typologies |
| **Risk administration and mitigation** | Identification and application of measures for efficient and effective management of money laundering and terrorism financing risk |
| **Continual monitoring** | Defining of policies and procedures to monitor changes in money laundering and terrorism financing risk |
| **Documentation** | Documenting risk assessments, and policies and procedures to monitor, manage and mitigate money laundering and terrorism financing risk |

Table 4: Elements of a risk-based approach

2.1.4.2.1. *IDENTIFICATION – risk recognition*

Identification begins with risk recognition. It would be beneficial if the Obliged Entity could make a list of potential factors which will be used to recognise the threats of and vulnerabilities to money laundering and terrorism financing within the Obliged Entity. The list should include all risk factors identified at the national level which are characteristic of the Obliged Entity concerned, the typologies identified in cases of money laundering or terrorism financing, trends and any circumstances which the supervisory authority found to be insufficiently addressed with regard to compliance with the Law (*e.g. if companies from a specific region are identified at the national level as risky, and in particular if transactions with such entities are recognised as risky, whether the obliged entity identified such entities as risky, how it assessed them in the past, whether there had been any instances of abuse by such clients that had not been observed in time and why, for example, transactions carried out by such clients were not identified as risky in terms of money laundering at the time. Other factors to consider include whether situations had been identified at the level of the Obliged Entity where an entity that was subsequently under an investigation had been a client of the Obliged Entity, but had not been flagged as risky, and whether the Obliged Entity could have had access to such information or not*).

After compiling a comprehensive and broad list, the Obliged Entity may examine which of the specific factors are not sufficiently relevant for the Obliged Entity, or determine that it does not offer a specific product identified as risky at the national level or that certain behaviour patterns are not characteristic of the Obliged Entity. Accordingly, the Obliged Entity may remove certain items from the list; however, if it recognised in the past certain behaviour patterns or circumstances that proved to be risky with regard to the Obliged Entity concerned, those should certainly be included in the list and analysed separately.

At this stage it is impossible to tell with certainty whether any specific factor bears a higher or lower level of risk; rather, this stage is about whether a given factor is sufficiently relevant to merit an assessment of money laundering or terrorism financing risk (*e.g. Obliged Entities may adopt different approaches, so that one Obliged Entity may opt to start from certain behaviour patterns, indicators and trends and build on certain assessments at the national level, and then analyse to what extent those assessments were characteristic of the Obliged Entity itself, whereas another Obliged Entity may choose not to start from assessment models at the national levels and opt for identifying at-risk services and transactions and then build on these initial assessments, using specific typologies that have been identified e.g. in relation to certain services or certain executed transactions, while of course taking into consideration also the results of the national risk assessment*).

There is no universal risk assessment template. While there are certain guidelines, ideas and suggestions based on national and international practice, it is up to the Obliged Entity to determine which methodology best suits its business (*e.g. factors relevant for inclusion in the list include: the type of identified past criminal offences which were definitely committed or are suspected to have been committed, i.e. whether clients are associated with illegal activities (the media, interviews etc.), transfers to high-risk countries, transfers from high-risk countries, the amount of cash transactions, the amount of suspicious activity reports, legislation, legislative compliance, number of clients, the share of corporate clients, the share of individual clients, the results of supervision, the results of supervision of the obliged entity, the results of supervision carried out at the level of the specific sector, the number of suspicious activity reports, feedback on suspicious activity reports, the system in which the obliged entity operates, obtaining of an operating licence, set-up procedure, communication with state authorities, impact of group procedures on the operations of the obliged entity, all products covered by the national risk assessment, all services covered by the national risk assessment, trends identified in the national risk assessments, methods of money laundering or terrorism financing identified in the national risk assessment, types of companies etc.*).

The Obliged Entity may assess the risk of money laundering differently from the risk of terrorism financing. Clients whose operations largely involve cash transactions must be subject to particular scrutiny by the obliged entity due to the risk of terrorism financing. In this context, particular attention should be paid to the operations of non-profit organisations, because they provide ample possibilities for abuse in terms of terrorism financing. Geographic risk with regard to terrorism financing is particularly high in those regions where, according to data provided by relevant international organisations, such as the UN, terrorists carry out their activities.

2.1.4.2.2. RISK CATEGORIES

Identification of risk categories is the first step in risk analysis, both for the Obliged Entity and for the client. It should be noted that risk categories may differ depending on specific features of the obliged entity’s operations, and each obliged entity should take into account risk categories that correspond to its scope of operations.

Under the Law, obliged entities are required to conduct a risk analysis proportionate to the nature and scope of their operations, which must take into account **the main types of risks (client risk, geographic risk, transaction risk and service risk)**, as well as other types of risks identified by the obliged entity as additional risk categories taking into account the specific nature of its operations; in addition to the above risk categories, the obliged entity may also set forth appropriate actions and measures provided for by the law in respect of those additional risk categories.

## *2.1.4.2.2.1.* ***Geographic risk***

Geographic risk is the risk determined by the geographic region of the country of origin of a client, its owner or majority founding member, beneficial owner or a person who otherwise controls the client’s operations, or the country of origin of a person executing a transaction with the client.

Geographic risk assessment and evaluation depends on the location of the obliged entity, i.e. its organisational units. (For example, the risk assessment of obliged entities situated in areas visited by expats or tourists and in border areas will be different from that of obliged entities situated in rural areas, where everyone knows each other an businesses know their clients).

clients from the same region as the Obliged Entity are less risky than clients with whom we have no business relations and who are established/reside outside of the region.

*2.1.4.2.2.2.* ***Client risk***

In order to identify client risk, including the client’s beneficial owner, the Obliged Entity should consider the risks associated with the manner of operation and the type of professional activity, reputation, ownership and organisational structure, as well as the client’s conduct in connection with the business relationship or transaction.

The obliged entity is required to identify this risk independently, by applying a client risk-based approach, governed by the generally accepted principles and its own experience.

Client risk involves an assessment to determine whether a client with which the obliged entity cooperates is associated with increased risk of money laundering and terrorism financing.

Client risk assessments are to be conducted not only when a business relationship with a client is established, but also throughout that entire relationship, during which time the risk level may change (*e.g., a business relationship with a client may initially be assessed as low risk, but circumstances may subsequently arise that would increase the risk, or vice versa*). This does not apply to cases which are categorised as high risk under the Law and which must be subject to increased customer due diligence actions and measures (*e.g. when the client is a public official, when the client is not physically present for identification and identity verification, when the client or a legal entity in its ownership structure is an off-shore legal entity, when establishing a business relationship or executing a transaction with a client established in a country with strategic deficiencies in its anti-money laundering and counter-financing of terrorism system*).

## *2.1.4.2.2.3.* ***Transaction risk***

When determining and assessing this risk, the Obliged Entity shall determine and assess in respect of each business relationship the type of property offered by the client in the execution of such business relationship, the way in which such property is placed in the business relationship, how it is transferred etc., taking into account that, under the Law:

1. transaction means the acceptance, provision, conversion, keeping, disposition or other dealing with property by the obliged entity, including the payment transaction within the meaning of the law governing the provision of payment services.
2. property means things, money, rights, digital assets, securities, and other documents in any form which can be used as evidence of ownership or other rights;
3. money means cash (domestic or foreign), funds in accounts (RSD or foreign currency) and electronic money;
4. bearer negotiable instruments means cash, cheques, promissory notes, and other bearer negotiable instruments that are in bearer form;

When determining and assessing this risk, the Obliged Entity shall also take into account the following:

1. The risk of cash transactions (*physical receiving or giving of cash*), since Article 46 of the Law prohibits the receipt of cash from clients as payment for sold or leased real estate or for a provided service in amounts of EUR 10,000 or more in dinar equivalent.
2. The risk of unusual transactions (*transactions departing from the client’s usual operations with the obliged entity*), which usually involve unusual demands by the client to execute the business relationship using new technologies or virtual currencies (*digital representations of value and not issued and backed by a central bank or another public authority, which are not necessarily linked to a legal tender and do not have the legal status of money or currency, but are accepted by natural persons or legal entities as a medium of exchange and can be bought, sold, exchanged, transferred and stored electronically*).

*2.1.4.2.2.4.* ***Service risk***

Service risk is the business risk associated with the core service, including real estate purchase, sale, lease and letting, as well as other, less risky real estate services, such as the service of property appraisal and integration of the entire set of documents when executing a sale agreement, real estate market research etc.

