Coat of arms of the Republic of Serbia
Republic of Serbia
MINISTRY OF FINANCE
GAMES OF CHANCE ADMINISTRATION
Number: 002194610 2025 10529 002 002 000 001
Beograd, 15 May 2025

Based on Article 6, paragraph 1 Law on the Prevention of Money Laundering and the Financing of Terrorism ("Official Gazette RS", no. 113/17, 91/19,153/20, 92/23, 94/24 and 19/25, hereinafter: the Law), Article 114, and in relation to Article 104, paragraph 1 points 4a) and 110, paragraph 3 of the Law, the director of the Games of Chance Administration adopted the following

GUIDELINES FOR ASSESSMENT OF RISK OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION FOR OBLIGORS ORGANISING SPECIAL GAMES OF CHANCE IN CASINOS AND GAMES OF CHANCE THROUGH MEANS OF ELECTRONIC COMMUNICATION

The Games of Chance Administration, in accordance with Article 104, paragraph 1, point 4a) and 110, paragraph 3 of the Law on the Prevention of Money Laundering and Financing of Terrorism (hereinafter: the Law), as the authority responsible for inspection in the field of games of chance, supervises the implementation of this Law by the obligors referred to in Article 4, paragraph 1, point 8) of the Law, i.e. in organisers of special games of chance in casinos and organisers of special games of chance through means of electronic communication who perform their activities based on the specific law.

The Games of Chance Administration may, in accordance with Article 114 of the Law, either independently or in cooperation with other authorities, adopt recommendations or guidelines for implementation of provisions of the Law on Prevention of Money Laundering and Financing of Terrorism.

With the aim of improving the system for combating the money launder, terrorism financing and financing of proliferation of weapons of mass destruction, amendments to the Law on Prevention of Money Laundering and Financing of Terrorism ("Official Gazette RS" no. 94/24) have been adopted, which entered into force on 6 January 2025, as well as amendments to the Law on the Prevention of Money Laundering and Financing of Terrorism ("Official Gazette RS", no. 19/25), which entered into force on 6 March 2025.

In December 2024, the National Risk Assessment was also adopted, and the results of this risk assessment provide essential information to obligors and serve as both the starting point and a mandatory basis for conducting their own risk assessments.

The purpose of these guidelines is to define the foundations and/or assumptions upon which obligors should conduct their assessment of the risk of money laundering and terrorist financing in relation to their business operations, as well as the methodology for carrying out risk assessments/analyses on a case-by-case basis, in order to ensure consistent application of the provisions of the Law and the establishment of an effective anti-money laundering and counter-terrorist financing system by obligors.

The guidelines for assessing the risk of money laundering and terrorist financing are adopted to ensure an adequate assessment of exposure to money laundering and terrorist financing risk, the development and regular updating of the risk analysis, and the development of procedures for identifying and managing risk, so that the provisions of the Law on the Prevention of Money Laundering and Terrorist Financing are applied in a harmonised manner.

The system must ensure that risks are comprehensively identified, analysed, assessed, monitored, mitigated, and managed in the most effective way. Obligors may apply these measures to varying extents, depending on the type and level of risk and in accordance with the different risk factors.

By adopting a risk-based approach, obligors should be able to ensure that the measures aimed at preventing money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction are proportionate to the risks identified, enabling them to make decisions on how to most effectively allocate their own resources.

MONEY LAUNDERING - DEFINITION AND STAGES

Money laundering is the process of disguising of an illegal origin of money or property acquired by criminal acts.

For the purpose of the Law, money laundering means:

- conversion or transfer of property acquired through the commission of a criminal offence;
- 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;
- acquisition, possession, or use of property acquired through the commission of a criminal offence.

For the purpose of the Law, all the above activities conducted outside the territory of the Republic are also considered money laundering.

Money laundering encompasses a range of activities undertaken to conceal the origin of proceeds derived from the commission of a criminal offence. The process of money laundering may involve a series of transactions in which the assets obtained through criminal activity represent the input value, while the output value of such transactions consists of "legitimate" goods and services.

Money laundering is a process that can be divided into three main stages, bearing in mind that in practice these stages may sometimes overlap or be omitted altogether.

1) The first stage involves breaking the direct link between the money and the illicit activity through which it was obtained, and is referred to as the ***placement stage***. During the placement stage, illicitly acquired funds are introduced into legitimate financial flows. There are numerous ways in which this can be achieved. One such method is depositing cash obtained through criminal activities into bank accounts, often under the guise of legitimate business activities where payments are typically made in cash, such as restaurants, consignment shops, boutiques, casinos, and similar establishments.
2) The second stage is the ***layering*** or ***concealment stage***. After the money has entered the legitimate financial system, it is transferred from the account into which it was initially deposited to other accounts held by legal entities, with the intention of presenting fictitious business activity or carrying out an apparently legitimate transaction. The main objective of these transactions is to obscure the connection between the money and the criminal activity from which it originated.
3) The third stage, known as integration, is the final phase of the process, after which the “dirty” money appears as funds derived from lawful business activity. A common method of integrating “dirty” money into legitimate financial flows is the purchase of real estate or controlling shares in joint-stock companies. This represents an example of large-scale concentration of illicit capital, which is precisely the objective of money launderers. Integration focuses on marketable assets—that is, on what can be bought and sold. Once the money reaches this stage, it becomes extremely difficult to trace its illegal origin.

TERRORISM FINANCING - DEFINITION AND STAGES

For the purpose of the Law, terrorism financing means the providing or collecting of property, 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:

- in order to carry out a terrorist act;
- by terrorists;
- by terrorist organisations.

Terrorism financing means aiding and abetting in the provision or collection of property, regardless of whether a terrorist act was committed or whether property was used for the commission of the terrorist act, where the pri8mary objective does not necessarily have to be the concealment of the origin of funds, but rather to obscure the nature of the activities for which those funds are intended.

Terrorist financings consists of several stages:

1) raising funds from legitimate operations or from criminal activities;
2) keeping of funds raised;
3) transfer of funds to terrorists;
4) use of funds.

The first stage entails raising of funds from persons operating in a legitimate manner, but are linked to a terrorist organisation or terrorists, or from persons linked to criminal activities, e.g. drugs trafficking, extortion, embezzlement, etc. A major source of funds are also donations by individuals supporting the objectives of terrorist organisations or funds raising funds and directing them to terrorist organisations.

In the second stage, the funds are kept, i.e. held either directly in bank accounts of individuals or accounts of intermediaries associated with terrorist organisations.

The third stage involves transfer of funds to a terrorist organisation's cells or individuals, so it can be used for terrorist activities. The funds are most frequently transferred through the money transfer and banking systems, even though informal methods of transfer are frequently used.

The use of funds becomes evident when they are employed for terrorist activities, such as the purchase of weapons, explosives, equipment, financing of training camps, propaganda, provision of safe houses, etc.

Money laundering and terrorist financing are global issues that can negatively affect the economic, political, security, and social structures of a country. The consequences of money laundering and terrorist financing undermine the stability, transparency, and efficiency of the financial system, cause economic disruption and instability, harm the country's reputation, and threaten national security.

FREEZING OF ASSETS WITH THE AIM OF PREVENTING TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

The Law on the Freezing of Assets with the Aim of Preventing Terrorism and Proliferation of Weapons of Mass Destruction ("Official Gazette RS", no. 23/15...94/24) lays down actions and measures for freezing of assets of designated persons; the competences of state authorities concerning the application of these measures; and rights and obligations of natural and legal persons in the application of the Law.

Freezing of assets means temporary prohibition of transfer, conversion, disposal and movement of assets or temporary management of such assets based on a decision of the competent state authority.

Designated person means natural person, legal entity or a group or an association, designated and listed as terrorist, terrorist organisation or terrorist financier, and listed on the list of persons linked to proliferation of weapons of mass destruction and special lists based on:

1. relevant United Nations Security Council Resolutions or acts of international organisations of which Republic of Serbia is a member;
2. proposal of competent state authorities or
3. a justified request of a foreign state.

The website of the Administration for the Prevention of Money Laundering provides access to the search engine for the UN Security Council list of designated persons: https://www.apml.gov.rs/liste-oznacenih-lica-i-pretrazivac

Data on designated persons are automatically retrieved on a daily basis from the database of relevant UN sanctions lists, ensuring accurate and timely results when using the search engine. Notifications about changes to the list are sent directly to the email addresses of obliged entities under the Law on the Prevention of Money Laundering and Terrorist Financing.

Proliferation of weapons of mass destruction (WMD) refers to the development, production, acquisition, trade, transportation, supply and use of WMDs, as well as the transfer of technology and the capacity building for their development and production by members of criminal groups and terrorist/extremist groups and organisations, non-state actors and regimes that support terrorism, with the aim of causing loss of life and material damage.

Financing of proliferation of weapons of mass destruction refers to all activities to raise funds or activities to provide financial services directed, wholly or in part, towards the development, production, acquisition, possession, storage, delivery, brokering, transhipment, transport and transfer of weapons of mass destruction and means of their delivery.

Procedure for Reporting a Designated Person

The Law provides that in the course of performing their activities every legal or natural person is obliged to determine whether they are conducting business or have any similar relationship with a designated person. If a person establishes that it has business with the designated person, it is obliged to immediately freeze the assets of the designated person and notify the Administration for the Prevention of Money Laundering without delay and no later than within 24 hours.

Notifications and information are submitted in written or electronic form. If submitted by telephone, the notification must be confirmed in writing.

The notification about the designated person and their assets, as well as any information relevant to identifying the designated person or their assets, is submitted using the Designated Person Reporting Form, which is available on the website of the Administration for the Prevention of Money Laundering.

