(Coat of arms)
Republic of Serbia
MINISTRY OF FINANCE
GAMES OF CHANCE ADMINISTRATION
No.: 424-01-159/2022-01
Belgrade, March 31, 2022

Pursuant to Article 6, paragraph 1 of the Law on the Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Serbia", No. 113/17, 91/19, 153/20 - hereinafter: the Law), Article 114, and in conjunction with Article 104, paragraph 1, item 4a) and Article 110, paragraph 3 of the Law, the Director of the Games of Chance Administration issues the following

GUIDELINES FOR THE ASSESSMENT OF RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM FOR OBLIGED ENTITIES WHO ORGANIZE SPECIFIC GAMES OF CHANCE IN GAMING VENUES AND GAMES OF CHANCE THROUGH MEANS OF ELECTRONIC COMMUNICATION

The Games of Chance Administration, according to Article 104, paragraph 1, item 4a) and Article 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 and supervision in the field of games of chance, supervises the application of this Law by the obliged entities referred to in Article 4, paragraph 1, item 8) of the Law, i.e. by the organizers of special games of chance in gaming venues and the organizers of games of chance through means of electronic communication, who perform their activities on the basis of the special law.

According to Article 114 of the Law, the Games of Chance Administration can, independently or in cooperation with other authorities, issue recommendations, i.e. guidelines for the application of the provisions of the Law on the Prevention of Money Laundering and Financing of Terrorism.

In order to further improve the system of combating money laundering and financing of terrorism, amendments to the Law on the Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Serbia", No. 91/19) were adopted and entered into force on January 1, 2020, as well as amendments to the Law on the Prevention of Money Laundering and Financing of Terrorism ("Official Gazette of the Republic of Serbia", No. 153/20), which are in force from June 29, 2021, except for Article 18, paragraph 8, Article 19, paragraph 7, and Article 21, paragraph 7 of the Law, which are in force from December 29, 2021.

Also, in September 2021, the National Risk Assessment was adopted, and the results of the mentioned risk assessment provide necessary information to obliged entities and serve as a starting point, but also a mandatory basis in the assessments they carry out themselves.

The aim of the guidelines is to define the bases and/or assumptions based on which obliged entities should perform an assessment of the risk of money laundering and financing of terrorism in relation to their business, as well as the way of carrying out risk assessment/analysis on an individual case, for the purpose of uniform application of the provisions of the Law and the establishment of an effective system of prevention of money laundering and financing of terrorism by obliged entities.

The guidelines for assessing the risk of money laundering and financing of terrorism are adopted for the purpose of adequately assessing susceptibility to the risk of money laundering and financing of terrorism, creating a risk analysis and regularly updating it, developing risk recognition and management procedures, in order to apply the provisions of the Law on the Prevention of Money Laundering and Financing of Terrorism in a uniform manner.

The system must ensure that the risks are comprehensively identified, analyzed, assessed, monitored, mitigated and managed in the best possible way. Obliged entities can apply these measures to different extents, depending on the type and level of risk and according to different risk factors.

MONEY LAUNDERING - DEFINITION AND PHASES

Money laundering is the process of concealing the illegal origin of money or property obtained through crime.

Money laundering, in terms of the Law, is considered to be:

- conversion or transfer of property acquired by committing a criminal offense;
- concealment or inaccurate representation of the true nature, origin, location, movement, disposition, ownership or rights in connection with the property acquired through the execution of a criminal offense;
- acquisition, possession or use of property acquired through the execution of a criminal offense.

Money laundering, in terms of the Law, also includes the aforementioned activities carried out outside the territory of the Republic of Serbia.

Money laundering includes numerous activities undertaken in order to conceal the origin of property benefits obtained by committing a criminal offense. The process of money laundering can involve a whole series of transactions, in which property acquired through the commission of a criminal offense represents the input value, while "legitimate" goods and services are the output value of such transactions.

Money laundering is a process that can be divided into three basic phases, but it should be kept in mind that in practice they sometimes overlap or some of them are missing.

1) The first phase is the severance of the direct connection between the money and the illegal activity by which it was acquired and is called the ***"investment" phase***. In the investment phase, illegally acquired money is introduced into legal financial flows. There are many ways in which this can be accomplished. One of the ways is to deposit cash obtained through criminal activities into bank accounts, most often under the pretext of some regular activity where payment is made in cash, such as restaurants, commissions, boutiques, casinos, etc.
2) The second phase is the ***phase of "layering" or the phase of "concealment".*** After the money has entered the legal financial system, it is transferred from the account in which it was deposited to other accounts of business companies with the aim of showing some fictitious business activity or carrying out some legal business The main goal of these transactions is to conceal the connection between the money and the criminal activity from which it originates.
3) The third phase, ***the "integration" phase***, is the last phase in this process, after which "dirty" money appears as money originating from legally permitted activities. A common

method of integrating "dirty" money into legal financial flows is the purchase of real estate or the purchase of controlling packages of shares in joint stock companies, which is an example of the concentration of "dirty" capital on a large scale, and that is the goal of "money launderers". Integration concentrates on market values, i.e. to what can be bought and sold. Once the money reaches this stage, it is very difficult to detect its illicit origin.

FINANCING OF TERRORISM - DEFINITION AND PHASES

The financing of terrorism, in terms of the Law, is considered to be the provision or collection of property or the attempt to provide or collect it, with the intention of using it or with the knowledge that it can be used, in whole or in part:

- for the execution of a terrorist act;
- by terrorists;
- by terrorist organizations

The financing of terrorism also include inciting and assisting in providing and collecting property, regardless of whether a terrorist act was committed and whether the property was used to commit a terrorist act, where the main goal does not necessarily have to be concealing the source of financial funds, but to conceal the nature of the activities which are intended to be financed with those funds.

The financing of terrorism consists of several phases, such as:

1) collection of funds from legal business or from criminal activities;
2) storing the funds that have been collected;
3) transfer of funds to terrorists;
4) use of funds.

The first phase includes the collection of funds from persons who operate legally, but are connected to terrorist organizations or terrorists, or from persons who are connected to criminal activities (e.g. drug trafficking, extortion, embezzlement, etc.). Donations from individuals who support the goals of terrorist organizations or funds that collect money and direct it to terrorist organizations are also a significant source of funds.

In the second phase, the funds are stored, that is, kept directly in the accounts of individuals or in the accounts of intermediaries connected to terrorist organizations.

The third phase includes the transfer of funds to units of terrorist organizations, i.e. individuals, in order to use the money for terrorist activities. Most often, money transfer systems and the banking system are used as mechanisms for money transfer, although informal ways of transfer are present in a large number of cases.

The use of funds becomes obvious when they are used for terrorist activities - the purchase of weapons, explosives, equipment, financing of training camps, propaganda, providing refuge, etc.

Money laundering and financing of terrorism are global issues that can have a negative impact on the economic, political, security and social structure of a country. The consequences of money laundering and financing of terrorism undermine the stability, transparency and efficiency of the state's financial system, cause economic disruptions and instability, harm the country's reputation and threaten national security.

CONCEPT OF RISK AND RISK ASSESSMENT

Risk is a function of three factors: threat, vulnerability, and consequence.

Threat is defined as a person or group of persons, objects, activities that have the potential to cause damage, for example to the state, society, economy, etc. In the context of money laundering, this means persons engaged in criminal activities, terrorist groups and their supporters, the means and assets at their disposal, the environment in which previous (preceding) criminal acts are committed and in which the proceeds of crime are realized, their size and scope.

Vulnerability includes everything that could be exploited in the event of a threat or that could support and facilitate the operation of a threat. In the case of obliged entities, it is everything that makes them particularly exposed to money laundering, i.e. financing of terrorism (insufficient knowledge of regulations governing this area, inadequate application of legal regulations, inadequate training, complex or inadequate organizational structure of obliged entities, unclearly defined obligations in the process, etc.).

Risk assessment represents a judgment about threats, vulnerabilities and consequences and it is the first step towards their mitigation.

Risk assessment:

- ***national risk assessment***
- ***at the level of the obliged entity***
- ***at the level of the business relationship (customers)***

NATIONAL RISK ASSESSMENT

In the Republic of Serbia, the National Risk Assessment was adopted in September 2021, and through the following thematically divided units:

1) ***Money laundering risk assessment***, which was carried out according to the methodology of the World Bank;
2) ***Assessment of the risk of financing of terrorism*** (according to the methodology of the World Bank);
3) ***Assessment of the risk of money laundering and financing of terrorism in the digital assets sector*** (performed according to the methodology of the Council of Europe), and
4) ***Risk assessment of the financing of weapons of mass destruction*** (performed according to the methodology of the RUSI Institute for Defense and Security Studies, using the Guide for conducting a national risk assessment of the financing of proliferation).

The money laundering risk assessment is the result of an assessment of money laundering threats and national vulnerability to money laundering, and the analysis carried out for the Republic of Serbia showed that the overall risk of money laundering is **"medium".**

The document "**National Risk Assessment"** is published on the Administration for the Prevention of Money Laundering website –
http://www.apml.gov.rs/ uploads/ useruploads/Documents/NRA2021.pdf

1) Money laundering risk assessment

The National Money Laundering Risk Assessment is the result of an assessment of threats and national vulnerabilities from money laundering.

Based on the analysis of previous crimes, review of threats by sectors and cross-border threats, the overall assessment of money laundering threats is "medium" with a tendency of "no change".

Sectors that are exposed to a high degree of threat from money laundering are the real estate sector, the sector of organizers of games of chance through means of electronic communication (online) and the banking sector.