Purchase involves an obligation for the buyer to pay the price of the property specified in the agreement and take possession of the property within a specified period.

Sale is the transfer of title and delivery of possession of the sold property against consideration, i.e. against payment of the cost of the item specified in the agreement.

Lease is the enjoyment and use of a property under an agreement, against lease payments, and its use until a specified date, with the care of a good steward.

Letting is the delivery of a property for use under an agreement to a tenant in usable condition for a specified lease term, together with all fixtures and fittings, against specified consideration.

*2.1.4.2.3. RISK ANALYSIS*

Risk analysis comprises:

1. Risk analysis regarding the Obliged Entity’s overall operations,
2. Risk analysis for each group or type of client or business relationship or service provided as part of its operations or transaction.

*2.1.4.2.3.1.* ***Risk analysis (assessment) at the level of the Obliged Entity (risk self-assessment)***

In the process of conducting a risk analysis pertaining to its overall operations, the Obliged Entity estimates the likelihood of its business being exploited for money laundering and terrorism financing purposes. The risk analysis pertaining to overall operations aims to identify the Obliged Entity’s exposure to the risk of money laundering and terrorism financing and the segments that should be prioritised when taking action to effectively manage this type of risk.

The Obliged Entity is required to conduct a risk assessment at the level of the Obliged Entity (risk self-assessment) once a year, **by the 31st of March each year in respect of the preceding year**, on the basis of an analysis of the self-assessment criteria set forth below.

A prerequisite for conducting a risk analysis at the level of the Obliged Entity is a completed risk analysis of all clients with which the Obliged Entity has established business relationships. Apart from the results of the National Risk Assessment and the imperative legislative provisions, such assessment should cover geographic risk, client risk, service risk and transaction risk, the assessment criteria for which are provided in the Specific Section of these Guidelines.

When conducting a risk assessment at the level of the Obliged Entity, the Obliged Entity is required to take into account at least:

1. The results of the National Risk Assessment, i.e. the risk of threats and the sectoral vulnerability. According to the results of the 2021 National Risk Assessment, the sector of real estate agents has medium vulnerability and medium exposure to money laundering threats. Furthermore, when conducting a risk self-assessment, the Obliged Entity should also take into account the risk level associated with its own legal form, based on the National Risk Assessment results provided below;
2. Whether there are any products or services offered by the Obliged Entity in its operations that could be abused;
3. The size of the Obliged Entity, whether it has a complex ownership structure, the number of its employees who are directly in charge of anti-money laundering and counter-financing of terrorism tasks relative to the total number of employees, the number of employees who are in direct contact with clients, the manner in which tasks and responsibilities are organised, the rate of staff turnover, the quality of training etc.;
4. The total number of clients;
5. The number of clients with a complex ownership structure;
6. The number of clients broken down by different legal forms – according to the results of the 2021 National Risk Assessment, limited liability companies and sole traders are the forms of legal entities with a high risk of money laundering, while joint-stock companies and cooperatives carry a medium risk and other forms (limited partnerships and partnerships) carry a low risk. On the other hand, the legal form of registered farms has been identified as a growing threat, because there is little to no control of the cash flows with these entities and it has been observed that organised criminal groups tend to exploit them for money laundering.
7. In addition, according to the results of the 2021 National Risk Assessment, exposure of non-profit organisations to abuse for terrorism financing purposes has been identified as low to medium;
8. An assessment of the Obliged Entity’s exposure to cross-border threats (the number of resident clients vs. the number of non-resident clients, the number of clients whose beneficial owners are Serbian nationals vs. the number of clients whose beneficial owners are foreign nationals and, if there are foreign nationals among the beneficial owners, information on their countries of origin);
9. The risk levels of its clients (the number of clients assigned to low, medium and high risk categories, focusing in particular on the number of off-shore legal entities, public official and clients who were not physically present during the establishment of the business relationship);
10. The number of clients with suspicious activities/transactions;
11. The number of suspicious activities/transactions identified in internal reports, and
12. The number of suspicious transactions reported to the Administration.

Based on the above criteria, as well as the measures it has undertaken to mitigate the risk of money laundering and terrorism financing, the Obliged Entity assesses its own overall exposure to the risk of money laundering and terrorism financing as low risk, medium risk or high risk.

Obliged Entities are not expected to determine whether a criminal offence of money laundering or terrorism financing has been committed.

The primary task of Obliged Entities is to ensure availability of all necessary customer due diligence information, to estimate whether certain patterns of behaviour can be associated with a criminal offence and, if so, to what extent, and to undertake all necessary measures in accordance with the Law and report suspicious activities, while the Administration for the Prevention of Money Laundering and law enforcement agencies will conduct further procedures in each case in order to determine whether a criminal offence has been committed or not.

*2.1.4.2.3.2.* ***Risk analysis (assessment) at business relationship (client) level***

The Obliged Entity is required to conduct a risk assessment at business relationship (client) level taking into account the following:

# **The results of the National Risk Assessment** (*if a client is an obliged entity under the Law, the obliged entity is required to take into account the threat level and the sectoral vulnerability of the client’s respective sector, as well as the risk level of the client’s legal form, regardless whether the client is an obliged entity under the Law or not*);

1. **Imperative provisions of the Law** (*the Law sets forth cases where the obliged entity si required to categorise a client as high risk and apply increased actions and measures*);
2. **Guidelines issued by the Ministry** (*geographic risk, client risk, service risk and transaction risk, the criteria of which are set forth in the Specific Section of these Guidelines*).

Based on the risk assessments conducted for each group or type of clients or business relationships, the services provided by the obliged entity as part of its business operations and the relevant transactions and risks identified at the national level, the obliged entity is required under the Law to categorise the client into one of the following risk categories:

* **Low risk** of money laundering and terrorism financing, in which case it applies simplified customer due diligence actions and measures;
* **Medium risk** of money laundering and terrorism financing, in which case it applies at least general customer due diligence actions and measures;
* **High risk** of money laundering and terrorism financing, in which case it applies increased customer due diligence actions and measures.

Accordingly, there should exist an internal category of *unacceptable risk*, where the Obliged Entity will potentially refuse to establish business cooperation or propose that business cooperation should be terminated if it has already been established.

Obliged Entities may use a risk matrix as a risk assessment method in order to identify low risk clients, those with slightly higher, but still acceptable risk and those carrying a high or unacceptable level of risk of money laundering and terrorism financing.

(*For example, the Obliged Entity may express risk levels numerically; but in that case it must accurately describe how it arrived at the representation of each risk level as a numeric indicator; or it may use descriptive terms to express different risk levels: high, low, medium risk or low , medium, high or very high likelihood of a factor being risky. Similarly, consequences may be expressed as significant, small, insignificant or highly significant. It is up to the Obliged Entity to decide how to express the assessed risk, whether descriptively or numerically, and which risk matrix it will use if it opts to do so*).

The Obliged Entity is required to change its risk matrix in accordance with changes in the circumstances of its operations (*for example, a client will be categorised as low risk for a real estate agent, while a bank will categorise the same client as high risk, exactly because of different impacts of the type of risk and business relationship. A low-risk service combined with a client from a high-risk country will result in a higher risk level, which may be categorised as medium risk; if the client subsequently establishes a new business relationship or uses a high-risk service, the level of client risk will be modified to “high”*).

International standards and the Law allow the Obliged Entity to apply three types of actions and measures in relation to a client, depending on the level of money laundering and terrorism financing risk:

* General measures and actions, which are common for all clients, in the initial stages of contracting a business relationship, followed by measures and actions ranging from simplified to increased.

1) **General customer due diligence actions and measures** include identification and identity verification of the client and its beneficial owner; obtaining and assessing information on the purpose and aim of the business relationship or the client’s transactions; and regular monitoring of the client’s operations and checks to determine whether its activities correspond to the nature of the business relationship and the type of the client’s business operations. These actions and measures are implemented as follows:

a) Identification and verification of the client’s identity

Obliged Entities are required to obtain the required client information before establishing a business relationship or executing transactions in excess of a threshold set by the Law or in other cases provided for by the Law, in order to identify the client or verify its identity.

A client may be accurately identified and its identity verified on the basis of documents, data or information obtained from reliable and veritable sources or by using means of electronic identification in accordance with the law, for example an official identity document or other official public document (*personal documents, official documents, originals or certified transcripts from a register, data obtained directly from the client*), which verify the identity of the client (*natural person, legal entity, legal representative, proxy-holder, foreign law entity, sole trader, civil law entity; a natural person may be identified and his/her identity verified by a qualified electronic certificate*).

