Pursuant to Article 90 of the Prevention of Money Laundering and Terrorist Financing Act (Official Gazette of the Republic of Slovenia), no. 60/07), I hereby issue

**Guidelines for the Implementation of the Prevention of Money Laundering and Terrorist Financing Act for Concessionaires and Operators Offering Games of Chance**

**Article 1**

These Guidelines shall enter into force on the date on which they are signed by the Director of the Office of the Republic of Slovenia for Gaming Supervision, and published on the website of the Office of the Republic of Slovenia for Gaming Supervision.

**Article 2**

Concessionaires shall bring their internal acts in line within three months of the entry into force of these Guidelines.

Boris Kovačič
Director
1. INTRODUCTION

Organised crime, specifically with regard to money laundering, remains a relevant issue, and various forms of terrorist financing have further increased the risk associated with organised crime in recent years. An effective fight against money laundering goes well beyond national boundaries and has become an increasingly complex and global challenge.

Therefore, the Member States of the European Union have undertaken to intensify activities in this field by adopting the following two Directives:

- Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of “politically exposed person” and the technical criteria for simplified customer due diligence procedure and for exemption on grounds of financial activity conducted on an occasional or very limited basis.

The adopted Directives follow the recommendations of the Financial Action Task Force (hereinafter: the FATF), which is one of the key international bodies involved in combating money laundering and terrorist financing. In line with these recommendations, their implementation is mandatory and no longer a matter of greater or lesser awareness. In June 2007, the National Assembly of the Republic of Slovenia adopted a new Prevention of Money Laundering and Terrorist Financing Act thus complying with the acquis and transposing the requirements of these Directives into Slovenian legislation. The Prevention of Money Laundering and Terrorist Financing Act (hereinafter: the APMLFT) entered into force on the fifteenth day of its publication in Uradni list RS (Official Gazette of the Republic of Slovenia) no. 60/2007, i.e. on 21 July 2007, and became fully applicable on 21 January 2008. One of the important novelties introduced by the APMLFT is a risk-based approach. Accordingly, the persons under obligation referred to in Article 4 of the APMLFT are obliged to draw up a risk analysis in order to assess risk for individual groups of customers, business relationships, products and services from the viewpoint of potential misuse for money laundering or terrorist financing purposes with a view to implementing appropriate measures based thereon.

An indirect or so-called ‘off-site’ supervision of implementing the provisions of the APMLFT is exercised by the Office of the Republic of Slovenia for Money Laundering Prevention (hereinafter: the Office) operating as an administrative body within the Ministry of Finance of the Republic of Slovenia. The Office acts as a clearing house between financial institutions and other business entities as well as law enforcement authorities. It receives, collects, analyses and disseminates data obtained from the persons under obligation referred to in Article 4 of the APMLFT, and submits such data to the competent authorities only in cases as provided by the law.

A direct or the so-called ‘on-site’ supervision of legal entities, i.e. concessionaires operating games of chance in the Republic of Slovenia, falls under the competence of the Office of the Republic of Slovenia for Gaming Supervision (hereinafter: the UNPIS). Article 90 of the APMLFT authorises the UNPIS, in its capacity as a supervisory body, to issue, autonomously or with other supervisory authorities, recommendations and guidelines relating to the implementation of the measures prescribed for the detection and prevention of money laundering and terrorist financing.

These guidelines are advisory in nature and intended for legal entities operating games of chance (hereafter: concessionaires) in order to enable an easier understanding and implementation of the APMLFT provisions.
2. GENERAL REMARKS ON MONEY LAUNDERING AND TERRORIST FINANCING

The APMLFT defines money laundering as an activity carried out for the purpose of concealing the origin of money or other proceeds of crime, and includes: the conversion or transfer of money or other proceeds of crime, and the concealment or disguise of the true nature, source, location, movement, disposal, ownership or rights of funds or other criminal proceeds.

Money laundering is a separate criminal offence through which one conceals or disguises the illegal nature or source of proceeds obtained by committing a criminal offence (usually the abuse of authority, fraud, tax evasion, illicit drug trafficking, illicit arms trafficking, corruption offences, etc.), for the purpose of making unlawfully obtained proceeds appear as legally acquired assets. The ultimate objective of money laundering is to gradually integrate 'laundered' money or property into a criminal activity (existing or new) or into standard business flows which form an integral part of a lawful business activity.

In accordance with the APMLFT, terrorist financing means the direct or indirect provision or collection of funds or other property of legal or illegal origin, or the attempted provision or collection of such funds or other property, with the intention that they be used in full or in part for the performance of a terrorist act, or that they be used by a terrorist or terrorist organisation. In contrast to money laundering, where the subject of concealment or disguise may be only illegally gained assets – which means assets gained by a previously committed criminal offence – terrorist financing resources that are intended for the performance of terrorist acts or used by terrorists or terrorist organisations may be either of legal (personal income, profit, humanitarian assets, sponsor assets, etc.) or of illegal origin (assets gained from criminal offences, e.g. tax evasion, offences related to corruption, drug or weapon trafficking, etc.).

In the field of combating terrorism, the Republic of Slovenia adopted the Act Relating to Restrictive Measures Introduced or Implemented in Compliance with Legal Instruments and Decisions Adopted within International Organisations (hereinafter: the ZOUPAMO – Official Gazette of RS, no. 127/06).