It is estimated that the games of chance sector is exposed to a high degree of threat of money laundering through means of electronic communication, taking into account the data on criminal proceedings initiated for the criminal offense of money laundering, i.e. criminal proceedings on the aforementioned basis involving employees in this sector, a small number reported suspicious transactions, the volume of funds that are paid, i.e. the fact that large amounts of money are traded within this sector, etc.

Sectors that are exposed to a medium-high level of threat are money changers, casinos and accountants.

The sector of organizers of special games of chance in gaming venues (casinos) is exposed to a medium-high level of threats from money laundering, first of all bearing in mind that the same represents an active "cash sector", with the turnover of large amounts of cash, a small number of reported suspicious transactions, as well as the average amount per reported suspicious transaction.

The sectors of lawyers, insurance, car sales, real estate brokerage, payment and electronic money institutions, postal operators and providers of services related to virtual currencies, represent sectors that are exposed to a medium level of threat from money laundering. The capital market, factoring and notary public sectors have a medium-low level of exposure to money laundering threats. The lowest degree of exposure to the threat of money laundering has the sectors of providers of financial leasing, voluntary pension fund management companies and voluntary pension funds.

National vulnerability to money laundering is assessed as "medium" based on an analysis of the country's ability to defend against money laundering and an analysis of sectoral vulnerability.

Sectoral vulnerability - national vulnerability, besides the country's ability to defend itself against money laundering threats, is also affected by the vulnerability of certain sectors that can be misused for money laundering, and in this sense, the financial and non-financial part of the system were analyzed during the assessment.

In the financial part of the system, the most vulnerable are banks, payment institutions, public postal operators and electronic money institutions (medium vulnerability), followed by exchange offices, factoring companies and the capital market sector (medium-low), and then life insurance companies, providers of financial leasing and voluntary pension funds (low).

The real estate sector, organizers of games of chance through means of electronic communication (online), organizers of special games of chance in gaming venues (casinos), accountants and postal operators, who were assessed as medium-vulnerable, were identified as the most vulnerable sectors in the non-financial part of the system, followed by lawyers, public notaries and auditing companies, whose vulnerability is assessed as medium-low.

Special games of chance in gaming venues

Gaming venues belong to a sector that is assessed as ***medium-vulnerable*** and has a ***medium-high exposure to the threat*** of money laundering. In this sector, there is a whole series

of elements that increase its vulnerability, and the most significant is the use of cash, which is dominant, as well as the fact that the customers are exclusively natural persons, which can carry specific risks in relation to the jurisdiction from which they come, as well as to exposure to high-risk clients (e.g. politically exposed persons).

Games of chance through means of electronic communication

Organizing games of chance through means of electronic communication, as one of the sectors in the non-financial part of the system, has been assessed as a ***medium-vulnerable*** sector with a ***high exposure to money laundering threats***. In this type of organizing, the exposure to risk is increased due to the large number of transaction flows and the lack of face-to-face interaction. Also, the elements that increase the vulnerability of the sector are the possibility of cash payments (the obliged entity can function as part of a mixed organization that includes machines and bookmakers, the so-called "land-based betting"), which allows cash to be added to registration accounts, etc.

2) ***The assessment of the risk of financing terrorism*** at the national level for the period 2018-2020 is based on the assessment of the threat of terrorism, the threat of financing terrorism at the national level, the sectoral risk of financing terrorism and the country's vulnerability to financing terrorism.

The overall assessment of the risk of financing terrorism in the Republic of Serbia is ***medium low***, taking into account that: the threat of financing terrorism organized by terrorists and terrorist organizations is assessed as low; threat from financing of terrorism at the national level as medium to low; sectoral risk from financing of terrorism as medium; country vulnerability from financing of terrorism as low.

From the aspect of misuse of financing of terrorism, the sectoral risk assessment showed that the financial sector is more susceptible to misuse than the non-financial sector, that is, the products of the following sectors are most susceptible to the misuse of financing of terrorism: issuers of electronic money, payment institutions, public postal operators, authorized money changers, providers services related to real estate, real estate agents and banks.

3) ***Money laundering and financing of terrorism risk assessment in the digital assets sector***

It has been assessed that there is a medium risk of money laundering and financing of terrorism related to transactions with virtual currencies, and a low risk when it comes to investment and user tokens. In the part that refers to service providers that are connected to digital assets, it is estimated that there is a medium risk.

4) ***Assessing the risk of financing the proliferation of weapons of mass destruction (WMD)***

The risk of financing WMD proliferation is assessed as low to medium.

The use of covert persons and companies that provide support for the proliferation of WMD and front entities that operate on behalf of persons under the sanctions regime of the United Nations and international organizations of which the Republic of Serbia is a member can be considered a high degree of threat from the financing of WMD.

The Law on Freezing of Assets with the Aim of Preventing Terrorism and Proliferation of Weapons of Mass Destruction ("Official Gazette of the Republic of Serbia", No. 23/15, 113/17 and 41/18) prescribes, in order to prevent terrorism and the spread of WMD, the actions and measures for regulating the disposal of assets of designated persons, the competence of state authorities for the implementation of those measures, as well as the rights and obligations of natural persons and legal entities in the application of the provisions of this law.

The financing of the proliferation of weapons of mass destruction, in terms of the aforementioned Law, refers to all actions of securing financial resources or actions of providing financial services that are aimed, in whole or in part, at the development, production, acquisition, possession, storage, delivery, provision of brokerage service, transshipment, transport and transfer of weapons of mass destruction, as well as means for their transfer.

APPROACH BASED ON RISK ASSESSMENT

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

Money laundering and the financing of terrorism is a problem that obliged entities must face, so that they do not inadvertently or otherwise enable, encourage or incite it.

It is necessary for obliged entities to adopt a risk-based approach to detect, assess and understand the risks of money laundering and financing of terrorism, in order to direct their resources where the risks are greatest and thus implement appropriate measures to mitigate them.

The analysis of the risk of money laundering and financing of terrorism starts from the assumption that the different products and services that obliged entities offer as part of their business, or the different transactions they perform, are not equally vulnerable to abuse for the money laundering and financing of terrorism. The analysis is performed to enable the application of control measures that are proportionate to the identified risk. It makes it possible for the obliged entity to focus on those clients, countries, products, services, and transactions, which represent potentially the greatest risk.

An approach based on risk assessment also requires documenting the risk assessment, as well as the existence of appropriate internal acts in order to determine the starting points and the application of adequate measures and procedures.

The key elements of a risk-based approach are:

a) ***Identification/recognition*** of business risks that are susceptible to money laundering and financing of terrorism, i.e. detection of risks faced by the obliged entity, taking into account the customers, the types of services provided, and taking into account publicly available information on the risks and typologies of money laundering and financing of terrorism. It would be useful for the obliged entities to make a list of potential factors that they will use to identify threats and vulnerabilities from money laundering, that is, financing of terrorism with the obliged entity. This refers, first of all, to those factors that are recognized as risky at the state level, those that are characteristic of a certain obliged entity, typologies, trends, models of behavior or certain circumstances, etc.

Having in mind that there is no universal model for risk assessment, but different guidelines, ideas, suggestions and examples from domestic and international practice, it is up to the obliged entities to assess which methodology best suits their work.

б) The phase of identification and description of risks is followed by the ***phase of analysis***, which is crucial for risk assessment and which determines the probability that money laundering and financing of terrorism will occur and what their impact would be in that case.

After identifying and considering all relevant factors, the obliged entity makes a decision on the risk levels. Obliged entities can use the risk matrix as a risk assessment method to identify customers that are in the low risk zone, those that are in the slightly higher risk zone, but that risk is still acceptable, and those that carry a high or unacceptable risk of money laundering and financing of terrorism.

Based on the data from the analysis, the same are entered into the risk matrix, and the degree of risk of money laundering to which the obliged entity is exposed to is determined as a final result.

c) ***Risk management*** implies the purposeful use of the results obtained in the risk analysis. Based on the analysis, the obliged entity applies risk management strategies and implements the appropriate business policy, i.e. appropriate procedures with adequate control systems and mechanisms for mitigating or overcoming them. Based on the obtained results, action priorities are defined.

IDENTIFICATION OF RISKS

➢

Recognizing the categories, that is, the types of risks - customer risk, geographic risk, transaction risk and service risk, is the first step in risk analysis, both of the obliged entity and the customer.

Depending on the specifics of the particular obliged entity's business, other categories in which money laundering and financing of terrorism may occur can be taken into account.

Risk analysis, according to Article 6 of the Law, must be proportionate to the nature and scope of the business, as well as the size of the obliged entity and must take into account the basic types of risks, such as:

1) *Geographic risk*

Geographic risk refers to the assessment of exposure to the risk of money laundering and terrorism financing, which depends on the country of origin of the customer, i.e. the person performing the transaction, the area or territory where the obliged entity is located, as well as the country of origin of the ownership and management structure of the games of chance organizer.

Factors that determine whether a particular country or geographic location carries a higher risk of money laundering and financing of terrorism include:

- countries against which the United Nations, the Council of Europe or other international organizations have applied sanctions, embargo or similar measures;
- countries that have been designated by credible institutions (FATF, Council of Europe, etc.) as countries that do not take adequate measures to prevent money laundering and financing of terrorism;

- countries that are designated by credible institutions (FATF, UN, etc.) as countries that support or finance terrorist activities or organizations;
- countries that have been designated by credible institutions (e.g. World Bank, IMF) as countries with a high degree of corruption and crime;
- countries that, as credible sources have shown, do not deliver beneficial ownership information to competent authorities, which can be determined from FATF mutual assessment reports or reports from organizations that also consider different levels of cooperation, such as the OECD Global Forum's reports on compliance with international tax transparency standards.