The website of the Administration also contains the Guidelines for Obligors of the Law on the Prevention of Money Laundering and Terrorist Financing for identifying, detecting, and preventing the financing of proliferation:

https://www.apml.gov.rs/uploads/useruploads/Documents/UPUTSTV0%20ZA%200BVEZN1KE-SPRECAVANJE%20FINANSIRANJA%20OMU.pdf

THE CONCEPT OF RISK AND RISK ASSESSMENT

Risk is a function of three factors: threats, vulnerabilities and consequences.

A ***threat*** is defined as a person or group of persons, objects or activities that have the potential to cause harm, for example, to the state, society, economy, etc. In the context of money laundering, this includes persons engaged in criminal activity, terrorist groups and their supporters, the assets and funds at their disposal, the environment in which predicate offences are committed and in which the proceeds of crime are generated, as well as their scale and scope.

Vulnerability encompasses all elements that could be exploited in the event of a threat or that could support and facilitate the actions of a threat. For obligors, this refers to anything that exposes them to an increased risk of money laundering or terrorist financing (e.g. insufficient knowledge of the relevant legal framework, inadequate implementation of legal obligations, inadequate training, complex or inappropriate organisational structure, poorly defined responsibilities within internal processes, etc.).

Risk assessment involves making judgements about threats, vulnerabilities, and consequences, and represents the first step toward mitigating them.

Risk assessment:

- **National risk assessment**
- **at the level of the obligor**
- **at the level of business relationship (customer level)**

NATIONAL RISK ASSESSMENT

In the Republic of Serbia, the National Risk Assessment 2021-2023 was adopted in December 2024 and contains the following thematically defined sections:

1) ***Money laundering risk assessment***
2) ***Terrorist financing risk assessment***
3) ***Money laundering and terrorist financing risk assessment in the digital assets sector***
4) ***Assessment of the risk of financing of proliferation of weapons of mass destruction***
5) ***Assessment of the risk of the misuse of the non-profit sector for the purpose of terrorist financing***
6) ***Risk assessment of legal persons and legal arrangements***

Document **"National Risk Assessment"** is posted on the website of Administration for the Prevention of Money Laundering - https://www.apml.gov.rs/nacionalna-procena-rizika-1000000259

1) Money laundering risk assessment

The national money laundering risk assessment is the result of an evaluation of money laundering threats and vulnerabilities.

An assessment of various sectors is presented in the following comparative overview:

2018	
H	Banks
	Organisers of online games of chance
	Real estate
MH	Casinos
	Accountants
	Exchange offices
M	Notaries public
	Lawyers
ML	Capital market
	Payment institutions and electronic money institutions
	Auditors
L	Voluntary pension funds
	Insurance companies
	Financial lease providers

2021	
H	Real estate
	Organisers of online games of chance
	Banks
MH	Accountants
	Exchange offices
	Casinos
M	Real estate agents
	Lawyers
ML	Factoring companies
	Capital market
	Payment institutions and electronic money institutions
L	Financial lease providers
	Insurance companies
	Voluntary pension funds
	Postal operators

2024	
H	Real estate
	Lawyers
	Accountants
MH	Banks
	Exchange offices
	Notaries public
	Real estate agents
	Organisers of online games of chance
	Providers of digital assets services
	Casinos
M	Postal operators
	Auditors
	Payment institutions and electronic money institutions
ML	Capital market
L	Factoring companies
	Financial lease providers
	Insurance companies
	Voluntary pension

Sectors exposed to a high level of money laundering risk include the real estate sector, accountants, and lawyers. Significant cash turnover, the investment of illicit funds and their integration, as well as the scale of activities associated with the real estate sector, contribute to its long-standing attractiveness for money laundering. Furthermore, accountants typically have direct knowledge of cash flows and their origin within business entities, while lawyers face significant exposure to money laundering risks due to the nature of the services they provide.

The games of chance sector has been assessed as exposed to a medium-high level of risk, with the following factors indicating a higher likelihood of money laundering: the nature of transactions – cash transactions (frequent cash deposits and withdrawals, frequent execution of cash transactions below the legal threshold, which facilitates concealment and layering of funds); structured transactions – payments made in smaller amounts; multiplied transactions carried out by a larger number of individuals indicate a typological pattern of money laundering – the intent to avoid the submission of suspicious activity reports; illegal organisation of games of chance – organising games without authorisation from the competent authority and the inability to trace the flow of funds; a low number of reported suspicious transactions, and similar factors.

In addition to organisers of special games of chance in casinos and organisers of games of chance through means of electronic communication, the following sectors have also been assessed as having a medium-high level of risk: exchange offices, banks, public notaries, real estate agents, and digital asset service providers. Postal operators, auditors, payment institutions, and electronic money institutions are assessed as medium risk; the capital market sector is assessed as having a medium-low level of risk, while the lowest level of risk exposure has been assessed for the financial leasing sector, insurance companies, voluntary pension funds, and factoring companies.

Tax offences, corruption-related criminal offences, abuse of position of responsible person, abuse of official position, unauthorised production and trafficking of narcotic drugs, and criminal offences committed by organised crime groups are classified as high-threat criminal offences, a trend that has remained unchanged in this risk assessment.

The following are recognised as emerging risks: pawnshops, crowdfunding, private individuals investing in real estate, and cryptocurrencies. Although cryptocurrencies are not necessarily intended for criminal use, their anonymity, decentralised nature, lack of sufficient control, ease of access, speed, and simplicity of use make them highly attractive for criminal transactions, i.e. for the payment of criminal products and services.

Special Games of Chance in Casinos

Casinos are part of a sector whose risk has been assessed as ***medium high*** as ***moderately vulnerable*** and ***highly exposed*** to the threat of money laundering. This sector includes a range of elements that increase its vulnerability, the most significant of which is the predominant use of cash, as well as the fact that customers are exclusively natural persons. This can entail specific risks related to the jurisdiction of origin, as well as exposure to high-risk clients (e.g. politically exposed persons).

Games of Chance through Means of Electronic Communication

The risk associated with ***organising games of chance through means of electronic communication*** has been assessed as ***medium high***, i.e. this sector is considered to be **moderately to highly vulnerable** with **high exposure** to the threat of money laundering. Risk exposure in this type of organisation is increased due to the large volume of transactional flows, the lack of face-to-face interaction, and the possibility of cash payments.

2) Terrorist financing risk assessment - The risk of terrorist financing in the Republic of Serbia for the period 2021-2023 has been assessed as medium. The sectoral risk assessment showed that no sectors were identified as being at high or medium-high risk. Sectors exposed to medium risk include exchange offices, payment institutions, the public postal operator, freelancers in the IT sector, and NPOs. Sectors assessed as medium-low risk include tourism and hospitality, postal services, and accountants, while low-risk sectors include the games of chance sector, notaries public, banks, lawyers, financial leasing, and others.

3) Money laundering and terrorist financing risk assessment in the digital assets sector

The risk associated with virtual currency transactions has been assessed as medium-high, while the risk related to investment and utility tokens has been assessed as low. The overall risk profile in the VASP sector has been assessed as medium-high.

4) Assessment of the risk of financing of proliferation of the weapons of mass destruction (FPWMD)

Sectors where the risk of FPWMD is considered moderate, i.e. medium include banks, real estate agents, accountants, tax advisers, lawyers and games of chance, while other sectors are considered to carry low risk.

5) Assessment of risk of the misuse of the non-profit sector for the purpose of terrorist financing

The terrorist financing risks within the non-profit organisation sector generally reflect the TF risks identified for Serbia as a whole and have been classified as moderate.

6) Risk assessment of legal persons and legal arrangements

Based on the results of the NRA, LLCs and sole proprietors are considered business entities with a high level of exposure to money laundering risk, while associations and cooperatives are assessed as medium risk, and other forms of legal persons are assessed as having a low level of exposure to risk.

The risk of money laundering and terrorist financing is the risk of adverse effects on the financial performance, capital, or reputation of the obligor, resulting from the use of the obligor (either through direct or indirect use of a business relationship, transaction, or service) for the purpose of money laundering and/or terrorist financing.

Money laundering and terrorist financing are issues that obligors must address in order to avoid enabling, encouraging, or facilitating such activities—whether inadvertently or otherwise.

It is essential that obligors adopt a risk-based approach to identify, assess, and understand the risks of money laundering and terrorist financing, in order to direct their resources toward the areas of highest risk and implement appropriate mitigating measures.

The analysis of the risk of money laundering and terrorist financing is based on the assumption that not all products and services offered by obligors within the scope of their business activities, nor all transactions they conduct, are equally vulnerable to misuse for the purposes of money laundering and terrorist financing. This analysis is conducted to enable the application of control measures that are proportionate to the identified risk. This allows the obligor to focus on those clients, countries, products, services, and transactions that present the highest potential risk.

The risk-based approach also requires the documentation of the risk assessment, as well as the existence of appropriate internal regulations to establish a basis for the application of adequate measures and procedures.

Key elements of risk-based approach:

a) ***Identification/recognition*** of business risks that are susceptible to money laundering and terrorist financing, i.e. detection of the risks faced by the obligor, taking into account the customers, the types of services it provides, as well as publicly available information on the risks and typologies of money laundering and terrorist financing. It would be useful for the obligor to compile a list of potential factors to be used for recognising threats and vulnerabilities related to money laundering and terrorist financing within the obligor's operations. This primarily refers to those factors identified as high-risk at the national level, those specific to a particular obligor, as well as typologies, trends, behavioural patterns, specific circumstances, and similar.

Given that there is no universal model for risk assessment, but rather various guidelines, ideas, suggestions, and examples from domestic and international practice, it is up to the obligor to assess which methodology is best suited to its operations.

b) Following the risk identification and description phase comes the ***analysis phase***, which is key to risk assessment. This phase determines the likelihood of money laundering and terrorist financing occurring, as well as the potential impact if such events were to take place.

After identifying and reviewing all relevant factors, the obligor draws conclusions regarding the risk levels. Obligors may use a risk matrix as a method for risk assessment in order to identify customers who fall into the low-risk category, those who fall into a slightly higher but still acceptable risk category, and those who pose a high or unacceptable risk of money laundering and terrorist financing.