The restrictive measures currently implemented in the Republic of Slovenia are based on the legal acts of the UN Security Council and the EU, but may also be introduced on the basis of binding or non-binding acts of other international organisations or associations (e.g. the OSCE).

These measures may entail the partial or full cessation of economic relations, and railway, maritime, air, postal, telegraphic, radio and other means of communication, and the severance of diplomatic ties, while the most common measure in combating terrorism is financial sanctions, including the freezing of funds on accounts and/or the prohibition of the disposal of property (economic resources) in general, a military embargo, which means prohibition from arms trading with a certain country or other entities, as well as a travel embargo, which includes banning certain persons from entering a country or transiting through its territory. Restrictive measures may be imposed against countries, international organisations, other entities, natural persons (e.g. heads of state, high state officials, terrorists) and other entities, especially terrorist organisations, whereas persons subject to sanctions may also include legal persons. The list of persons subject to sanctions form part of legal acts which introduce sanctions.

The implementation of the ZOUPAMO falls within the competence of the Ministry of Foreign Affairs – International Law Division. For more information, please visit the website of the Ministry (http://www.mzz.gov.si/si/zunanja_politika/mednarodna_varnost/omejevalni_ukrepi/) – or the Office (http://www.uppd.gov.si/slov/mnenjaAPMLFT/mnenja 13 1.htm).
3. REGULATION OF GAMES OF CHANCE, MONEY LAUNDERING AND TERRORIST FINANCING

In the Republic of Slovenia, games of chance, as a specific and special activity, are subject to strict and detailed regulatory law governing the aforementioned field, comprehensive implementing regulations, as well as subject to concession contracts that, among other things, impose on the concessionaire that special games of chance also be operated in accordance with the law governing money laundering and terrorist financing.

The operation of games of chance is an exclusive right of the state. The state may transfer this right to entities that must comply with the statutory requirements. By issuing a decision granting concession and a special concession contract, the Government of the Republic of Slovenia grants concessionaires and operators of special and classic games of chance the above-stated right for a limited period of time and within the previously stipulated scope of operation.

In the Republic of Slovenia, the entrance to casinos and gaming halls (concessionaires of specific games of chance) is only allowed to persons of 18 years of age or more; each player must register at the reception desk, where by means of a computer programme the following data are recorded and kept: name and surname, birth date, place and country of residence, address, type and number of personal identification document, date and time of entering the casino or gaming hall and a photograph of the player. The players must identify themselves to the receptionist at the entrance by producing a valid personal identification document with a photograph.

The reception and the entire gaming floor (including the retention of money, chips, etc.) are to be under continuous audio-video monitoring; these devices record all processes of the operation of games of chance; a concessionaire is obliged to keep the video-recordings for at least seven days since their being made.

The law also covers in detail the entirety of cash transactions of the concessionaire, which besides cash desk transactions also includes transactions through self-service kiosks, vaults and mandatory daily accounts.

In the course of the gaming activity, the concessionaire is obliged to monitor and keep records of all individual transactions of bets and wins of the games of chance; in the event of a one-off win at a gaming machine that exceeds EUR 15000, the concessionaire must take a photo in the gaming hall of the winning combination and record it in the log book of high winning amounts containing the following data: the registered number of the gaming machine that produced the winning prize, prize value, date and exact time of the prize winning, the name and surname of the surveillance person during the pay-out time, and the name and surname of the person who redeemed the amount.
The regularity of the gaming operation and a high level of professionalism in gaming are ensured through the verification of the technical performance of individual gaming machines prior to their use, which is carried out by a special and qualified institution appointed by the Minister of Finance, as well as the verification of the licence obtained by employees for a particular task or work (e.g. cashiers, in-house supervisors, providers of individual games of chance).

Within the framework of the prevention of money laundering and terrorist financing, the prescribed information system of monitoring gaming devices, connected with the information system of the supervisory authority, serves as an extremely efficient tool for concessionaires and the supervisory authority (UNPIS), enabling the supervisory authority a direct and continuous online monitoring of the processes connected with the operation of special games of chance. The monitoring information system reliably monitors, records and retains the data on gaming and the events on individual gaming machines, and comprehensively includes the cashier operation connected with the operation of the games of chance on individual gaming devices and in casinos. The gaming machines and gaming tables provided by the concessionaires of special games of chance are thus supervised through various and independent systems of internal and external monitoring, and constant comparisons of situations and data, which efficiently reduce the degree of risk of potential fraud and money laundering.

Within the framework of the prevention of money laundering and terrorist financing, the prescribed information system of monitoring gaming devices, connected with the information system of the supervisory authority, serves as an extremely efficient tool for concessionaires and the supervisory authority (UNPIS), enabling the supervisory authority a direct and continuous online monitoring of the processes connected with the operation of special games of chance. The monitoring information system reliably monitors, records and retains the data on gaming and the events on individual gaming machines, and comprehensively includes the cashier operation connected with the operation of the games of chance on individual gaming devices and in casinos. The gaming machines and gaming tables provided by the concessionaires of special games of chance are thus supervised through various and independent systems of internal and external monitoring, and constant comparisons of situations and data, which efficiently reduce the degree of risk of potential fraud and money laundering.