The list of countries that have strategic deficiencies in the system for combating money laundering and financing of terrorism is published on the website of the Administration for the Prevention of Money Laundering and is based on:

- the FATF (Financial Action Task Force) announcements about countries that have strategic deficiencies in the system for combating money laundering and financing of terrorism and that represent a risk to the international financial system;
- the FATF announcements about countries/jurisdictions that have strategic deficiencies in the system for combating money laundering and financing of terrorism, which, in order to eliminate the identified deficiencies, have expressed determination at the highest political level to eliminate the deficiencies, which for this purpose have created an action plan in cooperation with the FATF and which are required to report on the progress they make in eliminating deficiencies;
- reports on the assessment of national systems for combating money laundering and financing of terrorism by international institutions (FATF and the so-called regional bodies that function according to the model of FATF, such as the Committee of the Council of Europe Moneyval).

Countries that apply standards in the field of preventing money laundering and financing of terrorism that are at the level of European Union standards or higher are:

- EU member states
- third countries (other countries that are not members of the EU) with effective systems for preventing money laundering and financing of terrorism, assessed in reports on the assessment of national systems for combating money laundering and financing of terrorism by international institutions (FATF and the so-called regional bodies that operate on the model of FATF, such as the Committee of the Council of Europe Moneyval);
- third countries (other countries that are not members of the EU) which have been designated by reliable sources (e.g. *Transparency International*) as having low levels of corruption or other criminal activities;
- third countries (other countries that are not members of the EU) which, based on credible sources, such as reports on the assessment of national systems for combating money laundering and financing of terrorism by international institutions (FATF and so-called regional bodies that function on the model of FATF, such as the Committee of the Council of Europe Moneyval) and published reports on the progress of that country in fulfilling the recommendations from the evaluation report, have obligations

prescribed by law to fight against money laundering and financing of terrorism in accordance with FATF recommendations and effectively implement those obligations.

2) *Customer risk*

The obliged entities should describe all types or categories of customers with whom they do business and assess how likely it is that those types or categories of customers will abuse that obliged entity for money laundering or financing of terrorism, such as:

• customer category:
- regular customer;
- VIP customer;
- random customer, etc.
• type of customer:
- the customer who is not visiting for the first time and carries out small to medium transactions;
- the customer who is not visiting for the first time and carries out medium to large transactions;
- the customer who is visiting for the first time and is a citizen of the Republic of Serbia;
- the customer who is visiting for the first time and is not a citizen of the Republic of Serbia, etc.

The customer's risk involves an assessment of whether the customer is associated with a higher risk of money laundering and financing of terrorism and, based on their own criteria, the obliged entities shall determine whether a customer represents a higher risk based on the performed categorization.

The following represent a greater risk:

1) regular customers whose usual behavior changes:
   - customer has permanent or temporary residence in a country and/or region that are on the list of countries that have strategic deficiencies in the system for combating money laundering and financing of terrorism and that pose a risk to the international financial system (this list is on the official FATF website and should be monitored regularly);
   - regular customer who starts spending larger sums of money;
   - regular customer that begins to spend significantly less money, but more often participates in games of chance, etc.
2) customers representing politically exposed persons, that is, domestic and foreign officials;
3) customers from international corporations;
4) random customers, etc.

The above mentioned risk analysis is a general analysis for different types or categories of customers and represents the starting point for categorizing the risk of an individual customer. Based on the circumstances that are characteristic of individual customers, such as their origin and past, that is, on what can be concluded on the basis of the information they provide, the categorization of the given customer is also adjusted, especially taking into account also the following:

Customer risk – gaming venues

The obliged entity independently implements an approach on basis of the customer's risk assessment, based on generally accepted principles and own experience. Customer risk implies an

assessment of whether the customer dealing with the obliged entity is associated with a higher risk of money laundering and financing of terrorism.

The following activities can also indicate a higher risk of customers in the gaming venue:

- for the purposes of identification, the customer provides documents for review, and there are grounds for suspicion that they are falsified, altered or incorrect;
- the customer submits only a copy of the personal identification documents for review;
- the customer protests to provide a document for personal identification at the request of an authorized person in the gaming venue, or there are grounds for suspicion that false information is provided;
- the documents submitted by the customer for identification purposes were issued abroad and there are reasons why it is not possible to verify their authenticity;
- the customer has a permanent or temporary residence in a country and/or region that are on the list of countries that have strategic deficiencies in the system for combating money laundering and the financing of terrorism and that represent a risk to the international financial system (this list is located on the FATF official website and should be monitored regularly);
- the customer is a citizen of a country that does not respect the standards for preventing money laundering and financing of terrorism;
- the customer is a politically exposed person, that is, a domestic and/or foreign official;
- the customer appears in the company of suspicious persons or is known to have been punished for some criminal acts, etc.

Customer risk - games of chance through means of electronic communication

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

- the customer accesses from an IP address (Internet Protocol address) from a country and/or region that are on the list of countries that have strategic deficiencies in the system for combating money laundering and financing of terrorism and that poses a risk to the international financial system (this list is on the FATF official website and should be monitored regularly);
- the customer is a citizen of a country that does not respect the standards for preventing money laundering and the financing of terrorism;
- the obliged entity has knowledge that the customer is trying to hide the IP address;
- the obliged entity has knowledge that the customer has been punished for some criminal acts;
- the customer is a politically exposed person, that is, a domestic and/or foreign official;
- the customer owns cards that were issued in offshore destinations or in countries that are on the list of countries that have strategic deficiencies in the system for combating money laundering and financing of terrorism and that poses a risk to the international financial system (this list is on the official website FATF and should be monitored regularly);
- the customer requests that the realized profit be transferred to another account or to the account of a third party;
- the customer avoids confirming the identity in case of a large gain;
- the customer is interested in certain game packages and makes suggestions for certain packages;
- the customer submits and/or has submitted a request for the registration of multiple user accounts with the same data;

- the customer has several bank accounts and uses them alternately when participating in games of chance;
- bank account/payment card details do not match registered customer details (identity fraud/identity theft), etc.

3) *Transaction, product and service risks*

Transaction means receiving, giving, exchanging, storing, disposing or other disposition of property at the obliged entity, including payment transaction in the sense of the law governing the provision of payment services.

Assets mean things, money, rights, securities and other documents in any form, which can be used to determine ownership and other rights.

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

Cash transaction means the physical acceptance or giving of cash.

Cash transaction with obliged entities/**organizers of special games of chance in gaming venues**, implies the purchase of tokens or a loan for a specific game on a table, i.e. a machine, where by the nature of business a different game is activated on each table or machine, that is, one of the following basic transactions is carried out:

- exchanging money for tokens with a defined value;
- exchanging tokens with a defined value for money;
- exchanging money for credit at the machine;
- exchange of credit at the machine for money, etc.

Other transactions in the gaming venue can be: receiving, giving, exchanging, storing, disposing or otherwise dealing with the property at the obliged entity.

The following transactions also represent a greater risk of money laundering and financing of terrorism in gaming venues:

- several customers buy chips for cash (the transaction is for a slightly lower amount than the amount reported under the Law on Prevention of Money Laundering and Financing of Terrorism), and then gamble with minimal amounts;
- the customer asks a person employed in the gaming venue to monitor his game and to warn him when his winnings approach the amount of the transaction, which according to the law is to be reported to the Administration for the Prevention of Money Laundering;
- the customer, who is a big winner, asks for the support and service of another customer in the gaming venue, in order to collect some chips and thus avoid reporting transactions under the Law on Prevention of Money Laundering and Financing of Terrorism;
- the customer gambles on minimum amounts and soon after goes to the counter to cash in the chips;
- the customer tries to somehow influence the employee in the gaming venue and thus avoid reporting the transaction under the Law, requesting that the refund of cash for tokens or records of his cash transactions be kept in the name of another person;
- two players cover both sides of the same game by betting the same amounts frequently and simultaneously (for example, by betting both black and red, or even and odd in roulette).
- the customer buys chips for cash, invests in a game with a low chance of losing money (e.g. invests simultaneously on red and black on roulette), or engages in minimal gambling or does not gamble at all, and later goes to the cashier to cash in the chips by

demanding denominations that are higher than the denominations with which he purchased the tokens.
- the customer requires a winning certificate, which does not have to be issued in gaming venues;
- a random customer invests large sums of money in games of chance, etc.

The obliged entity/**organizer of games of chance through means of electronic communication** must have defined procedures for money laundering and recording of the total amount of money paid or deposited on registered accounts for playing through means of electronic communication, by each customer.