Under the Bylaw on the Conditions for and Manner of Identifying and Verifying the Identity of Natural Persons using Means of Electronic Communication (*Official Gazette of the Republic of Serbia* No. 69 of 9 July 2021), a client may also be identified using means of electronic communication, without mandatory presence of the person being identified by the obliged entity in accordance with the regulations.

Where it is impossible to identify or verify the identity of a client, as well as where it is impossible to identify the client’s beneficial owner and where it is impossible to obtain information on the purpose and aim of the business relationship or transactions or other data in accordance with the Law, the Obliged Entity must refuse to establish the business relationship or refuse to participate in the execution of the transaction, and is under an obligation to terminate any existing business relationships with such client.

b) Determination of the client’s beneficial owner

The Obliged Entity shall:

1. Identify the client’s beneficial owner, where the latter is a legal entity or a foreign law entity, by obtaining the data provided for by the Law, including: name, surname, date and place of birth and place of permanent or temporary residence of the client’s beneficial owner.
2. Obtain the above data by consulting the originals or certified copies of the documents contained in a register maintained by the competent authority of the client’s country of establishment, issued not more than six months prior to the date of their obtaining, and keep copies thereof in accordance with the law. On each such kept copy, the obliged entity shall indicate the date and time and the personal name of the person who consulted the original or the certified copy. Data may also be obtained by directly consulting a public register in accordance with the Law,
3. Take reasonable measures to verify the identity of the client’s beneficial owner, so that it knows the client’s ownership and management structure and the identity of its beneficial owners at all times.

(*For example, in order to obtain the above data, the Obliged Entity may consult documents contained in the relevant register maintained by the Business Registers Agency or other competent authorities of the client’s country of establishment. Unlike the document used in the identification and verification of identity of a legal entity, which must not be older than three months, the documents used in the identification of the beneficial owner of a legal entity or a foreign law entity must not be older than six months, counting from the issuing date. Data may also be obtained by directly consulting the relevant official public register. The printed extract should include the relevant data and bear the date and time and the personal name who consulted the documents, and such extract is to be kept in accordance with the law*).

If it is impossible to obtain all data on a client’s beneficial owner from a public register or a register maintained by the competent authority of the client’s country of establishment, the Obliged Entity shall obtain the missing data from an original document or a certified copy thereof or from other business documentation, as provided to it by the client’s representative, general proxy holder or assignee, while any data that cannot be obtained as described above due to objective reasons may also be obtained by the Obliged Entity by consulting commercial or other available databases and data sources or written statements of the client’s representative, general proxy holder or assignee or its beneficial owner. In the process of identifying a client’s beneficial owner, the Obliged Entity may obtain a copy of an identity document of the client’s beneficial owner or a printout of such document.

If the Obliged Entity is unable to identify the beneficial owner after undertaking all actions provided for by the law, it shall identify one or more natural persons who hold top managerial positions within the client.

The Obliged Entity shall document all actions and measures taken to identify a client’s beneficial owner.

The duty to identify the client’s beneficial owner applies also to natural persons.

(*For example, the beneficial owner of a client who is a natural person is the same person who has direct or indirect control of the client. Control of a client certainly includes controlling its transactions or business relationship, which effectively means the client does not act for his own account, i.e. it is the case where a client who is a natural person establishes a business relationship or executes a transaction in the presence of another natural person who gives him/her instructions, or executes a transaction by reading notes containing instructions etc.*)

When identifying a client’s beneficial owner, Obliged Entities may use the Guidelines on Identification of Beneficial Owners of Clients and the Guidelines on Recording Beneficial Owners of Registered Entities in Central Records, available on the Administration’s website at http://www.apml.gov.rs

2) **Increased customer due diligence actions and measures** include the following in addition to the general actions and measures:

* obtaining and assessing the authenticity of information on the origin of the assets which are or will be the object of the business relationship, and
* additional actions and measures to be undertaken by the obliged entity in cases specified by the Law, as well as in other cases where it assesses that a high risk of money laundering or terrorism financing exists or might exist.

The Obliged Entity shall set forth by an internal bylaw which increased measures and to what extent it will apply in each specific case.

Which additional measures the Obliged Entity will undertake when it categorises a client as high risk based on its ow risk assessment will depend on the situation (e.g. if a client is categorised as high risk because of its ownership structure, the Obliged Entity’s procedures may require mandatory obtaining of additional data and mandatory additional verification of the presented documents).

The duty to undertake increased actions and measures applies in the following cases provided for by the Law:

а) New technological developments and new services

The Obliged Entity is required to identify and understand risks associated with a new or innovative product or service, in particular where this involves the use of new technologies or new payment methods. New products and new business practices, including new ways of delivering products and the use of new technologies in product development (*whether for new or existing products*), in particular if they are not clearly understood, may contribute to an increased risk of money laundering and terrorism financing.

When new technological developments and new products or services are used, the Obliged Entity is required by the law to apply additional measures on top of the general customer due diligence actions and measures, to mitigate and manage the risk of money laundering and terrorism financing (*e.g. more frequent monitoring of the client in order to determine if its business operations are as expected based on the KYC intelligence, its revenues etc.*).

b) Public official

The Obliged Entity shall provide for a procedure to determine whether a client or a client’s beneficial owner is a public official (domestic or foreign), which includes immediate family members or immediate associates of a public official, as well as members of managing and steering bodies of a legal entity majority-owned by a foreign state, members of managing bodies of political parties and official of international organisations who hold or have held in the past four years a high public office at an international organisation, including: a director, a deputy director, a member of a managing body or another equivalent office at an international organisation.

customer due diligence actions and measures should be a key source of information as to whether a client is a public official (*e.g. information on the client’s main vocation or employment post*). The Obliged Entity shall also use other sources of information that may be useful in identifying public officials by undertaking any of the following activities:

1. Obtaining a written statement from the client as to whether he/she is a public official, an immediate family member of an official or a close business associate of a public official;
2. Using commercial electronic databases containing lists of politically exposed persons (*e.g. World-Check, Factiva, LexisNexis*);
3. Searching publicly available data and information (*e.g. register of public officials maintained by the Anti-Corruption Agency*);
4. Creating and using an internal database of public officials (*e.g. major financial groups keep their own lists of public officials*).

The order and number of these activities that will be undertaken by the Obliged Entity should be decided in such a way as to enable accurate determination whether a client or a client’s beneficial owner is a public official.

The said written statement shall contain the following data:

* Name and surname, date and place of birth, permanent or temporary residence address and Unique Master Citizen Number/personal identity number of the public official who establishes the business relationship or executes the transaction or on whose behalf the business relationship is established or the transaction executed, as well as the type and number of the identity document, name of the issuing authority and the date and place of issuing;
* A statement whether the client is a public official according to the criteria set forth in the Law (*e.g. the statement should exhaustively list all cases provided for by the Law*);
* Information as to whether the public official is a natural person who holds or has held in the past four years a high public office in the country or in a foreign country or an international organisation, and whether he/she is an immediate family member or a close business associate of a public official;
* Information on the period in which he/she holds or held such office;
* Information on the type of public office the official holds or has held in the past four years;
* Information on the family relationship, if the client is an immediate family member of a public official;
* Information on the type of business cooperation, if the client is a close business associate of a public official.

When establishing a business relationship with a client who is a public official, the Obliged Entity shall apply increased customer due diligence actions and measures.

The Obliged Entity shall apply these increased actions and measures even when a natural person no longer holds a public office (a former public official), for as long as necessary to ascertain that the person concerned did not abuse the public office he/she had held, and in any case at least four years after the date of termination of his/her public office.