With detailed and strict regulation of the gaming activity and the cross and separate system of internal and external monitoring, and constant comparisons of situations and data, Slovenia efficiently reduces the degree of risk of potential fraud, as well as the possibility of money laundering. The systems prescribed for audio and video monitoring (recorded material and records retention of the entire cashier operation, reception, all gaming machines, channels for transferring money, chips, vouchers, etc.), the documents prescribed for individual transactions, the information system for monitoring, the organisational structure that strictly separates the operational procedures from the procedures of supervision and control, on-line monitoring in combination with frequently unannounced inspections of the concessionaire by the UNPIS: all of these enable a high degree of transparency in operations and basically minimise potential violations related to the APMLFT.

All concessionaires have tasks and authorised persons who are responsible for the implementation of these tasks listed in their internal regulation laying down the organisation and tasks of the persons under obligation of the APMLFT; as regards the internal supervision, the supervisors monitor the events during the entire process of the operation of games of chance, ranging from the monitoring of the functioning of gaming machines, the behaviour of players, reception operations to cashier operations, and the transferring of chips, money and vouchers.

In any transaction, internal supervisors and other employees must pay special attention to indicators leading to a suspicion of money laundering.

The introduction of 'responsible gaming', defined in amended concession contracts and the proposal for legal changes, imposes on concessionaires greater concern and increased responsibility for the operation of games of chance, also in terms of the supervision of the excessive spending of cash intended for the participation in games of chance by individual players, which indirectly increases the supervision over a player's spending within the meaning of the APMLFT.

As regards non-face-to-face business, it should be noted that Slovenia allows the operation of games of chance via the Internet only to those concessionaires that have already obtained the concession for the casino or classic games of chance, and that have met all the conditions stipulated in special rules and additional contents under the concession contract.

Sports betting and business relations with customers/players via the Internet are regulated, besides the rules, by the 2009 amended Decree on detailed conditions to be met by permanent organisers of classic games of chance, which stipulates in Article 10 that the technological processes must be designed in accordance with the gaming rules and must lay down the procedures for the identification of customers and transactions in respect of which there are grounds to suspect money laundering or terrorist financing, and the conduct of the operator.
Concession contracts for classic games of chance lay down that the operator is bound by the APMLFT to indicate in the technological processes of such types of games of chance that the participation in these games is allowed only to players who are 18 years of age or older and have an open casino account (the age limit has been taken into account in the draft amendment to the Gaming Act) and that, prior to obtaining the gaming operator's licence, the operator must ensure the connection of the online gaming system with the monitoring information system of the UNPIS. A technological process, organised by the concessionaire, is confirmed by the UNPIS; the process lays down restrictions that mitigate the risk of money laundering and terrorist financing by setting limitations for the opening of a casino account, limitations for the amounts of daily and monthly deposits into the account, as well as by providing for the identification of the casino account holder, and for the amounts that the concessionaire offering sports betting deposits to the player's transaction account and are substantially lower from the amounts laid down by the APMLFT.

Such methods of operation and identification of players using internet casinos, and limitations for transfers to the casino account in the aforementioned system are supervised by the banks that are thus able to monitor suspicious transactions relating to deposits into the casino account or the pay outs made to the player's transaction account.

According to the report 'FATF 40 Recommendations' from 2003, the 'gaming sector' poses a higher money laundering or terrorist financing risk, which increases the obligation of casinos to perform enhanced customer due diligence, keep the data, report on suspicious transactions and adequate regulation and supervision of this activity. Casinos (as well as gaming halls and those entities operating casino internet services) deal in intensive cash transactions (open 24 hours a day, large cash transactions in a short time, etc.), offering a variety of financial services or transactions (currency exchanges, issuing cash, exchange of chips for cash); consequently, due to the nature and scope of business, they represent a number of challenges for the implementation of the guidelines for the prevention of money laundering and terrorist financing.

The overall regulation of the gaming sector must be complimentary with the APMLFT; accordingly, all persons under the obligation of the APMLFT must adopt measures within the framework of both laws in order to achieve the maximum effect in the prevention of money laundering and terrorist financing.

The UNPIS remains responsible for the supervision over the implementation of the APMLFT provisions in the gaming sector and it performs the tasks of the offence authority for the violations related to the APMLFT. The APMLFT imposes on supervisory authorities a new task, i.e. to issue recommendations or guidelines relating to the implementation of the provisions of this law and to cooperate in the drawing up of the list of the indicators referred to in the first paragraph of Article 51 of the APMLFT.

Pursuant to Article 4 of the APMLFT, the persons under obligation in the gaming sector are as follows: concessionaires organising special gaming in casinos or gaming halls, operators regularly offering sports betting, and operators and concessionaires offering games of chance via the internet or other telecommunications means (persons under obligations pursuant to the APMLFT; hereinafter: concessionaires).

One of the important new features introduced by the APMLFT is a risk-based approach. Consequently, on the concessionaires is imposed the obligation of drawing up 'a risk analysis' to assess the risk for individual groups of customers, business relationships, products and services from the viewpoint of potential misuse for money laundering or terrorist financing purposes with a view to implementing appropriate measures based thereon. The analysis is to be prepared in accordance with the guidelines issued by the competent supervisory authority, i.e. the UNPIS (referred to in Article 85 of the APMLFT), in accordance with its competencies.
4. TASKS OF CONCESSIONAIRES UNDER THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING ACT (APMLFT)

Article 5 of the APMLFT imposes on the persons under obligation, which also include concessionaires engaged in organising games of chance, measures to detect and prevent money laundering and terrorist financing. In view of the above, the persons under obligation must also include the preventive measures prescribed in order to mitigate the risk of money laundering or terrorist financing.