The following transactions represent a greater risk of money laundering and financing of terrorism for the *organizers of games of chance through means of electronic communication*:

- cash payments are allowed: most payments to the organizer through means of electronic communication are made directly from accounts with financial institutions. However, the obliged entity can operate as part of a mixed organization that also includes betting shops, i.e. the so-called "land-based betting". In this way, the customers have possibility to top up their registered accounts with cash at the incoming/outgoing payment points, and then use the same for "online" games;
- the customer has multiple accounts or online wallets in which he does not individually exceed the amounts of incoming/outgoing payments which must be reported under the Law on Prevention of Money Laundering and Financing of Terrorism;
- transfers between customers: obliged entities may allow or be aware that customers transfer money between themselves without using their registered account with them;
- use of third parties: criminals may use "third parties", either anonymous or identified agents, to gamble certain amounts on their behalf in order to avoid customer's identity check. "Third parties" can be used to gamble on behalf of others with a minimum amount;
- use of registered accounts with obliged entities: without satisfactory internal controls, customers can use these accounts for depositing and withdrawing without gambling and with minimal down payments;
- multi-user account - online wallet: the organizer can own and control multiple websites. Individual websites also offer a variety of different types of gambling. The customers may separate the different types of the games of chance through means of electronic communication, which take place at the same organizer or through the same website for legitimate reasons, e.g. to monitor their performance in different areas. However, users may open multiple accounts or "online wallets" for dishonest and inappropriate reasons, including an attempt to reduce the level of spending, or to avoid the verification threshold level;
- changes in financial institution accounts: customers may have accounts in several financial institutions and may wish to change some of the accounts they use for online betting. This may be for legitimate reasons, or perhaps there may be an intention to confuse the audit trail, or introduce third party transactions without drawing attention;
- identity fraud: account details of financial institutions can be stolen and used on websites. Identity theft can also be successfully used to open accounts with financial institutions and such accounts can be used on websites, through which multiple accounts can be opened to participate in games of chance through means of electronic communication, using stolen identities;
- prepaid cards: using cash to finance a prepaid card presents similar risks as with cash.

The following transactions of the customer with the *provider of games of chance through means of electronic communication* can also indicate a greater risk:

- the customer deposits cash for top-up on his registered account in order to participate in games of chance through means of electronic communication;
- the customer deposits a relatively high amount of money into his registered account and after a certain period withdraws it, without any activities or after very little participation in games of chance;
- the customer regularly invests large sums of money in games of chance, with the lowest acceptable level of loss;
- the customer invests little, but often, and his total annual consumption is large and significantly exceeds the person's annual income;
- several customers often effectively play "against each other", investing large sums on bad hands, expecting to lose from other players (so-called chip dumping);
- different customers are connected to the same bank accounts, which they use, withdraw funds, or deposit their winnings in the games of chance (current account authorizations).

WHAT IS A SUSPICIOUS TRANSACTION?

A transaction may be assessed as suspicious if the obliged entity and/or the competent authority assesses that, in relation to it or the person carrying it out, there are reasons to suspect money laundering or financing of terrorism, i.e. that the transaction includes funds derived from illegal activities.

All transactions that are unusual by their nature, scope, complexity, value or connection, i.e. do not have a clearly visible economic or legal basis, or are disproportionate to the usual or expected business of the customer, as well as other circumstances, which are related to the status or other characteristics of the customer, can be treated as suspicious.

The assessment of the suspiciousness of a particular customer, transaction or business relationship is based on the suspiciousness criteria specified in the list of indicators for identifying persons and transactions for which there are grounds for suspicion of money laundering or financing of terrorism. The list of indicators is the starting point for the obliged entity’s employees and authorized persons when recognizing suspicious circumstances related to a certain customer, the transaction the customer performs or the business relationship it concludes, and in this sense the obliged entity’s employees must be familiar with the indicators in order to use them in their work. However, a transaction may be suspicious without meeting any of the indicators. In this sense, it is necessary to look at a broader framework, in accordance with the principle that the obliged entities know their clients best, and to assess whether a certain transaction may still be suspicious without meeting any of the indicators.

In evaluating a suspicious transaction, the authorized person and his deputy are obliged to provide all professional assistance to employees.

Obliged entities/organizers of special games of chance in gaming venues, i.e. games of chance through means of electronic communication should especially monitor and recognize suspicious transactions that are performed in a way that avoids standard and usual control methods that include multiple participants, i.e. multiple interconnected transactions which are carried out in a shorter period of time or in several consecutive intervals, in an amount that is slightly below the legally prescribed maximum, in order to avoid recording and reporting.

The list of indicators for recognizing suspicious transactions is a starting point for employees/authorized persons in recognizing suspicious circumstances related to a certain customer and/or a transaction performed by the customer, in order to use them in their operations. In the process of determining the existence of elements for the qualification of a certain transaction or person as suspicious, one should first of all keep in mind the indicators for conveying the grounds of suspicion. However, a transaction may be suspicious without meeting any of the indicators. In this sense, it is necessary to look at a broader framework, in accordance with the principle that the obliged entities know their clients best, and to assess whether a certain transaction may still be suspicious without meeting any of the indicators.

The basic task of the obliged entity is to ensure that all the necessary data related to the knowledge and monitoring of their customers are obtained, to assess whether certain models of behavior can be linked to a criminal offense and to what extent, and to take all the necessary measures in accordance with the Law and reports of suspicious activity.

RISK ANALYSIS

➢

In order to prevent exposure to the negative consequences of money laundering and financing of terrorism, pursuant to Article 6 of the Law, the obliged entity is obliged to prepare and regularly update the analysis of the risk of money laundering and financing of terrorism, in accordance with the Law, by-laws, guidelines issued by the authority responsible for supervising the application of the Law and assessing the risk of money laundering and financing of terrorism, prepared at the national level (hereinafter: risk analysis).

According to the above, when making a risk analysis at the level of the obliged entities, i.e. in relation to their entire business, as well as the analysis at the level of the customer, i.e. the business relationship, the obliged entities are obliged to take into account the degree of threat and the sectoral vulnerability of the sector to which they belong according to the results of the national risk assessment.

The risk analysis must be proportionate to the nature and scope of the business, as well as the size of the obliged entity and must take into account the basic types of risk, such as: geographic risk, customer risk, service risk and transaction risk, as well as other sources of risk identified by the obliged entities due to the specifics of their business.

Risk analysis includes:

- risk analysis in relation to the obliged entity's entire business
- risk analysis for each group or type of customer, i.e. business relationship, service it provides within its activity, as well as transactions.

In the process of creating a risk analysis in relation to its entire business, the obliged entity assesses the probability that its business will be used for that purpose. The risk analysis in relation to the obliged entity’s entire business is aimed at identifying the obliged entity's exposure to the risk of money laundering and financing terrorism and the types of business of the obliged entity that should be prioritized in undertaking activities for effective risk management.

Based on the estimated probability of the occurrence of the risk and the estimated negative consequences, the obliged entity determines the level of exposure to the risk of money laundering and financing of terrorism for each segment of the business.

The risk analysis for each customer or type of customer, business relationship, transaction, service that the obliged entity provides as part of its activity and the way of establishing a business relationship with the customer (e.g. without the physical presence of the customer) is intended to determine the criteria based on which the obliged entity will classify a certain customer, business relationship, service or transaction into one of the risk categories in accordance with the Law. The classification of customers into one of the risk categories is performed both by analyzing certain types of risk and by their combination, depending on the specifics of each obliged entity. The risk category of the customer, business relationship, service or transaction also depends on which activities and measures of knowing and monitoring the customer the obliged entity will undertake in accordance with the Law (from simplified to increased).

Based on risk analysis, the obliged entity classifies the customer in one of the following risk categories:

1) low risk of money laundering and financing of terrorism and applies the minimum, simplified measures;
2) medium risk of money laundering and the financing of terrorism and applies the minimum general actions and measures;
3) high risk of money laundering and financing of terrorism and applies increased actions and measures.

In addition to the above, the obliged entity can, by internal acts, foresee additional risk categories and determine adequate actions and measures from the law for those risk categories.

An effective and high-quality development process, as well as an updated risk assessment, first of all implies the determination of parts of the system that may have information of essential importance in the obliged entity and that can recognize certain vulnerabilities of the system and contribute to the reduction of threats.

Also, it is necessary for the obliged entity to pay due attention to information from external sources, such as: the results of the national assessment of the risk of money laundering and financing of terrorism, changes in the law, feedback information which obliged entities receive about reported suspicious transactions, models of behavior recognized in indictments for money laundering, typologies, international research, FATF, etc.

The obliged entity's employees must have a clear picture of how and in what manner the obliged entity assessed certain risks at the institution level, how the results of the national risk assessment were implemented in the process, as well as an overview of the clear measures that the obliged entity intends to implement based on the obtained results.

Risk assessment is an activity that shows the extent to which a certain risk can affect the achievement of a goal, and it is performed on the basis of probability and impact.

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

Obliged entities assess exposure to the risk of money laundering and financing of terrorism, i.e. the probability of a negative impact arising from the risk, as well as the impact of the risk on business goals.

Risk exposure is calculated based on a matrix that shows the relationship between impact and probability. The main goal of using the risk matrix is the application of the principle based on risk assessment in the ranking of obliged entities according to their exposure to the risk of money laundering and financing of terrorism. Based on the data and information from the risk analysis, they are entered into the matrix, based on which the degree of risk to which the obliged entity is exposed is calculated.

Example of a 3 x 3 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 analysis of the risk of money laundering and financing of terrorism is based on the assumption that the different products and services that obliged entities offer as part of their business, or the different transactions they perform, are not equally vulnerable to abuse of money laundering or financing of terrorism. A risk analysis is performed to enable the implementation of control measures that are proportionate to the identified risk. This enables the obliged entity to focus on those clients, countries, products, services and transactions that represent potentially the greatest risk. The risks faced by the obliged entity must be analyzed from the point of view of determining the probability that a certain occurence will happen and assessing the negative impact that could arise in that case.

The matrix is a tool in the application of an approach based on risk assessment of the obliged entity's business, and the obliged entity should take into account other information and data in the process of assessing the risk of its business (e.g. measures adopted by the supervisory authority, auditor's report, etc.)