The data and documents obtained in this procedure are to be kept on the client’s file for 10 years after the date of termination of the business relationship.

c) Identification and identity verification without the client’s physical presence

If the client or its legal representative, or a person authorised to represent the legal entity or foreign law entity, are not physically present on the Obliged Entity’s premises for the identification and identity verification of the client, the Obliged Entity shall, in addition to the general customer due diligence actions and measures, apply also the additional measures provided for by the Law concerning the obtaining of additional documents, data or information on the basis of which it will verify the client’s identity; additional verification of provided documents or additional verification of the client’s information; obtaining information as to why the client was absent (additional contacts should be made with the client via phone, e-mail, Skype, Viber or otherwise and at least one more identification document of the client should be obtained).

d) Off-shore legal entities

The Obliged Entity shall establish a procedure according to which it will determine whether a client or a legal entity in its ownership structure is an off-shore legal entity. To determine whether an entity is an off-shore legal entity, the Obliged Entity may use IMF and World Bank lists or the list of countries incorporated in the Bylaw on the List of Jurisdictions with a Preferential Tax System (*Official Gazette of the Republic of Serbia* Nos. 122/12, 104/18 and 61/20). If it finds upon conducting such procedure that a client or a legal entity in its ownership structure is an off-shore legal entity, the Obliged Entity shall, in addition to the general customer due diligence actions and measures, undertake also additional (increased) measures in accordance with the Law.

e) Countries not applying international standards in the field of anti-money laundering and counter-financing of terrorism

When establishing a business relationship or executing a transaction where a business relationship is not established with a client established in a country with strategic deficiencies in its combat against money laundering and terrorism financing, the obliged entity shall apply the increased actions and measures provided for by the Law.

Strategic deficiencies in a country’s anti-money laundering and counter-financing of terrorism system concern in particular:

1. The country’s legal and institutional framework, including in particular prosecution of the criminal offences of money laundering and terrorism financing, customer due diligence measures, data keeping provisions, provisions governing the reporting of suspicious transactions, availability of true and accurate information on the beneficial owners of legal entities and foreign law entities;
2. Powers and procedures of the country’s competent authorities with regard to money laundering and terrorism financing;
3. Effectiveness of the anti-money laundering and counter-financing of terrorism in eliminating the risk of money laundering and terrorism financing.

З) **Simplified customer due diligence actions and measures** are undertaken in the cases and in the manner provided for by the Law and the Bylaw on the Methodology for Performing Duties in Accordance with the Law on the Prevention of Money Laundering and Financing of Terrorism (*Official Gazette of the Republic of Serbia* Nos. 80/20 and 18/22, hereinafter referred to as the “Bylaw”) and apply to clients carrying a low risk of money laundering and terrorism financing. Clients may also be assigned to this risk category on the basis of a conducted risk analysis.

The Obliged Entity shall undertake these measures in respect of a client identified as low risk. The simplified actions and measures are identical to the general customer due diligence actions and measures, except where the client is a national authority, an autonomous province authority, a local self-government authority, a public enterprise, a public agency, a public service, a public fund, a public institute or chamber or a company whose issued securities are listed in an organised securities market in the Republic of Serbia or a country which applies international standards equivalent to or higher than the EU standards, regarding reporting and submission of data to the competent regulatory authority, in which case obliged entities are not required to identify the client’s beneficial owner.

*2.1.4.2.4. CONTINUAL DUE DILIGENCE*

Apart from conducting a money laundering and terrorism financing risk analysis, Obliged Entities must carry out their registered business activity in compliance with their obligations provided for by the Law and undertake the following actions and measures to prevent and detect money laundering and terrorism financing before, during and after the execution of transactions or the establishment of business relationships, including:

* 1. Performing customer due diligence;
  2. Providing the Administration with information, data and documentation;

1. Designating a person responsible for compliance with the obligations provided for by the Law (the AML/CFT officer) and his/her deputy and ensuring the conditions required for their work;
2. Regular professional education, training and development of employees;
3. Ensuring regular internal control of compliance with the obligations provided for by the Law, as well as internal audits if appropriate for the scope and nature of the obliged entity’s business operations;
4. Compiling a List of Indicators for identified persons and transactions that can reasonably be suspected of money laundering or terrorism financing;
5. Keeping of records and protection and storage of data contained in those records, and
6. Taking other actions and measures pursuant to the Law.

## *2.1.4.2.4.1.* ***Frequency of customer due diligence based on risk category***

Once the Obliged Entity has categorised its clients according to risk levels as:

1. low money laundering and terrorism financing risk;
2. medium money laundering and terrorism financing risk;
3. high money laundering and terrorism financing risk,

the Obliged Entity shall apply customer due diligence actions and measures throughout the entire business relationship, with the frequency and intensity corresponding to the assessed risk and any changed circumstances concerning the client, so that:

1. it performs due diligence of clients categorised as low risk at least once every six months;
2. it performs due diligence of clients categorised as medium risk at least once every two months;
3. it performs due diligence of clients categorised as high risk at least once a month.

## *2.1.4.2.4.2.* ***Provision of data to the Administration for the Prevention of Money Laundering***

Within the framework of their statutory powers, Obliged Entities must ensure full cooperation with the supervisory authorities – the Ministry and the Administration. Cooperation between the Obliged Entity and the supervisory authorities is mandatory in particular with regard to provision of documents and requested data and information on clients or transactions in respect of which there are grounds for suspicion of money laundering. Cooperation is also necessary in case of notifying any activities or circumstances that were or could be associated with money laundering or terrorism financing.

The Administration passed the Bylaw on the Methodology for Performing Duties in Accordance with the Law, which sets forth in detail the methodology for performing the relevant duties. Obliged Entities are required to provide data to the Administration whenever there are grounds for suspicion of money laundering or terrorism financing in connection with a transaction or a client, in the manner and form and within the time limits provided for by the Law and the Bylaw. The duty to notify arises where the Obliged Entity, when establishing a business relationship or before executing a transaction, cannot identify the client or verify the client’s identity as provided for by the Law or cannot determine the client’s beneficial owner or obtain data on the purpose and intended nature of the business relationship or transaction or other data required by the law.

An employee of the Obliged Entity who determiners there are grounds to for suspicion of money laundering or terrorism financing must immediately alert the AML/CFT officer or his/her deputy. The Obliged Entity must arrange for a procedure to report suspicious transactions via AML/CFT officers, in compliance with the following instructions:

* Specify in detail the manner in which data are to be reported (by telephone, telefax, secure electronic means etc..),
* Specify the types of data to be provided (data on the client, reasons for suspicion of money laundering etc.),
* Specify the manner of cooperation between organisational units and the AML/CFT officer,
* Specify the course of action in relation to the client in case of suspension of transactions by the Administration for the Prevention of Money Laundering,
* Specify the role of the obliged entity’s the AML/CFT officer in reporting suspicious transactions,
* Prohibit the disclosure of information as to whether any data, information or documents will be submitted to the Administration for the Prevention of Money Laundering,
* Specify measures regarding continued operations with the client (suspension of operations, termination of the business relationship, increased customer due diligence actions and measures and monitoring of the client’s future business activities etc.).

## *2.1.4.2.4.3.* ***AML/CFT officer***

The Obliged Entity must designate an AML/CFT officer and his/her deputy, as persons who comply with the requirements set forth in the Law, to perform specific actions and measures to detect and counter money laundering and financing of terrorism.

The AML/CFT officer shall perform the following duties in the field of detecting and countering money laundering and financing of terrorism:

* 1. Ensure the establishment, operation and development of the system for detecting and countering money laundering and financing of terrorism and initiate and suggest to management appropriate measures to improve it;
  2. Ensure proper and timely submission of data to the Administration in accordance with the Law;

1. Participate in the development of internal bylaws;
2. Participate in the development of guidelines on internal controls;
3. Participate in the establishment and development of IT support;
4. Participate in the development of professional education, training and development of employees at the Obliged Entity.

The Obliged Entity must provide the AML/CFT officer with the required working conditions, assistance and support in the discharge of his/her duties, keep him/her updated of any fact that may be linked with money laundering or terrorism financing, grant him/her unrestricted access to the data, information and documentation necessary for the performance of his/her duties, provide him/her with appropriate human resources, financial assets, information technologies and other resources needed in his/her work, provide appropriate premises and technologies to ensure protection of confidential data held by the AML/CFT officer, provide continual professional training, arrange for a replacement during his/her leave, impose safeguards in terms of prohibiting the disclosure of information on him/her to unauthorised persons etc.

The AML/CFT officer shall perform his/her duties independently and shall report to the top management. The deputy AML/CFT officer shall substitute for the AML/CFT officer during his/her absence and perform other duties in accordance with the relevant internal bylaw of the Obliged Entity.

The Obliged Entity shall provide the Administration with information on the personal name and job title of the AML/CFT officer and his/her deputy, as well as information on the personal name and job title of the member of top management responsible for compliance with this law, and information on any changes thereof, within 15 days of appointment.