Based on the data from the analysis, the information is entered into the risk matrix, and the final result determines the degree of money laundering risk to which the obligor is exposed.

c) ***Risk management*** entails the purposeful use of the findings obtained through risk analysis. Based on the analysis, the obligor applies risk management strategies and implements an appropriate business policy, i.e. suitable procedures supported by adequate systems and control mechanisms for mitigating or overcoming the identified risks. The results obtained serve as the basis for defining action priorities.

RISK IDENTIFICATION

➢

The identification of risk categories or types - *customer risk, geographic risk, transaction risk and service risk* is the first step in the risk analysis, both for the obligor and the customer.

У Depending on the specific nature of the obligor's operations, other categories in which money laundering and terrorist financing may occur may also be taken into account.

Risk analysis, in accordance with Article 6 of the Law must be proportionate to the nature and scope of the business, as well as the size of the obligor, and must take into account the basic types of risk, including:

1) Geographic risk

Geographic risk refers to the assessment of exposure to the risk of money laundering and terrorist financing depending on the country of origin of the customer or the person conducting the transaction, the area or territory in which the obligor operates, and the country of origin of the ownership and management structure of the organiser of games of chance.

Factors used to determine whether a particular country or geographic location poses a higher risk of money laundering and terrorist financing include:

- countries subject to sanctions, embargoes, or similar measures imposed by the United Nations, the Council of Europe, or other international organisations;
- countries identified by credible institutions (such as the FATF, the Council of Europe, etc.) as not implementing adequate measures to prevent money laundering and terrorist financing;
- countries identified by credible institutions (such as the FATF, the UN, etc.) as supporting or financing terrorist activities or organisations;
- countries designated by credible institutions (e.g. the World Bank, IMF) as having high levels of corruption and crime;
- countries for which reliable sources indicate a failure to provide information on beneficial ownership to the competent authorities – this can be determined from FATF mutual evaluation reports or reports by organisations that assess various levels of cooperation, such as the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes.

A list of countries with strategic deficiencies in their systems for combating money laundering and terrorist financing is published on the website of the Administration for the Prevention of Money Laundering and is based on:

- FATF (*Financial Action Task Force*) public statements concerning countries with strategic deficiencies in their anti-money laundering and counter-terrorist financing systems that pose a risk to the international financial system;
- FATF public statements concerning countries/jurisdictions with strategic deficiencies in their systems for combating money laundering and terrorist financing that have committed, at the highest political level, to addressing the identified deficiencies, developed an action plan in cooperation with FATF, and are required to report on their progress in elimination of deficiencies;
- reports evaluating national systems for combating money laundering and terrorist financing prepared by international institutions (FATF and its regional-style bodies such as the Council of Europe's MONEYVAL Committee).

Countries that apply anti-money laundering and counter-terrorist financing standards that meet or exceed European Union standards include:

- EU member states
- third countries (non-EU countries) with effective anti-money laundering and counter-terrorist financing systems, as assessed in national system evaluation reports conducted by international institutions (FATF and FATF-style regional bodies such as the Council of Europe's MONEYVAL Committee);
- third countries (non-EU countries) identified by credible sources (e.g. *Transparency International*) as having a low level of corruption or other criminal activity;
- Third countries (non-EU countries) which, based on credible sources, such as national system evaluation reports on anti-money laundering and counter-terrorist financing by international institutions (e.g. FATF and FATF-style regional bodies such as the Council of Europe's MONEYVAL Committee), and published reports on the country's progress in fulfilling the recommendations from the evaluation reports, have legal obligations to combat money laundering and terrorist financing in accordance with FATF recommendations and effectively implement these obligations.

4) *Customer risk*

The obligor should describe all types or categories of customers with whom they do business and assess the likelihood that these types or categories of customers will misuse the obligor for money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction, including:

• customer category:

- regular customer;
- VIP customer;
- occasional customer, etc.

• customer type:

- customer who is not visiting for the first time, performing small to medium transactions;
- customer who is not visiting for the first time, performing medium to large transactions;
- customer who is visiting for the first time, who is a citizen of the Republic of Serbia;
- customer who is visiting for the first time, who is not a citizen of the Republic of Serbia, etc.

Customer risk refers to the assessment of whether a customer is associated with a higher risk of money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction. Based on their own criteria, the obligor determines whether a customer poses a greater risk based on the categorization performed.

The following customers represent a higher risk:

l) Regular customers whose usual behaviour changes:

- a customer who arrives, has permanent or temporary residence in a country and/or region listed among countries with strategic deficiencies in their system for combating money laundering and terrorist financing, posing a risk to the international financial system (this list can be found on the official FATF website and should be regularly monitored);
- a regular customer who starts spending larger sums of money;
- a regular customer who starts spending significantly smaller amounts of money but participates more frequently in games of chance, etc.

2) customers who are politically exposed persons, i.e. domestic and foreign officials;
3) customers from international corporations;

4) occasional customers, etc.

This risk analysis is a general analysis for different types or categories of customers and serves as a starting point for the categorisation of individual customer risks. Based on the specific circumstances of individual customers, such as their origin and history, or what can be concluded from the information they provide, the categorisation of the particular customer is adjusted, especially considering the following:

Customer risk - casinos

The obligor independently determines its approach based on customer risk assessment, relying on generally accepted principles and its own experience. Customer risk involves assessing whether a customer with whom the obligor cooperates is connected to a higher risk of money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.

Increased customer risk in a casino may be indicated by the following activities:

- the customer presents documents for identification that are suspected of being falsified, altered, or inaccurate;
- the customer provides only a copy of personal identification documents;
- the customer protests when requested by the authorised person in the casino to provide original personal identification documents, or there are grounds to suspect that the customer is providing false information;
- the documents provided by the customer for identification purposes were issued abroad, and there are reasons preventing the verification of their authenticity;
- the customer resides permanently or temporarily in a country and/or region listed among those with strategic deficiencies in the system for combating money laundering and terrorist financing, posing a risk to the international financial system (this list is available on the official FATF website and should be regularly monitored);
- the customer is a national of a country that does not adhere to standards for preventing money laundering and terrorist financing;
- the customer is a politically exposed person, i.e. a domestic and/or foreign official;
- the customer associates with suspicious individuals or is known to have been convicted of criminal offences, etc.

Customer risk - games of chance through means of electronic communication

In games of chance through means of electronic communication, the following activities of a customer may indicate higher risk:

- the customer accesses from an IP address (Internet Protocol address) located in a country and/or region listed among those with strategic deficiencies in their systems for combating money laundering and terrorist financing, posing a risk to the international financial system (this list is available on the official FATF website and should be regularly monitored);
- the customer is a national of a country that does not adhere to standards for preventing money laundering and terrorist financing;
- the obligor is aware that the customer is attempting to conceal their IP address;
- the obligor is aware that the customer has been convicted of criminal offences;
- the customer is a politically exposed person, i.e., a domestic and/or foreign official;
- the customer holds cards issued by offshore destinations or countries listed among those with strategic deficiencies in their systems for combating money laundering and terrorist financing, posing a risk to the international financial system (this list is available on the official FATF website and should be regularly monitored);

- the customer requests that winnings be transferred to another account or a third-party account;
- in the event of a large win, the customer avoids confirming their identity;
- the customer shows interest in specific game packages and suggests or proposes certain packages;
- the customer submits and/or has previously submitted requests for registration of multiple user accounts with the same details;
- the customer holds multiple bank accounts and alternates between them when participating in games of chance;
- the details of the bank accounts/payment cards do not match the registered details of the customer (identity fraud/stolen identity), etc.

5) *Transaction, product or service risk*

A transaction refers to the receipt, provision, exchange, storage, disposal, or any other handling of assets by the obligor, including a payment transaction in accordance with the law governing the provision of payment services.

Assets are items, money, rights, securities, and other documents in any form, which can be used to establish ownership and other rights.

Money refers to cash (both domestic and foreign), funds in accounts (both dinar and foreign currency accounts), and electronic money.

Cash transaction refers to the physical receipt or disbursement of cash.

A cash transaction at an organiser of special games of chance in casinos refers to the purchase of tokens or credit for a specific table or slot game, where, depending on the nature of the business, different games are activated at each table or slot machine, and the following core transactions take place:

- exchange of money for tokens with a defined value;
- exchange of tokens with a defined value for money;
- exchange of money for credit on a slot machine;
- exchange of slot machine credits for money, etc.

Other transactions in the casino may include: receipt, disbursement, exchange, safekeeping, disposal, or any other handling of assets by the obligor.

Higher risks of money laundering and terrorist financing in casinos are also represented by the following transactions:

- multiple customers purchase chips with cash (the transaction is for an amount slightly lower than the threshold that would trigger a report under the Law on the Prevention of Money Laundering and Financing of Terrorism), and then gamble with minimal amounts.
- a customer asks an employee at the casino to monitor their game and alert them when their winnings approach the transaction amount that, under the law, requires reporting to the Administration for the Prevention of Money Laundering;.
- a high winner asks another customer at the casino for assistance in cashing out some tokens, thus avoiding the reporting of transactions under the Law on the Prevention of Money Laundering and Financing of Terrorism.
- a customer gambles with minimal amounts and then immediately goes to the cashier to cash out chips.
- a customer tries to influence a casino employee in order to avoid reporting a transaction under the law, by requesting that the exchange of cash for chips or records of their cash transactions be made under a different person’s name.
- two players frequently and simultaneously place bets for the same amount, covering both sides of the same game (e.g., betting on both red and black or odd and even in roulette).
- a customer buys tokens for cash, places bets in games with low chances of losing money (e.g., betting on both red and black in roulette at the same time), or engages minimally in gambling, or does not gamble at all, then later goes to the cashier to

cash out the chips for tokens, requesting higher denominations than those originally used to purchase the tokens.