In order to determine the obliged entity's exposure to the risk of money laundering and financing of terrorism, the obliged entity must know each business segment in the domain where the threat of money laundering or financing of terrorism may appear, that is, it must assess the vulnerability in relation to the threat. It is necessary that risks are identified at all levels of management, from the operational level to the top management, and that all employees of the obliged entity are involved in that process.

RISK MANAGEMENT

➢

Risk management implies the purposeful use of the results obtained by risk analysis. Risk management, as well as monitoring and reporting on them, is a continuous process.

The effectiveness of the risk management of money laundering and financing of terrorism by obliged entities is assessed on the basis of the established quality of the control system and risk management system and is observed through the following levels of the obliged entity's activities: corporate management, risk management, internal regulation, internal control, compliance, reporting and training.

The obliged entity’s managers of all levels, through risk analysis processes, monitor whether certain risks still exist, whether new ones have appeared, whether the impact and probability of existing risks have changed, and whether the priority of risks has changed.

Identified risks with the obliged entities are discussed regularly, at top management meetings twice a year and as needed, and then communication takes place with lower managers, so that the response to the risks is effective.

Risks at the level of organizational units are monitored permanently, and reviewed quarterly and as needed, by managers of organizational units.

Based on the obtained results, action priorities are determined, i.e. methods that the obliged entity will apply (e.g. whether the use of certain products or services will be prohibited, whether greater attention will be paid to certain transactions, whether the level of education of the obliged entity must be enhanced, etc.).

It is necessary to respond to high risks without delay, to medium risks as soon as possible, and to monitor lower risks.

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

- obliged entity's business function for business control, in order to ensure that all foreseen procedures are regularly applied;
- compliance with regulations function, which periodically monitors whether established internal policies are followed and whether all systems are in operation;
- audit functions, determining whether business policies and processes are in accordance with the law and whether they are implemented in the manner prescribed by law;
- assessments of resources for risk management, such as provided financial resources and personnel solutions;
- determination of future needs that are important for the nature, size and complexity of the obliged entity's entire business.

Regular reports and all other important information must be submitted to the managers of the obliged entity so they can check the level of control over the prevention of money laundering and financing of terrorism, as well as the possible consequences for the business of the obliged entity if the control and prevention mechanisms do not function adequately for the assessed risks.

Management directs business policy by formulating goals and making decisions about strategic choices, and when developing final plans and business policy, it must take into account the risks of money laundering and financing of terrorism.

The established internal policy and procedures are approved by the management and they are valid for all obliged entity's employees. Through risk assessment and appropriate policies and procedures, the obliged entity ensures the continuity of risk management despite any changes that may occur in the structure of management and employees, that is, in the structure of the obliged entity.

Also, management is obliged to encourage ethical business culture and ethical behavior of employees. Ethical behavior represents the professional and individual responsibility of employees for the decisions they make and the steps they take when performing their activities.

For the decision-making and planning process, documentation and the manner in which the risks will be presented are of great importance. Indeed, when certain risks are determined, it is necessary to document the specified results, that is, to transfer them to a written document, which, in addition to the definition of basic terms and work methodology, also will contain the result of the risk assessment. It is necessary to describe the results and the manner of how certain results were obtained, as well as in what way the determined risks of the country reflect on the obliged entity himself.

In order to implement activities to establish the functioning and maintenance of the risk management process, the obliged entity adopts a *strategy* that represents a framework for

identifying, evaluating and controlling potential events and situations that may have a negative effect on the obliged entity's reputation and its business. It should contain the positions of the obliged entity towards the risks, the set goals, the roles of authority and the responsibilities in the risk management process, the indicators of effectiveness, and it should also be periodically updated or revised.

The purpose of the strategy is to increase the capacity of obliged entities to achieve set goals at the strategic and operational level, using the risk management system.

Adopted business policies and procedures allow the obliged entity to effectively manage risks, that is, to focus its efforts on those areas of business that are most susceptible to various types of abuse in terms of preventing money laundering and financing of terrorism. The higher the risk, the more control measures need to be applied, and in this sense, it is necessary to introduce policies and procedures for actions and measures at the level of the entire obliged entitiy in order to prevent and detect money laundering and financing of terrorism.

Actions and measures to prevent money laundering and financing of terrorism

When performing their registered activity, obliged entities must act in accordance with the obligations prescribed by the Law in the field of detection and prevention of money laundering and financing of terrorism and are obliged to ensure compliance with the prescribed measures and activities of obliged entity at all levels, so that the obliged entity's entire business is conducted in accordance with the Law.

Actions and measures for the prevention and detection of money laundering and financing of terrorism are undertaken before, during and after the transaction or the establishment of a business relationship and include the following:

1) knowing the customer and monitoring his business (hereinafter: knowing and monitoring the customer);

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

3) designation of the person in charge of carrying out the obligations from this law (hereinafter: authorized person) and his deputy, as well as providing the conditions for their work;

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

5) provision of regular internal control of the fulfillment of obligations from this law, as well as internal audit if it is in accordance with the scope and nature of the obliged entity's business;

6) creating a list of indicators for identifying persons and transactions for which there are grounds for suspicion of money laundering or financing of terrorism;

7) record keeping, protection and storage of data from those records;

8) implementation of the measures from this law in business units and subordinate companies of legal entities that are majority-owned by the obliged entity in the country and abroad;

9) execution of other actions and measures based on the law.

The obliged entity is also obliged to elaborate appropriate *internal acts*, which, for the purpose of effective management of the risk of money laundering and financing of terrorism, will include the actions and measures defined by the Law. The internal acts must be proportionate to

the nature and size of the obliged entity and must be approved by the top management, according to the article 5 of the Law.

Every obliged entity is also obliged to prepare a money laundering and financing of terrorism *risk analysis* (Article 6 of the Law).

I Knowing and monitoring the customer

Actions and measures of knowing and monitoring the customer are a key preventive element within the process of detecting and preventing money laundering and financing of terrorism. The purpose of conducting actions and measures of knowing and monitoring the customer is, first of all, to establish and confirm the real identity of the customer and the origin of the property in a credible manner, as well as to regularly monitor the compliance of the customer's activities with the usual scope and type of his business.

If the implementation of actions and measures of knowing and monitoring the customer would cause the customer to suspect that the obliged entity is carrying out the same for the purpose of providing data to the Administration for the Prevention of Money Laundering, the obliged entity shall stop taking the said actions and measures and make an official note in written form that will be submitted to the aforementioned Administration.

International standards and the Law define that the obliged entity, depending on the degree of risk of money laundering and financing of terrorism, implements three types of actions and measures related to knowing and monitoring the customer: *general, simplified and increased*.

General actions and measures of knowing and monitoring the customer

General actions and measures of knowing and monitoring the customer, in accordance with Article 7 of the Law, include the following activities: determining and verifying the identity of the customer, obtaining and evaluating information about the purpose and intention of the business relationship or transaction, obtaining and evaluating the credibility of information about the origin of property that is or will be the subject of a business relationship or transaction, business monitoring and verifying compliance of the customer's activities with the nature of the business relationship and the usual scope and type of business.

Actions and measures from Article 7 of the Law are performed by the obliged entity when withdrawing winnings, making deposits or in both cases, when transactions in the amount of 2,000 euros or more in dinar equivalent are carried out, regardless of whether it is one or more mutually related transactions (Article 8, paragraph 3 of the Law). Pursuant to Article 10 of the Law, the obliged entity is obliged to perform the mentioned actions and measures before executing the transaction.

The obliged entity is also obliged to apply actions and measures of knowing and monitoring the customer with frequency and intensity in accordance with the assessed risk and changed circumstances related to the customer.

Establishing and verifying the identity of the customer

Obligors are obliged to determine and confirm the identity of the customer before establishing a business relationship.

The obliged entity establishes and verifies the identity of the customer based on documents, data or information obtained from reliable and trustworthy sources or through means of electronic communication in accordance with the Law, by inspecting the corresponding identification document which is an official personal document.

If, during the establishment and verification of the customer's identity, the obliged entity doubts the veracity of the collected data or the credibility of the documents from which the data were obtained, it is obliged to obtain from the customer a written statement on the veracity and credibility of the data and documents.

When identifying a natural person, the obliged entity is obliged to obtain a copy, i.e. a read-out extract of that person's personal document. A digitized document that must contain a qualified electronic seal, i.e. a qualified electronic signature, with an associated time stamp is considered a read-out extract. The date, time and name of the person who inspected the document shall be written on the copy, i.e. the read-out extract of the personal document in paper form. The obliged entity shall keep a copy, i.e. a read-out extract of the personal document, in paper or electronic form in accordance with the law. The electronic form must contain a qualified electronic seal, that is, a qualified electronic signature with an associated time stamp.

Also, the obliged entity can establish and verify the identity of the customer who is a natural person based on the qualified electronic certificate of the customer, under the conditions and in the manner prescribed by Article 18 of the Law.

Special case of establishing and verifying the customer's identity when entering the gaming venue

Article 24 of the Law foresees a special case of establishing and verifying the identity of the customer when the customer enters the gaming venue, in such a way that the obliged entity/organizer of special games of chance in the gaming venue is obliged to establish and verify the identity of the customer and to obtain from him the data referred to in Article 99, paragraph 1, items 4) and 6) of the Law, such as his first and last name, date and place of birth, place of residence or living, as well as the date and time of entry into the gaming venue. The obliged entity is also obliged to obtain a written statement from the customer in the gaming venue declaring under material and criminal responsibility that he participates in the games of chance for his own account and in his own name.