*2.1.4.2.4.4.* ***Regular Professional Education, Training and Professional Advancement of Employees***

In accordance with the Law, the Obliged Entity shall ensure regular professional education, training and professional advancement of all employees engaged in prevention and detection of money laundering and terrorism financing, i.e. all employees who perform certain tasks on their jobs which are or could be indirectly or directly exposed to the risk of money laundering and terrorism financing, as well as all external associates and representatives, to whom it entrusted tasks based on contracts, unless they are individual Obliged Entities for implementation of measures for detection and prevention of money laundering and financing of terrorism.

The Obliged Entity shall ensure that each employee understands his/her role in the management of the risk of money laundering and financing of terrorism, to ensure appropriate management and implement relevant supervision of risks. Trainings for employees who are in direct contact with clients or perform critical transactions in management of the risk of money laundering and financing of terrorism are thus very important. All staff, from the level of employees to top management, must be aware of the risk of money laundering and terrorism financing.

Professional education, training and development includes learning about the provisions of the Law and regulations passed based on the Law and internal instruments, expert literature on prevention and detection of money laundering and terrorism financing, the list of indicators to recognise clients and transactions suspected to include money laundering or terrorism financing, as well as the provisions of regulations providing for freezing of assets with the aim of preventing terrorism and proliferation of weapons of mass destruction and regulations providing for personal data protection.

The Obliged Entity shall, **until the end of March for the current year at the latest**, prepare the Annual Programme for Professional Education, Training and Development of Employees in Prevention and Detection of Money Laundering and Terrorism Financing.

The Programme shall include:

1. The planned number of trainings annually;
2. The planned number of employees who will attend trainings, as well as the profile of employees for whom trainings are intended;
3. Topics in the field of anti-money laundering and counter-financing of terrorism which will be the subject of trainings, as well as topics in the field of freezing of assets with the aim of preventing terrorism and proliferation of weapons of mass destruction;
4. The manner of implementation of trainings (*seminars, workshops etc.*)

The Obliged Entity shall, in the year for which the Programme was passed or **by the end of March of the next year at the latest**, implement trainings set by the Programme and make an official note of such trainings.

An official note shall include the time and the place of training, the number of employees who attended training, name and surname of the person who held training and a short description of the topic addressed on training.

The Obliged Entity shall keep the Programme and documentation of annual professional education, training and development of employees (*official notes, presentations etc.*) in accordance with the Law.

Regular professional education, training and advancement at the Obliged Entity can be implemented by the AML/CFT officer, his/her deputy, or other trained person, appointed by the Obliged Entity’s management on proposal of the AML/CFT officer.

*2.1.4.2.4.5.* ***Ensuring******Regular Internal Control and Internal Audit***

The Obliged Entity shall establish regular, systematic internal control of regularity and efficiency of the implementation of statutory measures to detect and prevent money laundering and financing of terrorism.

Obliged Entities shall implement the control of regularity and effectiveness of the implementation of statutory measures to detect and prevent money laundering and financing of terrorism through regular or extraordinary supervisions, in the procedure of internal control in accordance with the Bylaw.

The Obliged Entity shall implement internal control in accordance with the identified risk of money laundering and terrorism financing. If the Obliged Entity assessed the risk of its business operations as high, internal control of business operations shall be performed periodically, quarterly or every six months, in full compliance with the assessed risk of business operations of the Obliged Entity.

In case of a change in the business process of the Obliged Entity (*e.g. expansion or narrowing of the business activity for which an authorisation was obtained from a supervisory authority, an organisational change, a change in business procedures, introduction of a new service*), the Obliged Entity shall check and bring into compliance its procedures within internal control, so that they would be appropriate for compliance with the duties under the Law.

The Obliged Entity shall check compliance of the system and procedures for implementation of the Law, as well as application of those procedures, **annually** and each time any changes occur in the business process, until such change is introduced in the business offer at the latest.

The Obliged Entity shall prepare the Annual Report on Performed Internal Control and Measures Undertaken after Such Control until **15 March of the current year** for the previous year at the latest.

The Annual Report shall contain the following data:

1. The total number of established business relations where the sale involves a cash transaction of EUR 10,000 or more in dinar equivalent;
2. The total number of reported transactions or persons suspected to be linked with money laundering or terrorism financing;
3. The total number of persons suspected to be linked with money laundering or terrorism financing who were reported to the AML/CFT officer by employees at the Obliged Entity, but were not reported to the Administration;
4. The total number of established business relations where the identity of the client was established based on the client’s qualified electronic certificate or in the video identification procedure, as well as the total number of business relations established through proxy holders;
5. The frequency of the use of individual indicators for recognition of suspicious transactions when transactions are reported to the AML/CFT officer by employees at the Obliged Entity;
6. The total number of internal controls performed based on the Bylaw, as well as findings of internal control (*the number of observed and eliminated shortcomings, description of observed shortcomings etc.*);
7. Measures undertaken based on performed internal controls;
8. Data on performed internal control of information technologies used in implementation of the provisions of the Law (*ensuring protection of data transferred electronically, keeping data on clients and transactions in a centralised database*);
9. Data on the content of training programmes in detection and prevention of money laundering and financing of terrorism, the place and persons who implemented training programmes, the number of employees who attended training, as well as needs assessment for further training and development of employees;
10. Data on undertaken measures to keep data that are (*marked as*) an official secret;
11. The total number of established business relations where certain “know-your-client” and monitoring actions and measures for the client are entrusted to a third party.

The Obliged Entity shall submit the above Annual Report to the Administration and the Ministry on their request, **within three days** of the date of submission of such request.

The management shall ensure that the scope of internal audit is in compliance with the level of risk of money laundering and terrorism financing to which the Obliged Entity is exposed.

*2.1.4.2.4.6.* ***Indicators to Recognise Grounds for Reasonable Suspicion***

According to the Law, the Obliged Entity shall prepare the List of Indicators to Recognise Suspicion of Money Laundering or Financing of Terrorism. When preparing the List, the Obliged Entity shall include the indicators published at the official website of the Administration which are included in the Directive on Publishing Indicators to Recognise Suspicion of Money Laundering and Terrorism Financing with Real Estate Agents, as well as indicators the Obliged Entity recognised itself in its business activities as indicators that can indicate money laundering and terrorism financing activities.

When preparing the List of Indicators to recognise persons and transactions, account should be taken of the complexity and scope of execution of transactions and business relations, unusual manners of execution, the value or connection between transactions that have no economically or legally justified purpose, which are not compliant or disproportional to the usual or expected business operations of the client, as well as other circumstances in connection with the status or other characteristics of the client.

When determining the grounds for suspicion of money laundering and terrorism financing, the Obliged Entity shall apply the List of Indicators and take into account other circumstances indicative of reasonable suspicion of money laundering or terrorism financing.

*2.1.4.2.4.7.* ***Records***

The Obliged Entity shall keep records and the content of data on clients, as well as on business relations and transactions in accordance with the Law.

*2.1.4.2.5. DOCUMENTATION*

The approach based on risk assessment also requires documenting of risk assessment, as well as relevant internal instruments in place, to ensure determination of baselines and application of appropriate measures and procedures.

The methodology implies that the Obliged Entity independently determines the techniques at the beginning which would be helpful in preparation of analysis documents, the manner in which it will select and process information and the scope and type of information it will use.

*2.1.4.2.5.1.* ***Internal Instruments***

In accordance with the provisions of the Law, the Obliged Entity shall pass and implement relevant internal instruments which will include all actions and measures for prevention and detection of money laundering and terrorism financing set by the Law, secondary legislation passed based on this Law and these Guidelines to ensure efficient management of the risk of money laundering and terrorism financing. The Obliged Entity shall include in internal instruments the set risks of money laundering and terrorism financing, where such instruments must be proportionate to the nature and the scope of business operations, as well as the size of the Obliged Entity, and must be approved by a member of the top management. The Obliged Entity shall ensure implementation of these instrument by establishing relevant internal control procedures and mechanisms.