- a customer demands a confirmation of their winnings, even though such documentation is not typically issued in casinos;
- a random customer bets large sums of money on games of chance, etc.

The obligor/***organiser of games of chance through means of electronic communication*** is required to use an information and communication system (ICS) that allows for the storage, archiving, and exchange of data electronically with the software solution of the Games of Chance Administration. This system must enable precise record-keeping of all deposits and withdrawals made on the player's created account.

Higher risks of money laundering and terrorist financing in the case of organisers of games of chance via electronic communication are represented by the following transactions:

- enabling cash payments: most payments with organisers through electronic means are made directly from accounts in financial institutions. However, the obligor may operate as part of a mixed organisation that also includes betting shops, i.e., so-called "land-based betting." Thus, it can be enabled for customers to deposit cash into their transactional accounts at the pay-in-pay-out desk, and then use them for "online" games;
- the customer has multiple accounts or online wallets where the individual amounts for deposits and/or withdrawals do not exceed the limits for reporting under the Law on the Prevention of Money Laundering and Terrorist Financing;
- transfers between customers: obligors may allow or be aware that customers transfer money between themselves without using their own transactional accounts with the same obligor;
- use of third parties: criminals may use "third parties", either anonymous or identified gambling agents, to gamble certain amounts on their behalf in order to avoid identity verification of the customer. "Third parties" may be used to gamble on behalf of others with minimal amounts;
- use of transactional accounts with the obligor: without satisfactory internal controls, customers may use these accounts for depositing and withdrawing without gambling and with minimal stakes;
- changes to accounts with financial institutions: customers may hold accounts with multiple financial institutions and may wish to change one of the accounts they use for online betting. This may be for legitimate reasons, or there may be an intention to obscure the audit trail or to introduce third-party transactions without drawing attention;
- identity fraud: details of financial institution accounts may be stolen and used on websites. Stolen identities can also be successfully used to open accounts with financial institutions, and such accounts can then be used on websites through which multiple accounts can be opened for participating in games of chance through means of electronic communication, using stolen identities;
- prepaid cards: using cash to fund a prepaid card poses similar risks to those associated with cash.

The following customer transactions with *organisers of games of chance through means of electronic communication* may also indicate a higher risk:

- the customer deposits cash to top up their transactional account for the purpose of participating in games of chance through means of electronic communication;
- the customer deposits a relatively large amount of money into their transactional account and withdraws it after a certain period, without any activity or after very limited participation in games of chance;
- the customer regularly stakes large amounts of money in games of chance with the lowest acceptable level of loss;

- the customer places small but frequent stakes, with their total annual expenditure being high and significantly exceeding their annual income;
- several customers frequently and efficiently play "against each other", placing large amounts on weak hands with the expectation of losing to other players (so-called chip dumping);
- different customers are linked to the same bank accounts, which are used either for depositing funds or for the payment of winnings in games of chance (authorisations over current accounts), etc.

WHAT IS A SUSPICIOUS TRANSACTION?

A transaction may be assessed as suspicious if the obligor and/or the competent authority determine that there are grounds for suspicion of money laundering or terrorist financing in relation to the transaction or the person conducting it, or that the transaction involves funds derived from unlawful activities.

Transactions may also be treated as suspicious if, by their nature, scope, complexity, value, or interconnection, they are unusual, lack a clearly visible economic or legal basis, or are disproportionate to the customer's usual or expected business activities, as well as due to other circumstances related to the status or other characteristics of the customer.

The assessment of suspicion regarding a particular customer, transaction, or business relationship is based on suspicion criteria defined in the list of indicators for identifying persons and transactions suspected of involving money laundering or terrorist financing. The list of indicators serves as a starting point for employees of the obligor and authorised persons in recognising suspicious circumstances related to a particular customer, the transaction carried out by the customer, or the business relationship concluded, and in this regard, employees of the obligor must be familiar with the indicators in order to apply them in their work. However, a transaction may be suspicious even if it does not meet any of the indicators. In this respect, it is necessary to consider the broader context, in accordance with the principle that the obligor knows their customer best, and to assess whether a specific transaction may still be considered suspicious, even if it does not meet any of the indicators.

In assessing a suspicious transaction, the authorised person and their deputy are required to provide all professional assistance to employees.

Obligors/operators of special games of chance in casinos, or games of chance through means of electronic communication, should particularly monitor and identify suspicious transactions carried out in a manner that avoids standard and
usual control methods, including multiple participants, several interrelated transactions conducted within a short time frame or in multiple successive intervals, in amounts just below the legally prescribed threshold, in order to avoid recording and reporting.

The list of indicators for identifying suspicious transactions serves as a starting point for employees/authorised persons in recognising suspicious circumstances related to a particular customer and/or the transaction conducted by the customer, so they can use them in their work. In the process of determining whether there are elements to qualify a certain transaction or person as suspicious, the indicators for identifying grounds for suspicion must primarily be taken into account. However, a transaction may be suspicious even if it does not meet any of the indicators. In this respect, it is necessary to consider the broader context, in accordance with the principle that the obligor knows their customer best, and to assess whether a specific transaction may still be considered suspicious, even if it does not meet any of the indicators.

The primary task of the obligor is to ensure the availability of all necessary data related to the knowledge and monitoring of their customers, to assess whether certain behavioural patterns may be connected to a criminal offence and to what extent, and, in accordance with the Law, to take all necessary measures and report suspicious activities.

Reporting obligation

Pursuant to Article 47 of the Law, the obligor is required to notify the Administration for the Prevention of Money Laundering whenever there are grounds for suspicion that a transaction or a customer is related to money laundering or terrorist financing. This notification must be made prior to the execution of the transaction, and the report must specify the deadline by which the transaction is to be carried out

How to report suspicious transactions?

The obligor shall submit data on suspicious activities/transactions using the *Form for Reporting Cash and Suspicious Transactions and Suspicious Activities – Form No. 1*, which is an integral part of the Regulation on the Methodology for Performing Activities in Accordance with the LPMLTF.

In order to improve the obligors' knowledge and awareness of the importance of timely identification of potentially suspicious customers and suspicious activities, the Administration for the Prevention of Money Laundering has prepared Recommendations for Reporting Suspicious Activities – https://www.apml.gov.rs/uploads/useruploads/Documents/Preporuke%20za%20prijavljivanje%20sumnjivih%20aktivnosti%2028122022.pdf

RISK ANALYSIS

In order to prevent exposure to the adverse consequences of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, the obligor is, pursuant to Article 6 of the Law, required to develop and regularly update a written risk analysis of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, in accordance with the Law, the guidelines issued by the authority responsible for supervising the implementation of the Law, and the national risk analysis of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (hereinafter: risk analysis).

In accordance with the foregoing, when preparing the risk analysis at the obligor level – in relation to its overall business operations – as well as the risk analysis at the customer or business relationship level, the obligor is required to take into account both the level of threat and the vulnerability of the sector to which it belongs, based on the results of the national risk analysis.

Risk analysis must be proportionate to the nature and scope of the business, as well as the size of the obligor, and must take into account the basic types of risk, including geographical risk, customer risk, service risk and transactions risk, as well as other types of risks identified by the obligor due to the specifics of its business operations.

The risk analysis includes:

- risk analysis in relation to the obligor's overall business operations,
- risk analysis for each group or type of customer, or business relationship, the service provided within its activities, and the transactions.

In the process of preparing the risk analysis regarding its overall business operations, the obligor assesses the likelihood that its business will be used for such purposes. The risk analysis regarding the obligor's overall business operations aims to identify the obligor's exposure to the risk of money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction, as well as the business segments of the obligor that should be prioritized in undertaking activities for effective risk management.

Based on the assessed probability of the occurrence of risks and the estimated negative consequences, the obligor determines the level of exposure to the risks of money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction for each segment of its business operations.

The risk assessment, in accordance with these Guidelines, should include at least the following basic types of risks:

- geographical risk,
- customer risk,
- risk of services provided by the obligor within its activities,
- transaction risk.

The risk analysis for each group or type of customer, business relationship, transaction, service provided by the obligor within its activities, and the method of establishing a business relationship with the customer (e.g., without the customer's physical presence) aims to determine the criteria based on which the obligor will classify a particular customer, business relationship, service, or transaction into one of the risk categories in accordance with the Law. The classification of the customer into one of the risk categories is carried out by analysing specific types of risks as well as their combination, depending on the specifics of each obligor. The actions and measures for customer knowledge and monitoring that the obligor will take in accordance with the Law (from simplified to enhanced) depend on the risk category of the customer, business relationship, service, or transaction.

Based on the risk analysis, the obligor classifies the customer into one of the following risk categories:

1) low risk of money laundering and terrorism financing, applying at least simplified measures;
2) medium risk of money laundering and terrorism financing, applying at least general actions and measures;
3) high risk of money laundering and terrorism financing, applying enhanced actions and measures.

The obligor, through internal acts, may also introduce additional risk categories and determine appropriate actions and measures under the law for those risk categories.

Frequency of customer monitoring

In line with the risk analysis and customer knowledge, the frequency of customer monitoring, according to the guidelines, should be at least as follows:

1. low risk level – once every two years
2. medium risk level - once a year
3. high risk level - twice a year

The obligor must realistically assess the adequacy of up-to-date customer monitoring based on new circumstances related to the customer. Therefore, for high-risk cases, more frequent updates may be required (quarterly, monthly, or an ongoing assessment), depending on the circumstances and threats related to money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.

An efficient and high-quality risk assessment and update process involves, first and foremost, identifying parts of the system within the obligor that may have crucial information, recognize system vulnerabilities, and help mitigate threats.

Additionally, the obligor should pay due attention to information from external sources such as: results of the national risk assessment for money laundering and terrorism financing, amendments to the law, feedback received from obligors regarding reported suspicious transactions, behaviour models identified in indictments for money laundering, typologies, international research FATF, etc.