Establishing and verifying identity without the physical presence of the customer/games of chance through means of electronic communication

Article 39 of the Law stipulates that if the customer is not physically present at the obliged entity during the establishment and verification of his identity, the obliged entity is obliged to take some additional measures, in addition to the general actions and measures from Article 7, paragraph 1 of the Law, such as: obtaining additional documents, data or information, on the basis of which it checks the identity of the customer; additional verification of submitted documents or additional confirmation of customer data, and other measures determined by the supervisory authority.

In the case of organizers of games of chance through means of electronic communication, the fact that the players are not physically present makes it difficult to verify the customer's identity.

In this regard, obliged entities can identify customers by asking for personal information, including name, home address and date of birth. All this information must be verified. It is also useful to obtain information on "sources of funds" and level of legitimate income (e.g. occupation). This information can help obliged entities make their assessments of whether a customer's level of gambling is within his approximate income or is questionable. Proof of identity can be verified using documents obtained from the customer (e.g. passport, driver's license, bank statement, utility bills, etc.), through electronic evidence.

Businesses that involve the absence of "face-to-face" contact may carry certain risks and require alternative or additional methods of compliance, in order to compensate for the fact that obliged entities are not able to verify the physical appearance of the client based on photographic identification documents.

Public sources of data can be particularly valuable for identifying politically exposed persons and individuals who are subject to various sanctions as a result of activities with organized crime and/or terrorist financing. The obliged entity should use all available data search options (e.g. various publicly available registers, subscription to organizations that enable the search of various business activities, legal sources and media, Internet search engines) in order to check the statements of the customers from the questionnaire with submitted personal data and thus achieve a satisfactory level of reliability, credibility, authenticity and acceptability thereof.

Some of the commercial agencies that access many sources of data that are available on the Internet browser can provide obliged entities with complex and comprehensive electronic verifications. Given that agencies use different databases, they can access high-risk alerts that use specific data sources to identify high risk. Negative information includes reviewing the lists of persons known to be involved in fraud, including identity fraud and registered person fraud. On the other hand, positive information related to full name, current address, date of birth, can prove that an individual exists, and some may offer a higher degree of trust than others. Verification of such information may be appropriate in the case of other factors that present an increased risk of fraud for misrepresentation. When electronic identification systems are used, the obliged entity must believe that the data provider is sufficiently reliable and accurate. The obliged entity must also ensure that the electronic verification process meets the standard level, i.e. the confirmation prescribed by law and that the supervisory authority can rely on them (example of verification: one match on the full name and current address, and another match on the customer's full name and current address and date of birth).

In the mentioned cases, when there is no "face-to-face" contact, i.e. when the customer is not physically present during the establishment and verification of identity, the obliged entity applies increased actions and measures of knowing and monitoring the customer.

According to all of the above, the main task of the *obliged entity/organizer of special games of chance in gaming venues and games of chance through means of electronic communication* is to ensure the availability of the necessary data related to the knowledge and monitoring of the customers, to assess whether certain models of behavior can be linked with the criminal offense and to what extent, and to take all necessary measures and report suspicious activities to the Administration for the Prevention of Money Laundering in accordance with the Law.

In the event that the identity of the customer cannot be established or verified or when the obliged entity has reasonable doubts about the veracity or reliability of the data or the documentation confirming the customer’s identity, and in situations where the customer is not ready or does not show willingness to cooperate with the obliged entity in determining the veracity and completeness of the data required by the obliged entity as part of the analysis, the obliged entity is obliged to refuse the establishment of a business relationship, as well as the execution of the transaction and is obliged to terminate existing relations with the customer (Article 7 of the Law).

Furthermore, in case that during the implementation of the actions and measures from Article 7 of the Law, the customer suspects that the obliged entity is carrying out the same in order to provide data to the Administration for the Prevention of Money Laundering, the obliged

entity is obliged to make an official note in a written form that shall be submitted to the said Administration.

Simplified actions and measures of knowing and monitoring the customer

Simplified actions and measures of knowing and monitoring the customer are undertaken in cases and in the manner prescribed by the Law and by-laws and are applied to customers with a low degree of risk of money laundering and financing of terrorism.

Pursuant to Article 42, paragraph 2 of the Law, the obliged entities can perform simplified actions and measures of knowing and monitoring the customer also in cases where, in accordance with the provisions of Article 6 of the Law, they assess that due to the nature of the business relationship, the form and manner of performing the transaction, the business profile customer, or other circumstances related to the customer, there is an insignificant or low level of risk for money laundering or financing of terrorism.

When performing simplified actions and measures of knowing and monitoring the customer, the obliged entities are obliged to establish an adequate level of monitoring of the customer's business so that they are able to detect unusual and suspicious transactions.

Increased actions and measures of knowing and monitoring the customer

In the event that a specific customer, service or transaction is categorized as high-risk of money laundering or financing of terrorism, obliged entities are obliged to apply, in addition to the general ones, additional, increased actions and measures of knowing and monitoring the customer.

Article 35 of the Law stipulates that increased actions and measures of knowing and monitoring of the obliged entity´s customer include additional measures that the obliged entity performs, such as: *when applying new technological achievements and new services; when establishing a business relationship or making a transaction in the amount of 15,000 Euros or more with a customer who is an official; when the customer is not physically present during the establishment and verification of identity; when establishing a business relationship or carrying out transactions with a customer from a country that has strategic deficiencies in the system of preventing money laundering and financing terrorism.*

In addition to the above, the obliged entities are obliged to carry out increased actions and measures of knowing and monitoring the customer in cases where they assess that due to the nature of the business relationship, the form and manner of performing 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 from money laundering or financing terrorism.

The obliged entities are obliged to define in their internal acts which increased actions and measures, and to what extent, they will apply in each specific case.

New technological achievements and new services

Pursuant to Article 37 of the Law, the obliged entities are obliged to assess the risk of money laundering and financing of terrorism considering the new service they provide within their business activity, new business practice, as well as the ways of providing the new service, before its implementation. Also, they are obliged to assess the risk of using modern technologies in the provision of existing or a new services, to take additional measures to reduce risks and to manage them.

Official

The obliged entities proceed with the procedure to determine whether the customer is an official, a member of the official's immediate family or a close associate of the official. The obliged entities are obliged to define the procedure of determination whether the customer is an official in their internal acts.

If the customer is an official, a member of the immediate family of an official or a close associate of an official, apart from the general actions and measures from Article 7, paragraph 1 of the Law, the obliged entities are obliged, pursuant to Article 38 of the Law, to obtain data on the origin of the property that is the subject of the transaction, from documents and other documentation submitted by the customer. If it is not possible to obtain such data in the described manner, the obliged entities shall take a written statement about their origin directly from the customer and obtain information about the entire property owned by the official, from publicly available and other sources, as well as directly from the customer. Also, the obliged entities are obliged to ensure that the employee who conducts the procedure of establishing a business relationship with the oficial, before establishing that relationship, obtains the written consent of the member of the top management from Article 52, paragraph 3 of the Law and to monitor with due care the transactions and other business activities of the official during the business relationship.

If the obliged entities determine that the customer has become an official in the course of a business relationship, they shall be obliged to obtain the written consent of a member of the top management from Article 52, paragraph 3 of the Law, for the continuation of the business relationship with that person.

Information about whether a certain person is an official or not, the obliged entity is obliged to obtain from a specially signed statement, which must be written in Serbian and English for an official of another state and an official of an international organization.

The written statement shall contain at least the following information:

1) first and last name, permanent residence, date and place of birth, number, type and name of the issuer of a valid personal document;
2) statement as to whether a customer is, according to the criteria from the Law, an official - a politically exposed person or not;
3) data on what type of politically exposed person he/she is (whether it is a person who acts or has acted in a prominent public position in the last four years, or a family member of a politically exposed person or a close associate);
4) data on the time of performance of such function, if the customer is a person who acts or has acted in the previous four years in a prominent public position;
5) data on the type of public function performed by the person;
6) data on the family relationship, if the customer is a family member of a politically exposed person;
7) data on the form and manner of business cooperation, if the customer is a close associate of the person;
8) signature of the customer.

The obliged entity can also obtain information about the official by looking at public and other data available to him/her, such as: the register of officials of the Anti-Corruption Agency,

electronic commercial databases (e.g. World-Check, Factiva, LexisNexis), his/her internal database if any, etc.

If the customer is a member of the immediate family of the official or a close associate of the official, the obliged entity shall also apply increased actions and measures of knowing and monitoring to such customer.

The obliged entity shall also apply these actions and measures when a natural person ceased to perform a public function (former official) and for as long as it takes to conclude that that person did not abuse the position he/she had, i.e. four years from the day he/she ceased to perform such function.

Countries that do not apply standards in the area of prevention of money laundering and financing of terrorism

When establishing a business relationship or performing a transaction when a business relationship has not been established, the obliged entity is obliged to apply the increased actions and measures prescribed in Article 41, paragraph 2 of the Law, with a customer from a country that has strategic deficiencies in the system for combating money laundering and financing of terrorism.

The Law defines that strategic deficiencies in the system for combating money laundering and financing of terrorism refer in particular to:

- the legal and institutional framework of the state, especially on the incrimination of criminal offenses of money laundering and financing of terrorism, measures of knowing and monitoring the customer, provisions regarding data storage, provisions regarding the reporting of suspicious transactions, the availability of accurate and reliable information about the real owners of legal entities and persons under foreign law;
- authorizations and procedures of competent authorities of those countries in relation to money laundering and financing of terrorism;
- the effectiveness of the system for combating money laundering and financing of terrorism in eliminating the risk of money laundering and financing of terrorism.