The Obliged Entity shall regulate by internal instruments in particular the following:

* The process of preparing the risk analysis of money laundering and terrorism financing;
* The procedures and mechanisms to detect suspicious transactions and/or clients, as well as the actions employees should take after recognition of such transactions and procedures for submission of information, data and documentation at the level of the Obliged Entity
* Appointing of persons responsible for compliance with the duties under the Law – the AML/CFT officer and his/her deputy, as well as ensuring conditions for their work[[12]](#footnote-12).
* The measures and actions to monitor business operations of the client which it will undertake or execute during business relations, the conditions for change of the client’s status according to the level of exposure to the risk of money laundering and terrorism financing and periods of monitoring the clients according to the risk level;
* Determining the eligibility of the client according to the level of the risk of money laundering and terrorism financing when establishing business relations and during those relations;
* Determining the risk categories of the client, services and transactions according to the risk factors in terms of the risk of money laundering and terrorism financing;
* The procedure for implementation of “know-your-client” actions and measures, and regular monitoring of the client’s business operations in accordance with the determined risk category, including verification of the client’s activities with the nature of business relations and the usual scope and type of the client’s business operations, as well as possible change of the client’s risk category;
* The procedure for implementation of intensified “know-your-client” and monitoring actions and measures for the client, when the client is high-risk according to the Law itself or based on the performed risk analysis, and in particular the procedure for determining whether the client or its beneficial owner is an official, as well as the procedure to determine whether the client or a legal entity included in the ownership structure of the client is an offshore legal entity;
* The procedure of regular internal control of compliance with the duties under the Law, in accordance with the Law and preparation of the annual report on performed internal control and measures undertaken after such control by 15 March of the current year for the previous year at the latest with the content set by the Bylaw;
* The procedure of regular professional education, training and development of employees in accordance with the annual professional education, training and development programme for employees engaged in prevention and detection of money laundering and terrorism financing, which is prepared by the end of March for the current year with the content set by the Bylaw[[13]](#footnote-13);
* Keeping records, protection and keeping of data in such records.

The List of Indicators to Recognise Persons and Transactions Suspected to be Involved in Money Laundering or Terrorism Financing and the List of Indicators to Recognise Suspicious Activities in connection with Terrorism Financing are also integral parts of internal instruments, which also contain all indicators for prevention of money laundering published on the website (http://www.apml.gov.rs/srp49/dir/lndikatori.html).

Obliged Entities can supplement the List of Indicators according to money laundering trends and typologies they are familiar with, as well as according to the circumstances arising from business operations of the Obliged Entity. The List of Indicators to Recognise Suspicious Persons and Transactions is a starting point for the Obliged Entity in recognising suspicious client’s activities. Namely, when determining if there are elements to qualify certain transactions as suspicious, one should take into account the indicators prepared by the Administration for Prevention of Money Laundering, or the Ministry/supervisory authority. However, a person and a transaction can be suspicious even if they cannot be included under any indicator. In such case, the Obliged Entity should consider wider circumstances, because it knows its clients best and in that sense it can conclude that a transaction is suspicious although it cannot be included under any published indicator. On the other hand, in case a person or a transaction can be marked a suspicious based on an indicator in the List, this does not mean that the Obliged Entity must immediately report such person as suspicious to the Administration for Prevention of Money Laundering; instead, it should monitor the client closely and, depending on future developments, evaluate whether it should report this to the Administration for Prevention of Money Laundering. Suspicious activities of clients are reported on the form which constitutes an integral part of the Bylaw.

If an employee at the Obliged Entity who is in direct contact with a client suspects that there is a risk of money laundering and terrorism financing in connection with that client or his/her transaction, such employee must prepare an internal written report thereof and submit it to a person responsible exclusively for compliance with the duties under the Law and other regulations providing for anti-money laundering and counter-financing of terrorism, i.e. AML/CFT officer, within the deadline and in the manner specified by an internal instrument of that Obliged Entity. This report should contain such data on the client and transaction which ensure the Obliged Entity can evaluate whether the client or the transaction is suspicious.

If the AML/CFT officer, based on the report or other information on the existence of the risk of money laundering and terrorism financing he/she learns directly, evaluates a transaction as suspicious, such officer shall further act in accordance with the Law, and if he/she does not evaluate a transaction as suspicious, he/she shall prepare an official note thereof.

In addition to the above, the Obliged Entity shall prepare an official note on implemented trainings, the content of which is also specified by the Bylaw.

In addition to preparation of internal instruments, the Obliged Entity shall document all actions and measures it undertakes against the client in accordance with the Law.

Identification of the client, its agent, proxy holders, beneficial owner, client risk analysis and registering data with the records (*all actions and measures*) are performed when business relations are established with the client and all data and documentation are updated regularly and kept in business documentation. Identification of the client is performed by inspecting documentation in the official register of a country where the client has his/her head office or by direct inspection of the register, or by inspecting a personal document the hard copies of which or printout of an identity document include the date, the place and personal name of a person who inspected the document, or an electronic copy of a document which contains a qualified electronic seal or a qualified electronic signature with the related time stamp. Also, a digitalised document or a copy of documentation are also considered a copy of documentation, i.e. printout of an identity document can be kept in hard copy or electronically.

The Obliged Entity shall keep data related documentation in connection with implementation of the Law for 10[[14]](#footnote-14) or 5[[15]](#footnote-15) years.

**II**

**SPECIFIC SECTION**

The Obliged Entity shall apply the Specific Section of these Guidelines taking into account specific circumstances concerning the risks.

1. ***Types of Risks with Real Estate Agents***

Risk assessment, within the meaning of these Guidelines, should include minimum the following four main risk types: geographic risk, client risk, service risk and transaction risk provided by the Obliged Entity within his/her business activities. In case other types of risks are identified, depending on the specific features of business operation, the Obliged Entity should also include in the assessment those types of risks.

1.1. **Geographic risk** includes the risk conditioned by a geographic area/territory of a country from which a client, its owner or majority founder, a beneficial owner or a person who otherwise controls business operations of a client originates (*from which he/she comes or where he/she resides*), or from where a person carrying out a transaction with a client comes from.

Factors to determine whether certain locations/countries from which a client originates are high-risk in terms of money laundering and terrorism financing include the countries:

1. Against which the United Nations, the Council of Europe or other international organisations imposed sanctions, embargo or similar measures;
2. Identified by the credible institutions (*FATF, the Council of Europe etc.*) as countries that do not apply appropriate anti-money laundering and counter-financing of terrorism measures;
3. Identified by the credible institutions (*FATF, UN etc.*) as countries that support or finance terrorist activities or organisations;
4. Identified by the credible institutions (*e.g. the World Bank, IMF*) as countries with a high level of corruption and crime;
5. For which credible sources demonstrated that they do not submit information on beneficial ownership to competent authorities, which can be concluded from FATF mutual evaluation reports or reports of organisations that also evaluate various levels of cooperation, such as OECD Global Forum reports on transparency and exchange of information for tax purposes.

The list of countries with strategic shortcomings in the system to fight money laundering and terrorism financing is published on the website of the Administration www.apml.gov.rs. This list is based on:

1. FATF (Financial Action Task Force) announcements on countries with strategic shortcomings in the system to fight money laundering and terrorism financing and which are a risk for the international financial system;
2. FATF announcements on countries/jurisdictions with strategic shortcomings in the system to fight money laundering and terrorism financing, which, for the purpose of eliminating the recognised shortcomings, expressed willingness at the highest political level to eliminate such shortcomings, which prepared action plans for this purpose in cooperation with FATF and which must report on the progress they achieved in elimination of such shortcomings;
3. Reports on evaluation of national systems to fight money laundering and terrorism financing by international institutions (FATF and the so-called regional bodies modelled on FATF, such as the MONEYVAL Committee of the Council of Europe).
4. Countries that apply standards in the field of anti-money laundering and counter-financing of terrorism at the level of the EU standards or higher include:
5. EU Member States;
6. Third countries (*other non-EU countries*) with effective systems for anti-money laundering and counter-financing of terrorism, evaluated in reports on evaluation of national systems to fight money laundering and terrorism financing by international institutions (FATF *(Financial Action Task Force) and the so-called regional bodies modelled on FATF, such as the MONEYVAL Committee of the Council of Europe*);
7. Third countries (*other non-EU countries*) identified by credible sources (*e.g. Transparency International*) as countries with low level of corruption and other criminal activities;
8. Third countries (*other non-EU countries*) which, based on credible sources, such as reports on evaluation of national systems to fight money laundering and terrorism financing by international institutions (FATF *(Financial Action Task Force) and the so-called regional bodies modelled on FATF, such as the MONEYVAL Committee of the Council of Europe*), published report on the progress of those countries after the report, have statutory duties to fight money laundering and terrorism financing in accordance with FATF recommendations and to efficiently implement those duties.
9. Countries with privilege tax systems, persons/clients established in those countries which have contractual relations and perform business activities with persons in offshore zones (*e.g. a person will be of high risk if he/she provides services to a client established in that country*).