For the purpose of detecting and preventing money laundering and terrorist financing, concessionaires must carry out the following tasks:

1. apply measures to acquire knowledge about the customer (hereinafter: customer due diligence) under the terms and conditions provided by the APMLFT, and prepare a preliminary risk analysis;
2. report prescribed and requisite data and submit the documentation to the Office;
3. provide regular professional training and education for employees;
4. protect and store the data and manage the records stipulated by the APMLFT;
5. prepare a list of indicators for the identification of customers and transactions for which grounds exist to suspect money laundering and terrorist financing;
6. appoint an authorised person and a deputy authorised person, and provide suitable conditions for their work;
7. provide regular internal control over the performance of tasks under the APMLFT.

4.1 Customer due diligence

Customer due diligence is the key preventive element in the system for the detection and prevention of money laundering. Through a customer due diligence, concessionaires determine and confirm in a credible manner the identity of a customer, the purpose of a transaction and the anticipated nature of a business relationship, thereby reducing the risk of engaging with an unknown customer who might use them for money laundering or terrorism financing.

Customer due diligence measures are applied:

1. when entering into business relations with a customer, whereby a business relation means any business or other contractual relationship linked with carrying out the activity of the person under obligation and is, at the time of the conclusion, anticipated to be of a lasting nature;
2. when carrying out a transaction amounting to EUR 15,000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which are clearly linked;
3. when there are doubts concerning the veracity and adequacy of previously obtained information about the customer;
4. when there is a suspicion of money laundering or terrorist financing in respect of a transaction or customer, irrespective of the transaction amount.

4.1.1 Normal customer due diligence

In accordance with the first paragraph of Article 7 of the APMLFT, customer due diligence comprises the following mandatory measures:

1. determine and verify a customer's identity on the basis of authentic, independent and objective sources;
2. obtain data on the purpose and intended nature of a business relationship or transaction, and other data pursuant to the APMLFT;
3. regularly monitor business activities undertaken by a customer through the person under obligation. Although the customer's identity is determined or verified at the entry to a casino or gaming hall, casinos and gaming halls must establish mechanisms for linking customers to specific transactions in which the customer subsequently, in the process of games of chance, becomes engaged: they must determine the ways to inform the customer of the relevant threshold and what type of due diligence should be conducted in the event of
exceeding the threshold, as well as determine the compulsory deadline for the renewal of records of players at reception.
Given the frequent use of false official personal identification documents (an official personal identification document is any valid official document that bears a photograph and was issued by a competent national authority, e.g. a driving licence), it seems reasonable to annually verify the identity of persons and the identity of a regular 'guest' against another official identification document; however, the aforementioned, as well as all the procedures for carrying out the aforementioned measures of a customer due diligence, must be laid down by the persons under obligation in their internal acts. In the fight against false identification documents, biometric techniques are increasingly used, in particular the system of face recognition, which enables the monitoring of individual guests on the entire casino floor or in the gaming hall, on the basis of the criteria laid down by the concessionaire. Consequently, at the reception desk, the system enables the recognition of persons who would like to enter the casino or gaming hall with false documents i.e. of potential money launderers.

**Ad 1 – Identifying a customer and verifying a customer's identity**

The customer's identity (verification) and/or information collected are verified on the basis of credible, independent and objective sources (e.g. official personal identification documents, public records, qualified digital certificates, passwords, etc.). By verifying a customer's identity, the person under obligation verifies whether or not the data submitted by the customer on his/her identity are true. Where the customer is a natural person, his/her identity is normally established and verified in one step, i.e. on the basis of an official personal identification document.

At the reception desk of a casino or gaming hall or in the event of organising online games of chance, the concessionaire determines and verifies the player's identity and obtains the information on the customer/player referred to in points 6 and 8 of the first paragraph of Article 83 of the APMLFT:

- by inspecting the official personal identification document in the presence of the customer concerned. If all the data required cannot be obtained from this document, the missing data are to be obtained from another valid official document submitted by the customer or directly from the customer.
- where Internet gaming is organised and the customer is not physically present when entering a business relationship, the concessionaire is obliged to conduct enhanced customer due diligence, taking into consideration the provisions of the implementing regulation concerning the operation of gaming via the Internet and other telecommunications means, and relating to the registration of the player under the APMLFT; the concessionaire must specify in the internal act the procedure for opening a casino account and the procedure for transferring the payment amounts from the casino account to the player's transaction account, all in conjunction with the identification of a customer.

When carrying out a transaction equal to or above EUR 15000 or more, the following data must also be obtained:

- full name, address of permanent or temporary residence, and place and date of birth date and place of birth, and tax number of the player;
- date and time of the transaction;
- amount of the transaction and currency in which the transaction is carried out;
- purpose of the transaction;
- manner of effecting the transaction.

**Ad 2 – Ongoing monitoring of business activities**

The concessionaires must closely monitor activities undertaken by their customers and thus acquire knowledge about the customer, including knowledge of the origin of assets used by the customer in games of chance. The scope and frequency of monitoring depend on the size of the business operation and the risks of money laundering and terrorist financing assessed.