In the above mentioned cases, the obliged entities are obliged to implement increased actions and measures of knowing and monitoring the customer, when, in accordance with the risk analysis, they assess that due to the form and manner of carrying out 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 financing of terrorism, and then they shall be obliged to collect data on the origin of the property that is the subject of a business relationship or transaction, to collect additional information on the purpose and intention of the business relationship or transaction, to additionally check submitted documents, to obtain the approval of a member of the top management from Article 52, paragraph 3 of the Law, as well as to take other adequate measures to eliminate risks. The obliged entities are obliged to define in their internal acts which increased actions and measures, and to what extent, they will apply in each specific case.

On the proposal of the Administration for the Prevention of Money Laundering, the Minister elaborates a list of countries that have 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 financing of terrorism by international institutions.

II Delivery of data to the Administration for the Prevention of Money Laundering

The obliged entity is obliged to submit data to the Administration for the Prevention of Money Laundering whenever there are grounds for suspicion regarding a transaction or a customer that it is money laundering or financing of terrorism, in the manner, form and within the deadlines foreseen by the Law and the rulebook by which the Administration for the Prevention of Money Laundering brings closer the methodology for the completion of operations in accordance with the Law.

The obliged entity is obliged to also submit to the Administration for the Prevention of Money Laundering the data on each cash transaction in the amount of 15,000 Euros or more in dinar equivalent immediately when it is performed, and no later than within 3 days from the date of the transaction, stating the first and last name, date and place of birth, place of permanent or current residence, and Unique Personal Identification Number of a natural person, type and number of personal document, name of the issuer, date and place of issuance, and in accordance with Article 99, paragraph 1, item 3) of the Law, and Article 99, paragraph 1, items 7)-10) of the Law, which refer to the date and time of the transaction; the amount of the transaction and the currency in which the transaction was made; the purpose of the transaction, as well as the first and last name and place of residence, that is, the business name and seat of the person to whom the transaction is intended, and the way the transaction is carried out.

The obliged entity is obliged to submit the data from Article 99, paragraph 1 of the Law to the Administration for the Prevention of Money Laundering, also when there are grounds for suspecting money laundering or financing of terrorism in relation to a transaction or a customer, in the manner and within the time limits provided for in Article 47 of the Law.

The obliged entity's employee who determines that there are reasons to suspect money laundering or financing of terrorism must immediately notify the authorized person or his deputy. The obliged entity must organize the procedure for reporting suspicious transactions between all organizational units and authorized persons, and on that occasion define, first of all:

- manner of reporting data;
- type of data to be submitted (data about the customer, reasons for suspecting money laundering, etc.);
- way of cooperation of organizational units with an authorized person;
- determine the actions to be taken with the customer in case of temporary suspension of the execution of the transaction by the Administration for the Prevention of Money Laundering;
- determine the role of the obliged entity's authorized person when reporting a suspicious transaction;
- prohibit disclosure of data, information or documentation that will be submitted to the Administration for the Prevention of Money Laundering;
- determine measures regarding the continuation of business with the customer (termination of the business relationship, application of increased actions and measures of knowing and monitoring the customer, monitoring of the customer's future activities).

III Authorized person and the provision of conditions for his work

Risk management process involves multiple participants and structures which have their own roles, powers and responsibilities. The obliged entity is obliged to appoint an authorized person and his deputy in accordance with Articles 49-52 of the Law.

The authorized person and his deputy must meet the conditions prescribed by Article 50, paragraphs 1 and 2 of the Law as follows:

1) employed at the obliged entity in a workplace with powers that enable him to effectively, quickly and efficiently perform the tasks prescribed by this law;
2) has not been legally convicted or criminal proceedings are not conducted against him ex officio for criminal acts that would make him unfit to perform the duties of an authorized person;
3) professionally qualified for the prevention and detection of money laundering and financing of terrorism;
4) knows the nature of the obliged entity's business in areas that are subject to the risk of money laundering or financing of terrorism;
5) owns a license to perform the duties of an authorized person, if the obliged entity is obliged to ensure that its authorized person has this license, in accordance with the Rulebook on professional exam for the issuance of a license to perform the duties of an authorized person, which is in force from January 1, 2021.

The aforementioned Rulebook prescribes the content and method of taking the professional exam, as well as the criteria based on which it is determined whether the obliged entity is obliged to ensure that its authorized person and deputy have a license to perform the duties of an authorized person.

Pursuant to the provisions of the above mentioned Rulebook, the criteria to determine whether the obliged entity is obliged to ensure that its authorized person has a license to perform the duties of an authorized person are:

1) if the authorized person does not possess an international certificate/license in the field of prevention of money laundering and financing of terrorism issued by the relevant international organization/body;
2) if the authorized person does not have a certificate of passing a professional exam for the performance of tasks in his field of activity, for the issuance of which knowledge in the field of preventing money laundering and financing оф terrorism is also checked;
3) if the authorized person is not employed by the obliged entity who has less than seven employees.

The authorized person's deputy must fulfill the same conditions as the authorized person.

The Administration for the Prevention of Money Laundering issues licenses to an authorized person and an authorized person's deputy, based on the results of professional exams, which are valid for 5 years.

The authorized person takes care of the implementation, operation and development of the system for preventing money laundering and financing of terrorism and initiates and proposes measures for its improvement; participates in the elaboration of internal acts; participates in the development of internal control guidelines; participates in the establishment and development of IT support; participates in the preparation of programs for professional education, training, and

development of employees and ensures proper and timely delivery of data to the Administration for the Prevention of Money Laundering in accordance with the law.

The authorized person's deputy replaces the authorized person in his absence and performs other tasks in accordance with the obliged entity's internal act.

The obliged entity's top management implements a system for preventing and detecting money laundering and financing of terrorism, i.e. internal policies and procedures, adopts an internal strategy, establishes, maintains and provides conditions for the implementation of activities in the process of risk management and provides the highest level of support, dedication and commitment to the management process risks. The obliged entity is obliged to prescribe the manner of cooperation between the authorized person and other organizational units.

The obliged entity is obliged to provide the authorized person with: unrestricted access to data, information and documentation necessary for the performance of his duties; appropriate personnel, material, informational and technical conditions, and other for work; appropriate space and technical possibilities that ensure the appropriate degree of protection of confidential data at the disposal of the authorized person; constant professional training; replacement during his absence; protection in terms of disclosure of his data to unauthorized persons, as well as protection from other procedures that may affect the unobstructed performance of his duties.

Effective communication is carried out vertically and horizontally within the obliged entity. All employees receive clear messages from managers about responsibility for risk management and how their individual activities are related to the work of other organizational units and employees.

Managers of organizational units ensure that communication effectively conveys the goals, importance and significance of effective risk management, susceptibility to risk and risk tolerance, as well as the roles and responsibilities of employees in the implementation of risk management components.

Management must ensure that employees follow internal procedures and established policies. It should encourage ethical business culture and ethical behavior of employees, continuously strengthen employees' capacities, knowledge and awareness of the importance of reviewing and updating risk assessment and the importance of effective risk management.

The obliged entity shall submit to the Administration for the Prevention of Money Laundering data on the personal name and job title of *the authorized person and his deputy*, as well as data on the personal name and job title of *the member of the top management* responsible for the implementation of the Law, and any changes to that data no later than within 15 days from the day of appointment.

IV Education, training and development

The obliged entity is obliged to provide regular professional education, training and development of employees who perform tasks of preventing and detecting money laundering and financing of terrorism.

The same applies to getting informed about:

- provisions of *the Law on the Prevention of Money Laundering and Financing of Terrorism*, regulations adopted based on it and internal acts;
- *list of indicators* for identifying customers and transactions for which there are grounds for suspicion of money laundering and financing of terrorism;
- provisions of the regulations aimed at *limiting the disposal of property in order to prevent terrorism and the proliferation of weapons of mass destruction* and
- regulations governing the *protection of personal data.*

The obliged entity is obliged to prepare a program of regular annual professional education, training and development of employees for the prevention of money laundering and financing of terrorism no later than the end of March for the current year, which shall contain at least:

1) planned number of trainings on an annual level;
2) planned number of employees who will attend the trainings, as well as the profile of the employees for whom the trainings are intended;
3) topics from the field of preventing money laundering and financing of terrorism that will be the subject of trainings, as well as topics from the field of limiting the disposal of property in order to prevent terrorism and the proliferation of weapons of mass destruction;
4) method of training implementation (seminars, workshops, etc.).

In accordance with Article 53, paragraph 1 of the Law, the obliged entity is obliged to conduct the training prescribed by the program on the annual professional education, training and development of employees in the year for which the program on annual professional education, training and development of employees was adopted, and no later than the end of March of the following year, and to make an official note on such trainings.

The official note must at least contain the time and place of the training, the number of participants who attended the training, the first and last name of the person who conducted the training and a brief description of the topic covered at the training.

V Internal control, internal audit and integrity of employees

Within the framework of the activities undertaken for the effective management of the risk of money laundering and financing of terrorism, the obliged entity is obliged to perform regular internal control in the prevention and detection of money laundering and financing of terrorism, pursuant to Article 54 of the Law. Internal control is performed in accordance with the established risk of money laundering and financing of terrorism.