This was also pointed out by the Country National Risk Assessment1, if we observe case studies, judgements for money laundering and typologies of criminal behaviour, in particular in case of organised crime groups, the Obliged Entity must be aware of assessed cross-border threats and diligently analyse relations when offshore zones and countries in the region appear as geographic elements.

Namely, although certain countries apply standards, this does not mean they will be immediately be included in the group of countries with low risk with the Obliged Entity; instead, the typology of behaviour and objects of money laundering must be taken into account, which pointed to a higher risk of certain countries which the Obliged Entity must treat with due diligence.

Low risk of money laundering can be borne by a client that has a contractual relation with a client in the region. For example, a client that trades goods with a client in the country of the region can be of low risk if such relation is economically justified.

1.2. **Client risk** - the Obliged Entity determines the client risk approach based on its own experience and knowledge of business rules.

Categories of clients whose activities may be **indicative of** **high risk** include the following cases:

1. The parties do not actually act on their behalf and they are trying to hide the identity of the actual buyer or seller;
2. The buyer/tenant does not show a particular interest in characteristics of real estate (*the quality of construction, location, the date of completion and acceptance*);
3. The buyer/tenant is not particularly interested in collecting better offers or achieving more favourable payment conditions;
4. The parties show great interest in fast purchase transaction, although there is no particular reason to do so, without interest in learning important details of the contract;
5. The client substitutes the parties (*brings a new person and presents him/her as the buyer*) immediately before implementation of the contract, without appropriate explanation for such actions;
6. The client buys real estate for cash, and soon uses that real estate as collateral for a loan to buy new real estate;
7. The client refuses to provide data normally collected in practice by inspecting personal documents;
8. The client gifts real estate to a person with whom he/she has no family or other personal or business relations;
9. Construction companies – firms with unproportionally low number of employees for the scope of the work they perform, which do not have their infrastructure, business premises, where ownership structure is opaque can be considered to be companies of particular risk;
10. The client is a domestic or a foreign public official and as a politically exposed person poses a risk, and the Obliged Entity must thus perform an analysis in all cases when such person acts as a client, before establishing of business relations or execution of transactions;
11. A person whose offer to establish business relations was rejected by another Obliged Entity, if such fact is learned in any way, or persons known for their bad reputation etc.
12. The client which is suspected to be linked with terrorist activities and/or is included in the UN sanctions list 1267, is interested in establishing business relations and investment in real estate;
13. The parties do not actually act on their behalf and they are trying to hide the identity of the actual client;
14. The client is trying to identify himself/herself by documents other than personal documents;
15. The client presents for inspection only copies of personal documents or inappropriate documents;
16. The client refuses to provide data normally collected in practice (*personal data, address, occupation*) and/or there are inconsistencies in enclosed documentation (*dates, signatures and other data, or suspected document forgery*);
17. The client is publicly known, according to the media, as a person involved in illegal economic (*informal economy*) and/or criminal activities;
18. The client substitutes the parties immediately before implementation of the contract, and he/she is known for his/her illegal activities;
19. The client is trying to establish good and friendly relations with the staff of the real estate agent, and according to publicly available sources he/she has a criminal background;
20. The client who is interested in a real estate, which he/she has not seen himself/herself, is buying the real estate through agents (*lawyers, proxies, close friends etc.*), suspicion is rising because intelligence suggests that the client/buyer performs various business activities that are borderline illegal (*illegally*);
21. Real estate is purchased on the same day or within a very short period, particularly when significant difference from the market price is observed and it is assumed that the clients are related parties;
22. Intelligence suggests that the client has a substantial quantity of cash to purchase real estate and it is assumed that payment will be made in cash;
23. The value of offered real estate is high, and the client provides unreasonable answers on the manner of payment for the real estate, i.e. requests to make transactions exclusively in cash or combined with unreliable sources of payment;
24. The client insists on electronic conclusion of the contract and electronic submission of a purchase order, and he/she is from a country known for production and distribution of narcotics, a country that does not have a regulated money laundering identification and prevention system and a country from the so-called “blacklist”, or a country suspected to incite terrorist activities and financing, although it is not certain that an intermediation service will be performed;
25. The client who has recently purchased a real estate is selling the real estate for a price several times higher than the purchase price, which is a sign of involvement of related parties for fictive money transfer and concealment of origin and layering of the next client;
26. Due to the structure, the legal form or complex and unclear relations, it is difficult to determine the identity of their beneficial owners or persons who manage them, such as offshore legal entities with opaque ownership structure which were not founded by companies in a country that applies standards for anti-money laundering and counter-financing of terrorism at the level of standards set by the Law;
27. A fiduciary or other similar foreign law company with unknown or hidden owners or management (*this includes foreign law companies which offer agent services for third parties, or companies founded by conclusion of a contract between a founder and a manager, who manages the founder’s assets, to the benefit of certain persons who are users or beneficiaries, or for other specified purposes*);
28. A complex status structure or a complex ownership chain (*which makes it difficult or impossible to determine the client’s beneficial owner, or persons who indirectly provide assets on the basis of which they exercise control, who can direct or otherwise significantly influence the client’s management or governance structure when making decisions concerning financing and operations, foundations, trusts or similar foreign law entities, charities and non-profit non-governmental organisations, agricultural cooperatives, off-shore legal entities with an opaque ownership structure, i.e. “shell companies”*);
29. Foreign arms dealers and manufacturers;
30. A foreign politically exposed person;
31. Non-residents and foreigners;
32. Clients who professionally represent other persons (*lawyers, accountants or other professional agents*), in particular when the Obliged Entity only has contact with the agents;
33. Companies with unproportionally low number of employees for the scope of the work they perform, which do not have their infrastructure and business premises, where ownership structure is opaque etc.;
34. The client offers money, gifts or other benefits as reciprocal favour for activities suspected not to be fully compliant with regulations;
35. The client often changes his/her agents;
36. Clients that perform activities characterised by large turnover or cash payments (*restaurants, filling stations, exchange offices, casinos, flower shops, traders in precious metals, vehicles, artworks, goods and passenger transporters, sports societies, construction firms*);
37. Private investment funds;
38. Clients whose source of funds is unknown or opaque, or the client is unable to demonstrate the source of funds;

It should be noted that if the Obliged Entity evaluates that a client which is an offshore legal entity or a legal entity included in the ownership structure of a client which is an offshore legal entity has a complex ownership structure (*e.g. a large number of legal entities as founding members, of which entities with a significant share in the initial capital are registered in offshore destinations and when it is difficult to determine who is the beneficial owner of those legal entities*), the Obliged Entity must obtain a written statement on the reasons for such structure from the beneficial owner or the client’s agent, as well as to consider whether there could be suspicion of money laundering or terrorism financing and to make an official note thereof, which it must keep in accordance with the Law.

The Obliged Entity must pay particular attention if it establishes business relations with a client engaged in: real estate buying and selling, investment, construction activities, real estate construction, sales of goods and services frequently and in substantial amounts without personal surety in the documentation, and must also pay attention to persons who invest money by buying securities.

Situations described in the National Risk Assessment indicate a high risk in the above activities. All listed activities which have been recognised with the client must be closely monitored and risk assessment must be made, and activities of these persons must be often monitored and assessed.

1.3. **Service risk**

This risk *inter alia* **particularly** includes the following services:

1. Services that are new on the market, i.e. they have not been offered before in the non-financial sector and must be particularly monitored to identify the actual risk level;
2. Electronic submission of trading contracts/orders in cases set by the Obliged Entity in its procedure;
3. Provision of the types of services which an employee at the Obliged Entity evaluated, based on his/her experience, as services of a high-risk level;
4. Provision of services by opening the so-called joint accounts for transactions, which mobilise funds from various sources and from various clients, which are deposited to one account opened in a single name;
5. Electronic conclusion of a contract if it is uncertain whether a service will be provided;
6. Services identified by internationally recognised sources as high-risk services in electronic transactions, such as international correspondent banking services in implementation of sales contracts (and international) private banking activities in transactions;
7. New innovative products or services not provided directly by the Obliged Entity; instead, various electronic agents or other channels with the Obliged Entity are used for their provision (*e.g. in case of receipt of a trading order, risk of money laundering is higher when orders are submitted electronically or through trading platforms or using mobile phones than when contracts/orders are submitted directly. In case of provision of receipt and transfer of orders for trade in real estate, the probability that those services are used for money laundering or terrorism financing is higher than in, for example, services of collecting the documentation during implementation of a sales contract or portfolio management*).
8. The client insists on new digital money services, where there might not be possible to identify real cash flows or participants in payment (*Crypto currency, PayPall, Ерау etc.*), which have not been available so far on the market with the agent, or to use various electronic or other payment channels;
9. The client offers a high agent fee, with the aim of bribing so that the actions and duties under the law are not complied with.
10. Rent in the amount significantly higher than rent for an apartment of similar characteristics in the same or similar location, which is paid in advance for a long period, when there is suspected criminal intent and fictive contract.