Employees of the obligor must have a clear understanding of how the obligor has assessed specific risks at the institutional level, how the results of the national risk assessment were implemented in the process, and a review of the clear measures the obligor intends to implement based on the obtained results.

Risk assessment is an activity that shows to what extent a specific risk can affect the achievement of a goal, and it is carried out based on probability and impact.

Probability represents the likelihood that a particular event will occur, while impact represents its effect.

Obligors assess exposure to the risk of money laundering and terrorism financing, i.e., the probability of negative impact arising from the risk, as well as the risk's effect on business objectives.

Exposure to risk is determined based on a matrix that shows the relationship between impact and probability. The primary purpose of using the risk matrix is to apply a risk-based approach in ranking obligors according to their exposure to the risk of money laundering and terrorism financing. Based on the data and information from the risk analysis, these are entered into the matrix, and the degree of risk to which the obligor is exposed is determined.

Example of 3x3 matrix

probability				
	high (1)	3	6	9
	medium (2)	2	4	6
	low (3)	1	2	3
		low (1)	*medium (2)*	*high (3)*

impact

The risk analysis of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction is based on the assumption that different products and services offered by obligors in the course of their business, or different transactions they carry out, are not equally vulnerable to abuse for money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction. This analysis risk is conducted to enable the application of control measures that are proportionate to the identified risk. This allows the obligor to focus on those clients, countries, products, services and transactions that present the highest potential risk. The risks the obligor faces must be analysed in terms of determining the likelihood that a particular event will occur and the assessment of the negative impact that may result.

The matrix is a tool used in applying a risk-based approach to the obligor's operations, and the obligor should also take into account other information and data during the risk assessment of its operations (e.g., measures taken by the supervisory authority, audit reports, etc.).

To determine the exposure of the obligor to the risk of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, the obligor must be aware of each business segment where the threat of money laundering or terrorist financing could arise, i.e., it must assess its vulnerability to the threat. It is necessary to identify risks at all management levels, from the operational level to the top management, and to involve all employees of the obligor in this process.

RISK MANAGEMENT

- Risk management entails the purposeful use of the findings obtained through risk analysis. Risk management, as well as *monitoring and reporting* on risks, is an ongoing process.

The effectiveness of managing the risk of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction by the obligor is assessed based on the established quality of the control system and the risk management system, and is viewed through the following levels of the obligor's activities: corporate governance, risk management, internal regulations, internal control, compliance, reporting, and training.

Managers at all levels of the obligor, through the risk analysis process, monitor whether certain risks still exist, whether new risks have emerged, whether the impact and likelihood of existing risks have changed, as well as whether the priority of risks has shifted.

The risks identified at the obligor are regularly discussed at meetings of senior management twice a year and as needed, after which communication is made with lower-level managers to ensure an effective response to risks.

Risks at the level of organisational units are monitored continuously and reviewed quarterly, or as necessary, by the heads of organisational units.

Based on the results obtained, priorities for action are determined, i.e., the methods the obligor will apply (e.g., whether the use of certain products or services will be prohibited, whether more attention will be paid to specific transactions, whether the level of training at the obligor should be increased, etc.).

High-risk issues must be addressed without delay, medium risks as soon as possible, and lower risks must be monitored.

The process of monitoring and reporting on money laundering and terrorist financing risks should be carried out as part of the following:

- the obligor's business function for operational control, ensuring that all prescribed procedures are regularly applied;
- the compliance function, which periodically checks whether established internal policies are complied with and whether all systems are functioning;
- the audit function, to determine if business policies and processes comply with the law and are implemented in accordance with legal requirements;
- the risk management resource assessment function, such as securing financial resources and staffing solutions;
- identifying future needs that are important for the nature, size, and complexity of the obligor’s entire business.

Managers at the obligor should be provided with regular reports and all other relevant information that will enable them to assess the level of control over money laundering and terrorist financing prevention, as well as the potential consequences for the obligor's operations if control mechanisms and preventive measures do not function as adequately assessed by the risks.

The management directs the business policy by setting goals and making decisions on strategic choices. When developing final plans and business policies, they must consider the risks of money laundering and terrorist financing.

The established internal policies and procedures are approved by the management and apply to all employees of the obligor. Through risk assessment and corresponding policies and procedures, the obligor ensures the continuity of risk management despite any changes that may occur within the management team or the employees, or in the structure of the obligor.

Furthermore, the management is obligated to foster a business ethics culture and ethical behaviour among employees. Ethical behaviour represents the professional and individual responsibility of employees for the decisions they make and the actions they take when performing their duties.

For the decision-making and planning process, *documenting* and the manner in which risks will be presented is of great importance. Namely, when certain risks are identified, the results must be documented and transferred into a written document, which, in addition to defining the key terms and methodology of work, also includes the outcome of the risk assessment. It is essential to describe the results and explain how the specific results were reached, as well as how the identified country risks reflect on the obligor itself.

To implement activities for establishing and maintaining a risk management process, the obligor adopts a strategy that provides a framework for identifying, assessing, and controlling potential events and situations that may have a negative impact on the obligor’s reputation and operations. It should include the obligor’s views on risks, set objectives, as well as roles, authorities, and responsibilities in the risk management process, effectiveness indicators, and should be periodically updated and revised.

The purpose of the strategy is to enhance the obligor's capacity to achieve set goals at the strategic and operational levels by using a risk management system.

The adopted business policies and procedures enable the obligor to effectively manage risks, focusing efforts on those areas of operation that are most susceptible to various forms of abuse in the context of preventing money laundering and terrorist financing. The greater the risk, the more control measures need to be applied. In this regard, at the obligor's level, it is necessary to implement policies and procedures for actions and measures to prevent and detect money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

Actions and measures to prevent money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction

In performing their registered activities, obligors must act in accordance with the obligations provided by the Law in the area of detecting and preventing money laundering and terrorist financing and are obliged to ensure compliance with the prescribed measures and activities at all levels, so that the entire business of the obligor is conducted in compliance with the law.

Actions and measures to prevent and detect money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction are undertaken before, during, and after the execution of a transaction or the establishment of a business relationship and include the following:

l) knowledge of the customer and monitoring of their business (hereinafter: customer due diligence);

2) providing information, data, and documentation to the Administration for the Prevention of Money Laundering;

3) designating a person responsible for carrying out the obligations under this law (hereinafter: authorized person) and their deputy, as well as ensuring the conditions for their work;

4) regular professional education, training, and development of employees;

5) ensuring regular internal control of the execution of obligations under this law, as well as internal audits if in accordance with the scope and nature of the obligor's business;

6) preparing a list of indicators to identify persons and transactions that are suspected to be related to money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction;

7) maintaining records, protecting, and storing data from those records;

8) implementing measures from this law in business units and subsidiaries of the legal entity in the majority ownership of the obligor, both domestically and abroad;

9) performing other actions and measures based on the law.

The obligor is also required to draft appropriate *internal acts* that will, for the purpose of effectively managing the risk of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, cover actions and measures defined by the law. The internal acts must be proportional to the nature and size of the obligor and must be approved by the top management, in accordance with Article 5 of the Law.

Each obligor is obliged to prepare a written risk analysis related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (Article 6 of the Law).

I Customer due diligence

The actions and measures for customer due diligence are a key preventive element within the process of detecting and preventing money laundering and terrorist financing. The purpose of implementing the actions and measures for customer due diligence is, primarily, to reliably establish and verify the true identity of the customer and the origin of their assets, as well as to continuously monitor the alignment of the customer's activities with the usual scope and type of their business.

If the implementation of the actions and measures for customer due diligence raises suspicion with the customer that the obligor is carrying them out to provide data to the Administration for the Prevention of Monez Laundering, the obligor is required to suspend these actions and measures and prepare an official written note, which is then submitted to the Administration.

The customer is required to provide the obligor with accurate, adequate, and up-to-date information necessary to establish and verify the identity of the customer and the beneficial owner.

International standards and the Law define that the obligor, depending on the level of risk of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, should implement three types of customer due diligence actions and measures: *general, simplified and enhanced.*

General customer due diligence actions and measures

General customer due diligence actions and measures, according to Article 7 of the Law, include the following activities: identifying and verifying the identity of the customer, obtaining and assessing the information on the purpose and intended nature of a business relationship or transaction, obtaining and assessing the credibility of information on the origin of property which is or which will be the subject matter of the business relationship, regular monitoring business transactions of the customer and checking the consistency of customer's activities with the nature of the business relationship and the usual scope and type of the customer's business.

The actions and measures specified in Article 7 of the Law must be carried out by the obligor when establishing a business relationship, or when withdrawing winnings, depositing stakes, or in both cases, when transactions amounting to 2,000 euros or more in dinar equivalent are conducted, regardless of whether they are a single transaction or several interrelated transactions (Article 8, Paragraph 3 of the Law). The obligor is required to carry out these actions and measures before establishing the business relationship or before executing the transaction.

The obligor is also obligated to apply the actions and measures for customer due diligence with the frequency and intensity corresponding to the assessed risk and changing circumstances related to the customer.

Identifying the customer and verifying its identity

Obligors are required to identify a customer and verify its identity before establishing a business relationship.

The obligor identifies and verifies the customer's identity based on documents, data, or information obtained from reliable and credible sources or through electronic communication means in accordance with the Law, by reviewing the appropriate identification document, which is an official personal document.

If the obligor doubts the authenticity of the collected data or the credibility of the documents from which the data was obtained, they are required to obtain a written statement from the customer regarding the truthfulness and credibility of the data and documents.

When identifying an individual, the obligor must obtain a photocopy or an extract printout of that person's identification document. An extract printout is also considered a digitalized document, which must include a qualified electronic seal or qualified electronic signature, along with an associated timestamp. On the photocopy or extract printout of the personal identification document in paper form, the date, time, and the name of the person who reviewed the document must be noted. The obligor is required to retain the photocopy or extract printout of the personal document in paper or electronic form in accordance with the law. The electronic form must contain a qualified electronic seal or a qualified electronic signature, along with an associated timestamp.