The monitoring of business activities carried out by customers with concessionaires includes:
- verification of the compliance of the customer's business operations with the purpose and intended nature of the business relationship which the customer entered when participating in games of chance;
- monitoring and verification of the compliance of the customer's business operations with his/her regular scope of business;
– verification and updating of obtained documents and information on the customer.
4.1.2 Special types of customer due diligence

As a rule, persons under obligation must conduct customer due diligence; the APMLFT envisages two special forms of customer due diligence – simplified and enhanced customer due diligence.

a) Enhanced customer due diligence

Customers who pose a high risk must be subject to enhanced due diligence, whereby the person under obligation ensures additional supervision in terms of providing adequate management of higher risks associated with such customers. The cases in which the person under obligation must carry out enhanced customer due diligence are specified in the APMLFT. Enhanced customer due diligence is also mandatory in cases where the obliged person's risk analysis indicates a higher risk.

When entering a business relationship or carrying out a transaction equal to or above EUR 15,000 for the politically exposed person (hereinafter: PEP) referred to in Article 31 of the APMLFT, enhanced customer due diligence must be carried out. In this case the concessionaire offering games of chance must, in addition to the measures referred to in the first paragraph of Article 7 of the APMLFT, also adopt the following measures:

- the person under obligation is to acquire information on the source of funds and property that are or will be the subject of a business relationship or transaction from documents and other credentials submitted by the customer. When such information cannot be obtained in the described manner, the person under obligation obtains it directly from the customer's written statement;
- the employee who conducts the procedure for establishing a business relationship with the customer who is a foreign PEP must obtain a written approval of a senior responsible person prior to concluding such a relationship;
- after the business relationship has been established, the person under obligation must monitor the transactions and other business activities effected through the person under obligation by the foreign PEP with due diligence.

Enhanced customer due diligence is conducted if a customer is not present in person when his/her identity is determined and verified (Article 32 of the APMLFT), and if a player participates in Internet special games of chance and sports betting.

If a customer is not present in person when business relationship is established with the person under obligation or when a transaction equal to or above EUR 15,000 is carried out, the person under obligation must, in addition to mandatory measures, take one or more additional measures, such as the acquisition of additional documents, data or information on the basis of which the person under obligation verifies the customer's identity or verifies his/her identity using a qualified digital certificate, which is issued by a certification authority located in the Republic of Slovenia in accordance with the Act governing electronic commerce and electronic signatures. Any data that are not available on the aforementioned certificate may be obtained from a copy of the official personal document sent by the customer to the person under obligation in paper or digital form. In cases in which all the data required cannot be obtained in the manner described above, the missing data are obtained from the customer directly. The use of the customer's qualified digital certificate is one of several options available to determine and verify his/her identity; as a rule, his/her attendance in person is required. A business relationship can be established in the absence of the customer solely if the person under obligation adopts a measure ensuring that the customer's first payment is made by debiting the account that the customer opens in his/her name or holds opened with a credit institution/bank prior to carrying out any subsequent transaction through the person under obligation.

Internet casinos and betting shops require specific methods of customer identification. The FATF Recommendations recognise that non-face-to-face business relationships or transactions can carry greater risks. For that reason, enhanced customer due diligence is necessary (application of new technologies, including the deposit and withdrawal methods offered on the website, and checks on the customer's IP address).
Internet casinos and betting shops often do not meet their customers, which prevents their subsequent identification on the basis of documents. If basic databases are not sufficient, Internet casinos and betting shops can use other sources: traditional checks using customer's personal documents, checks on customers' source of funds (a customer's credit history can be obtained from a credit reference agency with the written permission of the customer), using direct contact via telephone or email, etc.
Moreover, persons under obligation apply enhanced customer due diligence measures when they assess that there is or there may be a high risk of money laundering or terrorist financing due to the nature of the business relationship, form or manner of executing the transaction, customer's business profile or other circumstances associated with the customer.

b) Simplified due diligence

Simplified due diligence may be applied for customers representing a low risk, which enables the person under obligation to waive certain measures and acquire reduced set of data prescribed by law. Types of customers in respect of which simplified customer due diligence is allowed are defined by Article 33 of the APMLFT and the person under obligation must not extend simplified customer due diligence to other categories of customers.

Since the law allows to the application of simplified customer due diligence only to legal entities, such a check is not possible in the operation of games of chance, where the players are natural persons only.

5. REPORTING INFORMATION

5.1 Reporting of cash transactions

Pursuant to the APMLFT, the person under obligation must furnish the Office with the data on any customer's cash transaction exceeding EUR 30,000 immediately after the transaction is completed or not later than three working days following its completion; the data must be submitted on a reporting questionnaire on the cash transactions exceeding EUR 30,000, which forms an integral part of the Rules on the method for reporting information to the Office of the Republic of Slovenia for Money Laundering Prevention (Ur. l. RS, no. 10/08), and also available on the webpage of the Office (http://www.uppd.gov.si/slov/zakonodaja/obrazci_APMLFT.htm).

A cash transaction means any transaction through which the person under obligation receives or hands over cash in an amount exceeding EUR 30,000 (in banknotes and coins), irrespective of the currency. When establishing the cash transaction amount that the person under obligation must report to the Office, the cash amounts received and handed over are not to be aggregated.