1.4. **Transaction risk**

Transaction risk **includes in particular the following situations**:

1) Real estate is purchased or sold on the same day or within a very short period, particularly when significant difference from the market price is observed;

2) Purchase of real estate in the name of third persons (relatives, friends, lawyers, legal entities in offshore destinations and other legal entities), without any logical reason;

3) Real estate purchase/rent is unproportional to the buyer’s/tenant’s purchasing power, and he/she provides unreasonable answers about the origin of the property;

4) Transactions where the client requests payment consisting of several smaller payments, which cumulatively make up the price of the real estate (the so-called fragmentation);

5) Several real estate purchase and sale transactions for one real estate by a group of related natural persons and/or legal entities (family or business relations, persons living at the same address or agents or lawyers etc.);

1. Transactions made by agents (lawyers, proxies etc.) acting in the interest of potentially related natural persons (family or business relations, persons living at the same address etc.);
2. Transactions involving a newly founded legal entity, with a small initial capital, which purchases or sells real estate of high value;
3. Collateral for a loan to purchase real estate is provided by depositing 100% of the amount of the requested loan;
4. Transactions from territories which do not apply regulations in the field of prevention of money laundering and where there is a high geographical risk of money laundering, whether the client is from such territories or not;
5. The client promises an unrealistically high agent fee for performed task (real estate purchase/rent);
6. Rent in the amount significantly higher than rent for an apartment of similar characteristics in the same or similar location, which is paid in advance for a long period, when there is suspected fictive contract etc.
7. The client shows great interest in fast purchase transaction, although there is no particular reason to do so, and requests fast formal conclusion of the contract and expresses the intent to use complex and unusual payment methods;
8. Transactions where the client requests payment consisting of several smaller payments, which cumulatively make up the price of real estate (fragmentation), particularly in case of high-value real estate where intelligence suggests that the parties are linked to illegal or criminal activities;
9. Intelligence suggests that the client has sources of finance in a foreign country, or outside the financial system, and wishes to contract payments in several smaller amounts using money transfer payment institutions (*e.g. Western Union*);
10. Several purchase transactions performed by a group of natural persons and/or legal entities (non-governmental, charity, religious or other non-profit organisations) which are assumed to be involved in illegal actions, and intelligence suggests that sources of money for the payment are unrelated parties
11. A transaction executed by the client is not in accordance with his/her usual business practice, and within a short period he/she makes several purchases without any economic or legally founded reasons, with the obvious aim of money placing.
12. Transactions which were intended for persons or entities subject to measures of the United Nations or the Council of Europe, as well as transactions which the client would make on behalf and for the account of a person or an entity subject to measures of the United Nations or the Council of Europe.

Financial practice varies between the countries and cultural differences are also taken into account; while on some markets cash transactions in large amounts can be considered a high risk, on other markets this can be usual, particularly where currency exchange rate varies, or where mortgage market is not well regulated.

***2. Risk Assessment with Persons Providing Real Estate Agent Services***

In addition to the above criteria, when determining the risk level of a certain client, business relations, service or transactions, the Obliged Entity shall, based on its experience, also include other types or risk or other criteria, such as:

1) The client’s size, structure and business activity, including the scope, structure and complexity of tasks performed by the client;

1. The client’s status and ownership structure;
2. The purpose of establishing of business relations, services or transactions;
3. Knowledge of services and the client’s experience, i.e. knowledge of that field;
4. Other information showing that the client, business relations, services or transactions can pose a high risk.

High risk is possible in:

1. Locations with high concentration of foreigners or where numerous transactions are made with foreigners;
2. Clients or their beneficial owners, if they are domestic or foreign officials;
3. Buyers/tenants who show particular interest in a specific real estate or location, without expressing particular interest in price of real estate (the so-called purchase at any cost);
4. Clients, who did not see real estate in person, are buying/renting the real estate through agents (lawyers, representatives, close friends etc.);
5. The client who provides personal documents issued by a foreign country, the authenticity of which is difficult to verify;
6. Ownership of real estate, where ownership is the only relation of a buyer who is a foreign national with our country;
7. A legal entity that provides an address which is a P.O. box number for communication with real estate agents, or the address where the legal entity is registered is unknown etc.

In summary, for the Obliged Entity to be able to conduct a comprehensive risk assessment, it should describe all products and services it offers, contractual relations it establishes, to evaluate the probability that clients will abuse a product/service for money laundering or terrorism financing, as well as to assess the impact or the result of such phenomenon similarly as it assesses the above client risk.

**III**

**TRANSITIONAL AND FINAL PROVISIONS**

The Guidelines shall be binding for all Obliged Entities who are real estate agents.

The Guidelines shall enter into force on the date when they are signed and shall take effect on the eighth day of their publication on the official website of the Ministry.

On the date when these Guidelines take effect the „Guidelines on the Assessment of Money Laundering and Terrorism Financing Risk by Real Estate Agents” of 28 May 2020 shall be repealed.

Obliged Entities shall bring their internal instruments in compliance with these Guidelines within 30 days of their publication.

Number: 334-00-1165/2022-06

Done in Belgrade, on 30 June 2022

MINISTER

Tatjana Matić

1. <http://www.apml.gov.rs/uploads/useruploads/Documents/NRA2021.pdf> [↑](#footnote-ref-1)
2. Criminal Code (*Official Gazette of the Republic of Serbia* Nos. 85/05, 88/05 – corrigendum, l07/05 – corrigendum, 72/09, P 1/09, 121/12, 104/13, 108/14, 94/16 and 35/19) [↑](#footnote-ref-2)
3. The 2018 National Risk Assessment separated real estate agents from real estate developers, as it was determined that these constituted two entirely different business activities, although parts of the same sector. [↑](#footnote-ref-3)
4. Obliged Entities under the Law are insurance companies licensed to perform life-insurance business and insurance brokerage companies when they perform life-insurance brokering; insurance agency companies and insurance agents with a licence to perform life-insurance business, except for insurance agency companies and insurance agents for whose work the insurance company is responsible according to the law. [↑](#footnote-ref-4)
5. *Official Gazette of the Republic of Serbia* Nos. 75/2014, 88/2018 and 105/2020 [↑](#footnote-ref-5)
6. *Official Gazette of the Republic of Serbia* Nos. 75/2014, 39/2017, 70/2018 and 98/2020 [↑](#footnote-ref-6)
7. *Official Gazette of the Republic of Serbia* No. 75/2014 [↑](#footnote-ref-7)
8. *Official Gazette of the Republic of Serbia* No. 95/2013 [↑](#footnote-ref-8)
9. 8 July 2019 [↑](#footnote-ref-9)
10. 28 May 2020 [↑](#footnote-ref-10)
11. *Official Gazette of the Republic of Serbia* Nos. 29.15, 13/17 and 41/18) [↑](#footnote-ref-11)
12. The Obliged Entity must submit to the Administration for Prevention of Money Laundering data on personal name and title of the AML/CFT officer, his/her deputy and a member of top management responsible for implementation of the Law (a notification or a decision on appointment with indicated data), as well as any change to such data within 15 days of appointment at the latest. [↑](#footnote-ref-12)
13. In addition to the above, the Obliged Entity must prepare an official note on implemented trainings, the content of which is also specified by the Bylaw. [↑](#footnote-ref-13)
14. For data and documentation in connection with the client, established business relations with the client, performed risk analysis and executed transactions, of the date of termination of business relations. [↑](#footnote-ref-14)
15. For data and documentation on the AML/CFT officer, deputy AML/CFT officer, professional training of employees, performed internal controls, of the date of termination of office of the AML/CFT officer, implemented professional training or performed internal control. [↑](#footnote-ref-15)