Additionally, the obligor may determine and verify the identity of a customer who is a natural person based on the customer's qualified electronic certificate, under the conditions and in the manner prescribed by Article 18 of the Law.

Special case of identification and verification of identity of a customer when entering a casino

Article 24 of the Law provides for a special case of identification and verification of the identity of a customer when entering a casino. It stipulates that the obligor/organiser of special games of chance in casino is required to determine and verify the identity of the customer and obtain the information referred to in Article 99, paragraph 1, points 4) and 6) of the Law, which refers to the name and surname, date and place of birth, and place of permanent or temporary residence of the natural person entering the casino, as well as the date and time of entry into the casino. The obligor is also obliged to obtain a *written statement* from the customer in the casino, in which the customer declares, under civil and criminal liability, that they are participating in the games of chance for their own account and in their own name.

Identification and verification of identity without the customer's physical presence (non-face-to-face customer)/games of chance through means of electronic communication

Article 39 The Law stipulates that if, during the identification and verification of identity, the customer is not physically present at the obligor, the obligor is required, in addition to the general actions and measures set forth by Article 7, paragraph 1 of the Law, to take some additional measures, such as: obtaining additional documents, data, or information to verify the customer's identity; additional verification of submitted documents or further confirmation of the customer's data; ensuring that the first payment to the account opened by the customer with the obligor is made from the customer's account opened at a bank or similar institution in accordance with Article 17, paragraphs 1 and 2 of the Law, before any other transactions are carried out with the obligor and other measures determined by the supervisory authority.

In the case of organisers of games of chance through means of electronic communication, the fact that the players are not physically present complicates the process of verifying the customer's identity In this context, obligors may identify customers by asking personal information, including name, home address, and date of birth. All of this information must be verified. It is also useful to obtain information about the "sources of funds" and the level of legitimate income (e.g., occupation). This information can help obligors assess whether the customer's level of gambling is within their approximate income range or if it appears suspicious. Proof of identity can be verified using documents provided by the customer (e.g., passport, driver's license, bank statement, utility bills, etc.), or through electronic evidence.

Business operations that do not involve face-to-face contact may carry certain risks and require alternative or additional compliance methods to compensate for the fact that obligors cannot verify the customer's physical appearance based on identity documents with a photograph.

Publicly available data sources can be particularly valuable for identifying politically exposed persons and individuals who are subject to various sanctions due to activities related to organised crime and/or terrorism financing. Obligors should use all available data searching options (e.g., various publicly accessible registers, subscriptions to organisations that provide searches of different business activities, legal sources, and media, internet search engines) to verify the information provided by the customers in the questionnaire, where they submit personal data. This will help achieve an acceptable level of reliability, credibility, authenticity, and acceptability of the data.

Some commercial agencies, which have access to many data sources available through internet search engines, can provide obligors with complex and comprehensive electronic verifications. Given that these agencies use different databases, they can access high-risk alerts, using specific data sources to identify high-risk individuals. Negative information includes the consideration of lists of individuals known to be associated with frauds, including identity fraud and registered individuals. On the other hand, positive information regarding full name, current address, and date of birth can confirm that an individual exists, and some may offer a higher level of trust than others. Verification of such information may

be appropriate in cases where other factors present an increased risk of fraud due to misrepresentation. When using electronic identification systems, the obligor must be satisfied that the data provider is sufficiently reliable and accurate. The obligor must also ensure that the electronic verification process meets the standard level, or confirmation, prescribed by law, and that the supervisory authority can rely on them (example of verification: one match with full name and current address, and another match with the full name of the customer and their current address and date of birth).

In the above cases, where there is no "face-to-face" contact, or when the customer is not physically present during the identification and verification of identity, the obligor applies enhanced measures and actions for customer due diligence.

Based on everything stated above, the primary task of the obligor/organiser of special games of chance in casinos and games of chance through means of communication is to ensure the availability of necessary data related to customer due diligence, to assess whether certain behaviour patterns can be linked to criminal activity and to what extent, and to take all necessary actions and report suspicious activities to the Administration of the Prevention of Money Laundering in accordance with the Law.

In cases where the customer cannot be identified or its identity cannot be verified, or when the obligor reasonably doubts the truthfulness or authenticity of the data or documentation with which the customer verifies their identity, and in situations where the customer is unwilling to or demonstrates an unwillingness to cooperate with the obligor in verifying the truthfulness and completeness of the required data within the analysis, the obligor is required to refuse to establish a business relationship, as well as to refrain from executing the transaction, and has the obligation to terminate the existing relationship with the customer (Article 7 of the Law).

Also, in cases where, during the implementation of actions and measures specified in Article 7 of the Law, the customer suspects that the obligor is conducting such actions in order to provide data to the Administration for the Prevention of Money Laundering, the obligor is required to prepare an official written note and submit it to the Administration.

Simplified customer due diligence actions and measures

Simplified actions and measures of customer due diligence are undertaken in cases and in the manner prescribed by the Law and its by-laws, and are applied to customers with a low risk of money laundering and terrorist financing.

Pursuant to Article 42, paragraph 2 of the Law, the obligor may perform simplified actions and measures of customer due diligence in cases where, in accordance with the provisions of Article 6 of the Law, it is assessed that due to the nature of the business relationship, the form and manner in which the transaction is conducted, the business profile of the customer, or other circumstances related to the customer, there is a negligible or low risk of money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction.

When performing simplified actions and measures of customer due diligence, the obligor is obliged to establish an adequate level of monitoring of the customer's activities so that they are capable of detecting unusual and suspicious transactions.

Enhanced customer due diligence actions and measures

In addition to general measures, the obligors are required to apply enhanced actions and measures of customer due diligence when a certain customer, service or transaction is categorized as high risk for money laundering or terrorist financing.

Article 35 of the Law provides that enhanced actions and measures of customer due diligence include additional measures performed by the obligor, such as: *when implementing new technologies and services; when establishing a business relationship or executing a transaction in the amount of 15.000 euro or higher with a customer who is an official; when a customer is not physically present during identification and verification of identity; when establishing a business relationship or carrying out a transaction with a customer from a country which has strategic deficiencies in the system for the prevention of money laundering and terrorist financing.*

In addition to the cases specified above, the obligor is required to apply enhanced customer due diligence actions and measures also in circumstances when, in accordance with the risk analysis referred to in Article 6 of the Law, it assesses that due to the nature of business relationship, form or manner of execution of a transaction, customer's business profile or other circumstances related to a customer there exists or there may exist a high level of risk of money laundering., terrorist financing or risk of financing of the proliferation of weapons of mass destruction.

The obligor is also required to define, through internal regulations, which enhanced actions and measures will be applied, and to what extent, in each specific case.

New technologies and new services

According to Article 37 of the Law, the obligor is required to assess the risk of money laundering and terrorist financing with respect to any new service offered as part of their activities, new business practices, and the methods of delivering the new service, before its introduction. Additionally, the obligor must assess the risk associated with the use of modern technologies in the provision of existing or new services and take additional measures to mitigate and manage these risks.

Official

The obligor shall establish a procedure to determine whether a customer is an official, a close family member of an official, or a close associate of an official. The obligor is required to define the procedure for determining whether the customer is an official in its internal regulations.

If the customer is an official, a close family member of an official, or a close associate of an official, in addition to the general actions and measures set out in Article 7, paragraph 1 of the Law, the obligor is, in accordance with Article 38 of the Law, required to obtain information about the origin of the property involved in the transaction, through documents and other documentation submitted by the customer. If this information cannot be obtained in the described manner, the obligor must obtain a written statement directly from the customer regarding the origin of the property and gather information about all assets owned by the official, both from publicly available and other sources, as well as directly from the customer. Furthermore, the obligor is obliged to ensure that the employee responsible for establishing a business relationship with the official obtains written consent from a member of the top management, as per Article 52, paragraph 3 of the Law, before establishing that relationship and monitors, with due diligence, the transactions and other business activities of the official throughout the course of the business relationship.

If the obligor determines that the customer has become an official during the business relationship, it must obtain written consent from a member of the top management for continuing the business relationship with that individual, as per Article 52, paragraph 3 of the Law.

The information regarding whether a specific person is an official or not must be obtained from a specially signed statement, which must be drafted in both Serbian and English for officials from other countries and international organisations.

The written statement must contain at least the following information:

1) full name, place of permanent residence, date and place of birth of the customer, number, type, and name of the authority who issued the valid identity document;
2) a statement on whether the customer is considered an official (politically exposed person) under the criteria set out in the Law;
3) information about the type of politically exposed person (whether the it is a person who performs or has been performing a prominent public function during the last four years, or a family member or close associate of a politically exposed person);
4) information about the period during which the individual held the prominent public function, if the customer is a person who has held such a position in the last four years;
5) information about the type of public function the person performs;
6) details on family relations, if the customer is a family member of a politically exposed person;
7) details of the form and nature of the business relationship, if the customer is a close associate of the official;
8) customer's signature.

The obligor may obtain information about the official by reviewing public and other available data, such as: The register of officials maintained by the Anti-Corruption Agency, electronic commercial databases (e.g., *World-Check, InCode, Factiva, LexisNexis*, etc.), its internal database, if available, and others.

An international organization conducting a mission in the Republic of Serbia is obliged to publish and update the list of prominent public officials in that international organization, in accordance with Article 3, Item 26 of the Law, and provide this list to the Administration for the Prevention of Money Laundering immediately after publication and update.

If the customer is a family member of the official or a close associate of the official, the obligor shall apply enhanced customer due diligence measures to that customer as well.

These actions and measures must also be applied when a person ceases to hold a public function (former official), for as long as necessary to conclude that the person has not abused their position, or for four years after ceasing to perform that function.