5.2 Reporting of suspicious transactions

The persons under obligation - concessionaires must furnish the Office with the data referred to in the first paragraph of Article 83 of the APMLFT whenever there is a suspicion of money laundering or terrorist financing associated with a transaction; this information must be submitted prior to carrying out the transaction and must specify the time limit in which the transaction is to be carried out. Such report may be submitted by telephone but must also be sent to the Office in writing the next working day at the latest. The aforementioned data are submitted to the Office in a Questionnaire for reporting information about the transactions and customers in respect of which there are grounds for suspicion of money laundering or terrorist financing, stipulated in the Rules on the method for reporting information to the Office of the Republic of Slovenia for Money Laundering Prevention (Ur. l. RS, no. 10/08) and also available on the webpage of the Office (http://www.uppd.gov.si/slov/zakonodaja/obrazci_APMLFT.htm).

A customer, transaction or business relationship is assessed based on the suspiciousness criteria from the list of indicators for identification of customers and transactions in respect of which reasonable grounds to suspect money laundering exist or from the list of indicators for identification of customers and transactions in respect of which reasonable grounds to suspect terrorist financing exist. The aforementioned lists are annexed to these Guidelines and help employees detect suspicious circumstances associated with a customer, transaction carried out by a customer, or business relationship concluded by a customer, therefore the employees must be acquainted with the indicators and use them continuously in their work.
What is a suspicious transaction?

The APMLFT does not provide a definition of a suspicious transaction. Under the APMLFT provisions, the term 'suspicious transaction' may imply any transaction whose nature, complexity, scope, value or relation renders it unusual, or any transaction which has no apparent economic or visibly lawful purpose and/or is not in compliance or is out of kilter with the usual or expected business of a customer, as well as other circumstances related to the status and other characteristics of the customer. Individual transactions, customers and business relationships may be qualified as suspicious.

6. PROTECTION AND STORAGE OF INFORMATION AND MANAGEMENT OF RECORDS

Any information acquired and managed under the APMLFT and the Rules on exercising internal control, authorised person, storage and protection of information, and management of records with respect to organisations, lawyers, law firms and notaries (Ur. l. RS, no. 10/08) must be protected by persons under obligation - concessionaires as a business secret or classified information in accordance with the law regulating classified information, provided that the information is classified as such by the Office.

Persons under obligation - concessionaires must keep the information and supporting documentation for ten years after the expiry of a business relationship or the execution of a transaction.

The duty to protect the aforementioned classified information does not apply if the data are necessary to establish facts in criminal proceedings, if the submission of the data is required or imposed in writing by the competent court, or if the data from the concessionaire are required by the Office appointed for the supervision of the implementation of the APMLFT.

The exemption from the principle of the protection of classified information also applies in the event that a concessionaire is obliged to submit information to the Office pursuant to the APMLFT. In such event, the concessionaire's employees are not held liable for the damage caused to customers or third persons if they have acted in accordance with the APMLFT or at the request of the Office.

Pursuant to the first paragraph of Article 82 of the APMLFT, concessionaires must manage the records of data on all the customers, business relationships and transactions referred to in Article 8 of the APMLFT, as well as the records of data reported to the Office referred to in Article 38 of the APMLFT.

7. PROFESSIONAL TRAINING AND EDUCATION

The concessionaire must provide regular professional training and education for all employees carrying out tasks for the detection and prevention of money laundering and terrorist financing. Professional training and education relate to information about the provisions of the APMLFT and any ensuing regulations and internal regulations, about professional literature relating to the prevention and detection of money laundering and terrorist financing, and information about lists of indicators for identifying customers and transactions in respect of which reasons exist for a suspicion of money laundering or terrorist financing.

Persons under obligation must draw up an annual professional training and education programme for the prevention and detection of money laundering and terrorist financing by no later than the end of March for the current year.

8. AN AUTHORISED PERSON FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

In order to carry out tasks pertaining to the detection and prevention of money laundering and terrorist financing stipulated by the APMLFT and ensuing regulations, the concessionaires must appoint an authorised person and one or more deputies for the prevention of money laundering and terrorist financing (hereinafter: the authorised person) in accordance with Article 40 of the APMLFT.
The persons under obligation must ensure that the authorised person who performs the tasks under the APMLFT also observes the following guidelines:

1. offers professional assistance to employees in the operational implementation of measures for the detection and prevention of money laundering and terrorist financing;
2. advises the management of the person under obligation on the money laundering and terrorist financing risk management policy;
3. updates the management of the person under obligation on such person's activities relating to the detection and prevention of money laundering and terrorist financing;
4. cooperates with other persons under obligation in formulating a consistent policy for the detection and prevention of money laundering and terrorist financing.

9. INTERNAL CONTROL

The persons under obligation must set up regular, systematic and independent control over the regularity and efficiency of the implementation of the measures prescribed for detecting and preventing money laundering and terrorist financing in accordance with the Rules on exercising internal control, authorised person, storage and protection of information, and management of records with respect to organisations, lawyers, law firms and notaries (Ur. l. RS, no. 10/08). The primary purpose of internal control is to detect and remedy deficiencies in the implementation of measures prescribed for detecting and preventing money laundering, and to improve the system for detecting customers or transactions that raise a suspicion of money laundering and terrorist financing.

As a part of internal control, the concessionaire is obliged to ensure control of the regularity and efficiency of the implementation of the measures prescribed for detecting and preventing money laundering and terrorist financing by external contractors and representatives entrusted with the implementation of part of the concessionaire's tasks on the basis of an appropriate contract.