The purpose of internal control is the prevention, detection and elimination of deficiencies in the application of the Law, as well as the improvement of internal systems for detecting persons and transactions suspected of money laundering or financing of terrorism.

When performing internal control, the obliged entity is obliged to check and test the implementation of the system against money laundering and financing of terrorism and adopted procedures, by using the method of random sampling or in another appropriate way,

In the event of a change in the business process (e.g. organizational changes, changes in business procedures, introduction of a new service), the obliged entity is obliged to check and harmonize its procedures within the framework of internal control, so that they are adequate for the fulfillment of obligations under the Law.

The obliged entity is obliged to check the compliance of the system and procedures for the implementation of the Law and internal procedures once a year, as well as every time there are changes, no later than by the date of implementation of those changes.

The obliged entity assigns by its act the powers and responsibilities of the management body, organizational units, authorized persons and other subjects to the obliged entity in the exercise of internal control, as well as the manner and schedule of the exercise of internal control.

The obliged entity is obliged to prepare an annual report on the performed internal control and the measures taken after that control, no later than March 15 of the current year for the previous year.

The annual report must contain the following information:

1) the total number of reported cash transactions in the amount of 15,000 Euros or more in dinar equivalent;
2) the total number of reported persons or transactions suspected of being related to money laundering and financing of terrorism;
3) the total number of persons or transactions suspected of being related to money laundering and financing of terrorism, which were reported to an authorized person by employees of the obliged entity and were not reported to the Administration for the Prevention of Money Laundering;
4) the total number of established business relationships where the customer's identity was determined on the basis of the customer's qualified electronic certificate;
5) the frequency of using individual indicators for identifying suspicious transactions when reporting transactions to an authorized person by the obliged entity's employees;
6) total number of performed internal controls, as well as internal control findings (number of observed and corrected errors, description of observed errors, etc.);
7) measures taken on the basis of internal controls;
8) on the performed internal control of information technology used in the implementation of the provisions of the Law (ensuring the protection of data transmitted electronically, saving data on customers and transactions in a centralized database);
9) on the content of the training program on detection and prevention of money laundering and financing of terrorism, the place and person who conducted the training program, the number of employees who attended the training, as well as the assessment of the need for further training and improvement of employees;
10) on the measures taken to protect data that are an official secret;

The obliged entity is obliged to submit the relevant report to the Administration for the Prevention of Money Laundering and the supervisory authority for the implementation of the Law, at their request, within three days from the date of submission of such request.

The obliged entity is also obliged to organize an independent *internal audit*, the scope of which is the regular assessment of the adequacy, reliability and efficiency of the money laundering and terrorist financing risk management system when the law governing the activity of the obliged entity stipulates the obligation to have an independent internal audit, or when the obliged entity assesses that, taking into account the size and nature of the work, it is necessary to have an independent internal audit in terms of the Law.

The obliged entity is also obliged to *determine the procedure by which, when establishing an employment relationship* at a workplace where the provisions of the Law on the Prevention of Money Laundering and the regulations adopted on its basis are applied, the candidate for that workplace shall be checked whether he has been convicted of criminal offenses for obtaining illegal financial gain or crimes related to terrorism. In the aforementioned procedure, other criteria are also checked in order to determine if the candidate for that position meets high professional and moral qualities.

VI Creating a list of indicators

The obliged entity is obliged to create a list of indicators for identifying persons and transactions for which there are grounds for suspicion of money laundering or financing of terrorism. When creating the list of indicators, they are obliged to enter the indicators created by the competent authority, which are published on the website of the Administration for the Prevention of Money Laundering.

When creating the list of indicators, among other things, the obliged entity takes into account the complexity and scope of the transaction, the unusual way 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.

When establishing grounds for suspicion of money laundering or financing of terrorism, the obliged entity is obliged to apply a list of indicators, and to take into account other circumstances that indicate the existence of grounds for suspicion of money laundering or financing of terrorism. It is especially important that all employees are familiar with the indicators and trained to recognize and resolve the risk of money laundering and financing of terrorism within the scope of their work.

VII Data protection and storage, record keeping

The obliged entity is obliged to keep data and documentation related to the customer, the established business relationship with the customer, the performed risk analysis and the completed transaction, obtained in the manner prescribed by law, for at least ten years from the date of termination of the business relationship, completed transaction, i.e. from the last entry into the gaming venue, and in accordance with Article 95, paragraph 1 of the Law.

Furthermore, in accordance with Article 95, paragraph 3 of the Law, the obliged entity is obliged to keep data and documentation about the authorized person, the authorized person's deputy, the professional training of employees and the internal controls performed for at least five years from the date of termination of the duties of the authorized person, the performed professional training or the performed internal controls.

After the expiration of the mentioned deadlines, the obliged entity is obliged to act with the above mentioned data in accordance with the law that requires the protection of personal data, provided that it is not the data used by competent authorities for special purposes.

The obliged entities, i.e. their employees, including members of the administrative, supervisory and other management bodies, as well as other persons who have access to data from Article 99 of the Law, are obliged to protect them, in accordance with Articles 90 and 91 of the Law.

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

Article 48, paragraph 1 of the Law stipulates that the obliged entities are obliged to ensure that the actions and measures for the prevention and detection of money laundering and financing of terrorism, equal to those prescribed by this law, are performed in the same scope in their business units and subordinate companies of the legal entity in their majority ownership, regardless of whether their place of business is in the Republic of Serbia or in foreign countries.

Paragraph 14 of Article 48 stipulates that the provisions of the above mentioned Article 48 of the Law shall be applied accordingly to the obliged entity who is a member of a non-financial group in terms of the law governing the activity of that obliged entity.

IX Execution of other actions and measures

Data protection

The obliged entities, i.e. their employees, including members of the administrative, supervisory and other management bodies, as well as other persons who have access to data from Article 99 of the Law, may not disclose to a customer or a third party the data defined in Article 90, paragraph 1, items 1) - 4) of the Law. Paragraph 2 of Article 90 of the Law also prescribes to which cases the above mentioned prohibition does not apply.

Record keeping

Pursuant to Article 98 of the Law, the obliged entity keeps records of data on customers, business relationships and transactions from Article 8 of the Law, data from Article 99, paragraph 1, items 4) and 6) of the Law, as well as those submitted to the Administration for the Prevention of Money Laundering in accordance with Article 47 of the Law (transactions over 15,000 Euros or more in dinar equivalent, suspicious transactions).

The obliged entity is obliged to keep records of the data and information collected in accordance with the Law and by-laws in electronic form, as well as the documentation related to those data and information in chronological order and in a way that allows adequate access to those data, information and documentation .

The obliged entity is obliged to provide a comprehensive search of data and information records that are kept in electronic form at least according to the following criteria: first and last name, date of transaction, amount of transaction, currency of transaction.

The obliged entity shall determine in its acts the manner and place of storage and the persons who have access to the mentioned data, information and documentation.

Protection of the integrity of the authorized person and employees

The obliged entity is obliged to take the necessary measures to protect the authorized person and employees who implement the provisions of the Law from violent actions aimed against their physical and psychological integrity.

X Internal acts

In accordance with the provisions of the Law, the obliged entity is obliged to adopt and apply appropriate internal acts, which, for the purpose of effective management of prevention of money laundering and financing of terrorism, will include all actions and measures for the prevention and detection of money laundering and financing of terrorism defined by the Law, by-laws adopted on the basis of the Law and these guidelines. The obliged entity is obliged to take into account the established risks of money laundering and financing of terrorism in its internal acts, whereby those acts must be proportionate to the nature and scope of business, as well as the size of the obliged entity, and must have the approval of a member of the top management. The obliged entity is obliged to ensure the implementation of these internal acts by determining the appropriate procedures and internal control mechanisms.

The obliged entity is obliged in particular to regulate by internal acts the following:

- the process of creating a risk analysis of money laundering and terrorist financing;
- procedures and mechanisms for detecting suspicious transactions and/or customers, as well as the way employees act after recognizing such transactions and the procedures for providing information, data and documentation at the obliged entity's level;
- determining the persons in charge of performing the obligations from the Law - the authorized person and his deputy, as well as ensuring the conditions for their work;
- determination of the customer's risk category, services, transactions;
- the procedure for carrying out actions and measures of knowing and monitoring the customer, regular monitoring in accordance with the established risk category, including checking the compliance of the customer's activities with usual behavior, as well as a possible change in the risk category;
- the procedure for implementing increased actions and measures of knowing and monitoring the customer in the case of high-risk customers, and especially the procedure for determining whether the customer is an official;
- the procedure of regular internal control of the fulfillment of obligations stipulated by the Law;
- the procedure for conducting regular professional education, training and development;
- procedures for internal reporting for violations of the provisions of the Law through a separate and anonymous channel of communication;
- record keeping, protection and storage of data from those records.

An integral part of the internal acts is a list of indicators for identifying persons and transactions for which there are grounds for suspicion of money laundering or financing of terrorism.

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

APPLICATION OF GUIDELINES

Obliged entities are obliged to coordinate their business activities with the contents of the Guidelines and to elaborate internal acts, in accordance with the provisions of the Law on the Prevention of Money Laundering and Financing of Terrorism.

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

On the day the application of these Guidelines begins, the Guidelines for assessing the risk of money laundering and financing of terrorism for obliged entities who organize special games of chance in gaming venues and games of chance through means of electronic communication No.424-01-116/2021-01 from February 23, 2021 shall cease to be valid.

Director
Zoran Gašić (*signed*)

Republic of Serbia
Ministry of Finance
Games of Chance Administration
(*round seal*)