Countries that do not apply standards in the area of anti-money laundering and counter-terrorist financing

The obligor is required, when establishing a business relationship or conducting a transaction where no business relationship has been established, with a customer from a country that has strategic deficiencies in its anti-money laundering and counter-terrorist financing system, to apply enhanced customer due diligence measures as prescribed by Articles 41, Paragraphs 2 and 3 of the Law.

The Law defines strategic deficiencies in the anti-money laundering and counter-terrorist financing system, which particularly relate to:

- legal and institutional framework of the country, especially the criminalisation of the criminal offences of money laundering and terrorism financing, customer due diligence actions and measures, provisions governing the keeping of data, provisions governing reporting of suspicious transactions, availability of accurate and credible information on beneficial owners of legal persons and persons under foreign law;
- powers and procedures of relevant state authorities of these countries in relation to money laundering and terrorism financing;
- effectiveness of the system for the fight against money laundering and terrorism financing in eliminating money laundering and terrorism financing risks.

In the cases described, the obligor is required to apply enhanced due diligence measures when, in accordance with the risk analysis, they assess that due to the nature and manner of the transaction, the business profile of the customer, or other circumstances related to the customer, there is or could be a high degree of risk for money laundering or terrorist financing. The obligor is then required to gather information about the origin of the property involved in the business relationship or transaction, collect additional information regarding the purpose and intended use of the business relationship or transaction, further verify submitted documents, obtain approval from a member of top management in accordance with Article 52, Paragraph 3 of the Law, and take other appropriate measures to mitigate the risk. The obligor is required to define in its internal acts the enhanced measures and procedures to be applied in each specific case and to what extent.

The obligor must also implement enhanced due diligence of the business relationship and transactions carried out by the customer in the following ways: Increase the frequency and number of controls performed and identify patterns or methods of executing transactions that require further examination; ensure more frequent reporting by compliance officer and restrict business relationship or transactions with those customers.

The Minister, at the proposal of the Administration for the Prevention of Money Laundering, establishes a list of countries with strategic deficiencies, taking into account the lists of relevant international institutions, as well as reports on the assessment of national systems for combating money laundering and terrorist financing issued by international institutions.

II Submission of data to the administration for the prevention of money laundering

The obligor is required to submit data to the Administration for the Prevention of Money Laundering whenever there is a suspicion that a transaction or customer may involve money laundering or terrorist financing, in the manner, form, and within the deadlines prescribed by the Law and the regulation by which the Administration for the Prevention of Money Laundering more closely defines the methodology for conducting business in accordance with the Law.

The obligor is also required to submit data to the Administration for the Prevention of Money Laundering on every cash transaction amounting to €15,000 or more in the dinar equivalent, immediately after the transaction is executed, and no later than 3 days from the date of the transaction. The data must include the name and surname, date and place of birth, permanent or temporary place of residence, and personal number (JMBG) of the natural person, the type and number of the personal document, the name of the issuing authority, the date and place of issuance, as specified in Article 99, Paragraph 1, point 3 of the Law, as well as the data specified in Article 99, Paragraph 1, points 7–10 of the Law, which include the date and time of the transaction; the value of the transaction and the currency in which it was executed; the purpose of the transaction; as well as the name and surname, place of permanent residence, or business name and registered offices of the entity to whom the transaction is directed, and the method of executing the transaction.

The obligor is required to submit data to the Administration for the Prevention of Money Laundering as specified in Article 99, Paragraph 1 of the Law, even when there are grounds for suspicion that a transaction or customer involves money laundering or terrorist financing, in the manner and within the deadlines set out in Article 47 of the Law.

An employee of the obligor who establishes that there are grounds for suspicion of money laundering or terrorist financing must immediately notify the compliance officer or their deputy. The obligor must organise the procedure for reporting suspicious transactions between all organisational units and the compliance officer, and in doing so, must define, primarily:

- the manner of reporting the data;
- the type of data to be submitted (data on the customer, reasons for suspicion of money laundering, etc.);
- the method of cooperation between the organisational units and the compliance officer;
- the procedure to follow in relation to the customer if the Administration for the Prevention of Money Laundering temporarily suspends the execution of a transaction;
- the role of the responsible person of the obligor when reporting a suspicious transaction;
- the prohibition on disclosing information that data, information, or documentation will be submitted to the Administration for the Prevention of Money Laundering;
- the measures to be taken regarding continued business relations with the customer (termination of the business relationship, application of enhanced customer due diligence, monitoring future activities of the customer).

III Compliance officer and ensuring conditions for their work

The risk management process involves multiple participants and structures, each with its own roles, authorities, and responsibilities. The obligor is required to appoint a compliance officer and their deputy for performing certain actions and measures for the prevention and detection of money laundering and terrorist financing, in accordance with Articles 49-52 of the Law.

The compliance officer and his deputy must meet the requirements set in Article 50, paragraphs 1 and 2 of the Law, which are:

1) to be employed at the obligor in a position with powers allowing for an effective, efficient and good quality performance of all tasks laid down in this Law;

2) not to have been sentenced by a final court decision or subject to any criminal proceedings for criminal offences prosecuted ex officio rendering him unsuited for the job of a compliance officer;

3) be professionally qualified for the tasks of prevention and detection of money laundering and terrorism financing;

4) be familiar with the nature of the obligor's business in the areas vulnerable to money laundering or terrorism financing.

5) have a licence to perform the tasks of a compliance officer in case that the obligor is required, by the Regulation on the Professional Examination for Issuing a License to Perform the Duties of Compliance Officer, which is in effect from 1 January 2021, required to ensure that the compliance officer holds such a license.

The aforementioned Regulation prescribes the content and manner of taking the professional examination, as well as the criteria based on which it is determined whether the obligor is required to ensure that their compliance officer and deputy hold a licence to perform the duties of a compliance officer.

In accordance with the provisions of the Regulation, the criteria based on which it is determined whether the obligor is required to ensure that their compliance officer holds a licence to perform the duties of a compliance officer are as follows:

1) if the compliance officer does not hold an international certificate/licence in the field of anti-money laundering and counter-terrorist financing issued by a relevant international organisation/body;

2) if the compliance officer does not hold a certificate of having passed a professional examination for performing duties within their field of activity, which includes prior assessment of knowledge in the area of anti-money laundering and counter-terrorist financing;

3) if the compliance officer is not employed by an obligor with fewer than seven employees.

The deputy compliance officer must meet the same requirements as the compliance officer.

The Administration for the Prevention of Money Laundering issues a licence to the compliance officer and their deputy based on the results of the professional examination, and the licence is valid for five years.

The compliance officer is responsible for establishing, operating and developing the system for the prevention of money laundering and terrorist financing, and initiates and proposes measures for its improvement; participates in the drafting of internal acts; contributes to the development of internal control guidelines; participates in the establishment and development of IT support; takes part in the preparation of professional education, training and professional development programmes; and ensures accurate and timely submission of data to the Administration for the Prevention of Money Laundering in accordance with the law.

The deputy compliance officer replaces the compliance officer in their absence and performs other duties in accordance with the obligor’s internal act.

The obligor’s top management defines the system for the prevention and detection of money laundering and terrorist financing, including internal policies and procedures, adopts the internal strategy, establishes, maintains and ensures the conditions for implementing activities in the risk management process, and provides the highest level of support, commitment and dedication to the risk management process. The obligor is required to prescribe the manner of cooperation between the compliance officer and other organisational units.

The obligor must provide the compliance officer with: unrestricted access to data, information and documentation necessary for the performance of their duties; appropriate human, material, IT and other resources; suitable spatial and technical conditions that ensure an adequate level of protection for the confidential data held by the compliance officer; continuous professional training; a replacement during their absence; protection against the disclosure of their personal data to unauthorised persons, as well as protection from any other actions that could hinder the smooth performance of their duties.

Effective communication is carried out both vertically and horizontally within the obligor. All employees receive clear messages from management regarding their responsibility for risk management and the way in which their individual activities are linked to the work of other organisational units and employees.

Managers of organisational units must ensure that communication effectively conveys the objectives, importance and relevance of effective risk management, the risk appetite and tolerance, as

well as the roles and responsibilities of employees in implementing risk management components.

Management must ensure that employees adhere to internal procedures and established policies. It should promote a culture of business ethics and ethical behaviour among employees, and continuously strengthen employee capacity, knowledge and awareness of the importance of reviewing and updating risk assessments and of effective risk management.

The obligor must submit to the Administration for the Prevention of Money Laundering the full name and job title of the *compliance officer* and *their deputy*, as well as the full name and job title of the top management member responsible for the implementation of the Law, and any changes to that information must be reported no later than 15 days from the date of appointment.

IV Education, training and professional development

The obligor is required to ensure regular professional education, training and development of employees performing tasks related to the prevention and detection of money laundering and terrorist financing.

This also includes familiarisation with:

- the provisions of the *Law on the Prevention of Money Laundering and Terrorist Financing*; regulations adopted based on this Law and internal acts;
- the *list of indicators* for identifying customers and transactions for which there are grounds to suspect money laundering or terrorist financing,
- provisions of regulations governing the freezing of assets with the aim of *preventing terrorism and the proliferation of weapons of mass destruction*; and
- regulations governing *personal data protection.*

The obligor is required to prepare an annual programme of regular professional education, training and development for employees in the area of prevention of money laundering and counter-terrorist financing no later than the end of March for the current year. The programme must include at least the following:

1) the planned number of training sessions at the annual level;

2) the planned number of employees who will attend the training sessions, as well as the profile of employees the training is intended for;

3) topics in the field of money laundering and terrorist financing prevention to be covered by the training, as well as topics related to asset freezing for the purpose of preventing terrorism and the proliferation of weapons of mass destruction;

4) the training delivery methods (seminars, workshops, etc.).

The obligor is required to carry out the training sessions prescribed in the annual programme of professional education, training and development during the year for which the programme was adopted, and no later than the end of March of the following year, in accordance with Article 53, paragraph 1 of the Law, and to prepare a report on the sessions.