If so requested by the Office, the persons under obligation must draft in writing an annual report on internal control and measures carried out in the previous year and submit it to the Office no later than 15 days of receipt of the request.

10. RISK ANALYSIS

10.1 Purpose of Risk Analysis

Concessionaires must comply with the requirements imposed by the legislation on games of chance and implement measures to prevent money laundering and terrorist financing in accordance with the APMLFT. Notwithstanding the scope and efficiency of these measures, the fact remains that perpetrators of criminal offences will persist in their endeavours to surreptitiously carry out transactions in illegal resources and will therefore also target non-financial undertakings and companies operating games of chance. With regard to the effectiveness of the prevention of money laundering and terrorist financing, this potentially renders the operators of games of chance more vulnerable or exposed.

According to the APMLFT, a risk of money laundering or terrorist financing means the risk of a customer misusing the person under obligation for money laundering or terrorist financing purposes, or a risk of a business relationship, transaction or product or service offered by the person under obligation, e.g. the operation of games of chance, being misused for money laundering or terrorist financing purposes. In order to prevent excessive exposure to the negative effects of money laundering and terrorist financing, the person under obligation must, in accordance with the APMLFT, draw up a risk analysis in order to establish the level of risk of money laundering or terrorist financing associated with an individual customer, business relationship, service or transaction (risk assessment).
The preparation of a risk analysis is a prerequisite for the implementation of prescribed customer due diligence, as the placement of a customer, business relationship, service or transaction in one of the risk categories determines the type of customer due diligence the person under obligation will have to carry out in accordance with the APMLFT (normal due diligence, enhanced due diligence, simplified due diligence). The risk analysis or the procedure to establish a risk assessment must reflect the specific features of an operator of games of chance and its operations (e.g. its size and composition, scope and structure of business, types of customers doing business with, types of services offered, types of technology used for organising games of chance or making payments, etc.). By dealing with their customers and businesses on the basis of a risk-based approach, the concessionaires can adjust to current risks more successfully and efficiently and focus their attention and resources on those customers and businesses that pose a greater risk for money laundering and terrorist financing.

The risk-based approach to combating money laundering and terrorist financing should enable the customers to access the services provided by the concessionaires, but creates barriers to those who seek to misuse the gaming system. The risk-based regime is not set up in a manner to hinder the concessionaires in their business operations, but it allows the flexibility of measures to more efficiently adjust to the development and application of new methods for combating money laundering and terrorist financing.

A risk analysis of the concessionaires operating games of chance must take into account the following factors related to players-customers (number, frequency of visits, domestic-foreign relations, the manner and frequency of playing), transactions (manners of payment to and from the account, the number of transactions above/below the threshold of compulsory supervision or a substantial number of transactions with non-gaming activity, etc.), and the frequency and the manner of paying out the prizes won through games of chance.

The analysis and risk assessment are made with respect to each organisational unit, individual section, which allows the concessionaire to specify to which customers, transactions and prizes particular attention must be paid in individual stages of games of chance.

The concessionaire may adopt different strategies and approaches in the development of risk-based programmes for anti-money laundering and combating terrorist financing.

The risk analysis should also take into account the following:

- a comprehensive understanding of the risk of the concessionaires, since they provide not only games of chance and entertainment but, within their scope of business, also other services and financial transactions, which expose them to money laundering and terrorist financing risks;
- the diversity, frequency and scope of transactions make the gaming industry more vulnerable to money laundering and terrorist financing as the majority of transactions are cash-based, electronic transactions;
- the use of casino-based gaming tours (so-called 'junkets') that include transport, accommodation, incentives to play at the casino and the movement of funds to and from the casino or gaming hall, the sales of special 'junket chips', payment to agents for the purchase of these chips in percentage, etc.;
- potential criminal interest in casinos, because organised crime groups seek ways to control or own the concessionaires for the purpose of theft, fraud, money laundering and other crimes; casinos and gaming halls are attractive venues for their socialising; they are also often the place providing opportunity for money lending, credit cards fraud, and for inviting casino employees to become involved. Criminals often attempt to take advantage of the gaming equipment and connected computer systems for money laundering in all the stages of games of chance;
- possibility of the employee complicity in money laundering operations in the gaming process (e.g. accomplices in criminal offences), which most often makes it conditional on the bribability of employees or inadequate training of employees (e.g. this is confirmed by the statistics of such criminal offences in Nevada). The methods include: failing to file suspicious transaction reports or threshold transaction reports, destroying of documents, transactions reports related to the customer due diligence or reporting processes, falsifying player ratings, etc.;
various methods of payments and pay outs in the gaming process. The concessionaires simultaneously use various payment options for betting with respect to the participation of players in games of chance, from direct cash deposits into gaming machines via note acceptors to the 'credit' obtained by the player through a direct deposit into note acceptors, tickets or chips that can be bought at the cashier's desk or won, as well as the possibilities of the direct purchase of chips at tables, and deposits through a casino account (online casinos). The purchase of tickets, chips and deposits to a casino account for the purpose of participating in a game of chance can be made through credit cards, various cheques, payments in betting shops, online bank payment systems, mobile payment systems; in organising sports betting: in addition to the match-fixing and connections to betting shops and their setting of the quota, it is also necessary to take into account the regulatory tools that a concessionaire incorporates into the operational system, e.g. automatic bet amount limitations for specific amounts of money, limitations on the number of betting slips per individual player, payment methods for betting, e.g. if a player places a higher number of betting slips on a higher quota and not on a favourite, etc.;

compliance with and knowledge of money laundering methods and techniques in gaming processes (from structuring and refining, cash, casino chips, tickets, use of gift certificates, chip purchase vouchers, casino reward cards, purchase of chips from 'clean' players at a higher price, use of chips as currency in illegal transactions, false documents, currency exchange).