The report must contain at least the time and place of the training, the number of employees who attended, the full name of the person who delivered the training and a brief summary of the topic covered.

V Internal control, internal audit and employee integrity

The obligor is required, as part of its activities aimed at effective risk management related to money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction, to conduct regular *internal control* of the performance of tasks related to the prevention and detection of money laundering, terrorist financing, and financing of the proliferation

of weapons of mass destruction, in accordance with Article 54 of the Law. Internal control is conducted based on the identified level of risk.

The purpose of internal control is to prevent, detect, and correct deficiencies in the application of the Law, and to improve internal systems for identifying individuals and transactions suspected of involving money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction.

In conducting internal control, the obligor must verify and test the implementation of systems and procedures for preventing money laundering, terrorist financing, and the financing of proliferation, using random sampling or other appropriate methods.

When changes occur in business processes (such as organisational changes, changes in business procedures, or the introduction of new services), the obligor needs to review and adjust its procedures as part of internal control to ensure compliance with the Law.

The obligor conducts a compliance review of its systems and procedures for applying the Law and internal procedures at least once a year, as well as each time changes are introduced, no later than the date such changes take effect.

By means of its internal act, the obligor defines the responsibilities and authorisations of the governing bodies, organisational units, compliance officers, and other relevant parties involved in carrying out internal control, along with the method and schedule of these activities.

The obligor prepares an annual report on internal control activities and the measures taken as a result, no later than 15 March of the current year for the previous year.

The annual report must include the following information:

1) total number of reported cash transactions amounting to EUR 15,000 or more, in dinar equivalent;

2) total number of reported individuals or transactions suspected to be linked to money laundering or terrorist financing;

3) total number of individuals or transactions suspected to be linked to money laundering or terrorist financing, reported by employees to the compliance officer but not reported to the Administration for the Prevention of Money Laundering;

4) total number of business relationships established where customer identity was verified based on the customer's qualified electronic certificate;

5) frequency of use of individual indicators for identifying suspicious transactions reported to the compliance officer by employees;

6) total number of internal controls conducted, along with findings (number of errors identified and corrected, description of identified issues, etc.);

7) measures taken based on internal control findings;

8) internal control of information technologies used for the implementation of the Law (ensuring the protection of electronically transmitted data, maintaining customer and transaction data in a centralised database);

9) overview of the training programme related to the prevention and detection of money laundering and terrorist financing, including the place and person delivering the training, number of employees trained, and an assessment of further training needs;

10) measures taken to safeguard classified data;

The obligor is required to submit the report to the Administration for the Prevention of Money Laundering and the supervisory authority for the implementation of the Law, upon their request, within three days from the date of the request submission.

The obligor is also required to organise an independent *internal audit* which includes regular assessment of adequacy, reliability, and efficiency of the

system for management of risks of money laundering and terrorist financing when the law governing the activities of the obligor stipulates the obligation for an independent internal audit, or when the obligor assesses that, considering the size and nature of the business, an independent internal audit is necessary in accordance with the Law.

The obligor must also establish a *procedure for verifying, when employing* for a job subject to the provisions of the Law on the Prevention of Money Laundering and related regulations, whether the candidate has been convicted of criminal offences involving unlawful financial gain or criminal offences related to terrorism. In this process, other criteria are also checked to ensure that the job candidate meets high professional and moral standards.

VI Preparation of the indicator list

The obligor is required to prepare a list of indicators for identifying persons and transactions for which there are grounds for suspicion that they involve money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction. When preparing the list of indicators, the obligor must include those indicators developed by the competent authority, which are published on the website of the Administration for the Prevention of Money Laundering.

In preparing the list of indicators, the obligor, among other factors, takes into account the complexity and scope of the transaction, the unusual manner of execution, the fact that the transaction is disproportionate to the usual or expected business of the customer, as well as other circumstances related to the status or other characteristics of the customer.

The obligor is required to apply the list of indicators when determining the grounds for suspicion of money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction, and to consider other circumstances that may indicate grounds for suspicion of money laundering or terrorist financing. It is particularly important that all employees are familiar with the indicators and trained to identify and address the risks of money laundering, terrorist financing, or the financing of the proliferation of weapons of mass destruction within the scope of their work.

VII Data protection, storage and record keeping

The obligor is required to store the data and documentation related to the customer, the established business relationship with the customer, the risk analysis performed, and the executed transaction, obtained in accordance with the law, as well as the customer’s file, for at least five years from the completion of the business relationship, the executed transaction, or the last entry into the casino, in accordance with Article 95, paragraph 1 of the Law.

The obligor is also required, in accordance with Article 95, paragraph 3 of the Law, to store the data and documentation on the compliance officer, deputy of the compliance officer, professional training of employees, and completed internal controls for at least five years from the termination of the compliance officer's duties, the completion of staff training, or the execution of internal controls.

The obligor must handle the above-mentioned data in accordance with the law regulating personal data protection and is required to delete this data after the expiration of the five-year period.

Exceptionally, the obligor may retain and further process the mentioned data after the expiration of the above period, only if the data is not used by competent authorities for special purposes. The extension of the retention period is carried out based on a detailed assessment by the competent authorities and may not exceed an additional five years.

The prohibition on disclosure, under which certain data specified in Article 90 of the Law must not be revealed to the customer or a third party, applies to the obligor, its employees,

including members of the management, supervisory, and other governing bodies, as well as other persons who have access to such data.

VIII Implementation of actions and measures in business units and subsidiaries of a legal entity majority-owned by the obligor - Article 48 of the Law

Article 48, paragraph 1 of the Law stipulates that the obligor must ensure that the actions and measures for the prevention and detection of money laundering and the financing of terrorism, identical to those prescribed by this law, are implemented to the same extent in its business units and subsidiaries of a legal entity in which it holds a majority ownership, regardless of whether their place of business is located in the Republic of Serbia or in foreign countries.

Article 48, paragraph 14 provides that provisions of this Article are also applicable to the obligor who is a member of a non-financial group, within the meaning of the law regulating the activity of that obligor.

IX Implementation of other actions and measures

Data protection

The obligor, or its employees, including members of the management, supervisory, and other governing bodies, as well as other persons with access to the data referred to in Article 99 of the Law, must not disclose to the customer or third party the information defined in Article 90, paragraph 1, points 1) - 4) of the Law. Article 90, paragraph 2 of the Law also specifies cases to which this prohibition does not apply.

Record keeping

In accordance with Article 98 of the Law, the obligor must maintain records of data regarding customers, business relationship and transactions outlined in Article 8 of the Law, as well as data referred to in Article 99, paragraph 1, points 4) and 6), 7), 10), 11) and 12) of the Law, and information submitted to the Administration for the Prevention of Money Laundering in accordance with Article 47 of the Law (cash transactions over 15.000 euro or the equivalent in dinars, suspicious transactions).

The obligor is required to keep records of data and information collected in accordance with the Law and related regulations in electronic form, as well as documentation related to that data and information, in chronological order, in a manner that ensures adequate access to those data, information, and documentation.

The obligor must ensure appropriate searching of records about data and information stored in electronic form, at a minimum based on the following criteria: name and surname, date of transaction, transaction amount, currency of the transaction.

The obligor determines, through its internal acts, the method and location for storing this data, information, and documentation, as well as the individuals who have access to it.

Protection of the integrity of the compliance officer and employees

The obligor is required to take necessary measures to protect the compliance officer and employees who implement the provisions of the Law from exposure to threats, violent or repressive actions, or any other hostile actions, especially from unfavourable or discriminatory actions aimed at their physical or psychological integrity in the workplace.

The compliance officer and employees who have been subjected to any of the aforementioned actions due to the implementation of the provisions of the Law have the right to judicial protection in accordance with the law.

X Internal acts

In accordance with the provisions of the Law, the obligor is required to adopt and apply appropriate internal acts that will cover all actions and measures for the prevention and detection of money laundering and terrorist financing, as defined by the Law, the regulations enacted based on the Law, and these guidelines, for the effective management of money laundering and terrorist financing prevention. In its internal acts the obligor must take into account the identified risks of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. These acts must be proportional to the nature and scope of the business, as well as the size of the obligor, and must be approved by the member of top management. The obligor must ensure the application of these internal acts by establishing appropriate procedures and mechanisms for internal control.

Specifically, the obligor's internal acts must regulate:

- the process of conducting a risk analysis for money laundering and terrorist financing
- procedures and mechanisms for detecting suspicious transactions and/or customers, as well as the manner in which employees should proceed after recognising such transactions and the process for submitting information, data, and documentation within the obligor's organisation
- determining the persons responsible for fulfilling obligations under the Law—compliance officers and their deputies—and ensuring the conditions for their work
- determining the risk categories of customers, services, and transactions
- the procedure for implementing customer due diligence actions and monitoring, regular monitoring in accordance with the established risk category, including verifying the client's activities against typical behaviour, as well as potential changes in the risk category
- the procedure for conducting enhanced due diligence actions and measures for high-risk customers, especially in determining whether a customer is an official
- the procedure for regular internal control of performing the obligations under the Law
- the procedure for conducting regular professional training, education, and development
- procedures for internal reporting of violations of the Law via a dedicated and anonymous communication channel.
- maintaining records, protecting, and storing data from those records

A component of the internal acts is also a list of indicators for identifying individuals and transactions for which there are grounds to suspect that they are related to money laundering, terrorist financing, or the financing of weapons of mass destruction.

To ensure the proper implementation of the provisions of these internal acts, it is particularly important that relevant employees are familiar with them and their obligations and responsibilities arising from these acts.

APPLICATION OF THE GUIDELINES

Obligors are required to align their operations with the content of the Guidelines and to develop internal acts in accordance with the provisions of the Law on the Prevention of Money Laundering and Terrorist Financing.

The Guidelines enter into force on the day of adoption and will be published on the website of the Game of Chance Administration www.uis.gov.rs