A risk-based approach requires the concessionaires to adjust requirements and recommendations to their own business in such a way that, for example, two casinos that are owned by one legal entity may follow the guidelines in a different way in terms of the specification of individual contents.

10. 2 Preparation of Risk Analysis

For an appropriate preparation of risk analysis, first the circumstances affecting the risks in a particular environment or country have to be understood. For these purposes, a risk assessment of a particular country may be prepared with regard to money laundering or terrorist financing.

The following factors (general) must be taken into account:
• legal environment and the regulation of games of chance;
• a country's economic structure;
• sources, location and concentration of criminal activity in connection with games of chance;
• size and nature of the activity carried out by operators of games of chance;
• ownership structure of concessionaires (state-owned, private capital);
• nature of payment systems and prevalence of cash-based transactions;
• geographical spread of concessionaires with regard to customers and businesses;
• types of services offered by concessionaires;
• financial services offered by concessionaires and their intermediaries (e.g. foreign exchange offices, junket promoters, agents);
• type of customers (players, nationality, regular or casual customers);
• types of previous offences committed by participants in games of chance;
• main channels and instruments used for money laundering or terrorist financing, both in general terms and within games of chance;
• characteristics of the economy as well as the casino/ 'gaming sector'.

For establishing an appropriate approach based on the risk assessment, the concessionaires must determine the factors or criteria for assessing possible money laundering or terrorist financing risks. The identification of such risks (to the extent to which terrorist financing risks can be detected in advance) and customers or groups of customers, and transactions, will enable the concessionaires to select and implement proportional measures and controls for the management of these risks.
The risk of money laundering and terrorist financing may be determined based on assessments of various types of risks. The following are the most frequently used factors for assessing the existing risks or types of risks:

- country or geographic risk;
- customer risk;
- transaction risk, including financial risk.

10.2.1 Country or geographic risks

In this context, it is essential to take into account that some countries pose different degrees and types of risks. Factors that may influence the concessionaire's assessment whether a country or a player-citizen participating in games of chance in Slovenia represents a higher risk of money laundering or terrorist financing include:

- countries identified by credible sources as having poor regulations to combat money laundering and terrorist financing, or the regulations are poorly implemented;
- countries identified by credible sources as providing funding or support for terrorist activities of terrorist organisations operating within their country;
- countries identified by credible sources as having significant levels of corruption or other criminal activity;
- countries where the registration of operators of games of chance is not compulsory.

'Credible sources' refers to information or reports of reputable authorities, such as the FATF, MONEYVAL, the International Monetary Fund, the World Bank, etc. that do not have the effect of a legally binding document.

Customers that are associated with higher risk countries (that have poor regulations to combat money laundering and terrorist financing or poorly implement these regulations), as a result of their citizenship, or residence, etc. may require enhanced due diligence; the same applies to cases when the 'location' of the concessionaire is different than the 'location' of the customer-player, i.e. in connection with non-face-to-face cross-border business or transactions (e.g. Internet casinos and betting sites).

10.2.2 Customer risk

The category of a customer and the customer's conduct in individual business transactions, as well as the motivation or the reason for such a deal may pose potential money laundering or terrorist financing risks. Depending on the category they fall into, customers may be a source of concern or reasons for the suspicion, on the basis of which the data about a particular customer must be communicated to the authorised person for money laundering prevention.

The main categories of customers indicating a higher risk are as follows:

- A customer is a politically exposed person.

Politically exposed persons (PEPs)

The APMLFT defines a foreign politically exposed person as any natural person who is or has been entrusted with prominent public function in the previous year and resides in another Member State or in a third country, or a person who is or has been entrusted with prominent public function in another Member State or in a third country in the previous year, including immediate family members and close associates.

Natural persons who are or have been entrusted with prominent public function are the following:

a) heads of state, prime ministers, ministers and their deputies or assistants;
b) elected representatives in legislative bodies;
c) members of supreme and constitutional courts and other high-level judicial authorities against whose decisions there is no ordinary or extraordinary legal remedy, save in exceptional cases;
d) members of courts of audit and boards of governors of central banks;
e) ambassadors, chargés d'affaires and high-ranking officers of armed forces;
f) members of the management or supervisory bodies of undertakings in majority state ownership.

The immediate family members of the persons referred to above are: spouse, common-law partner, parents, brothers and sisters and children and their spouses or common law partners. The close associate means any natural person who has a joint profit from property or business relationship or has any other close business links.

The person under obligation-concessionaire must establish an appropriate procedure to determine whether a person is a foreign PEP. Such a procedure must be defined in the person's under obligation internal acts while taking account of these guidelines. It is recommended that the concessionaires have their customer sign a statement declaring that the customer is a foreign PEP. Casinos and gaming halls must place a notice, in the Slovenian and two foreign languages, on a visible spot in front of the reception desk, demanding that a foreign PEP declare himself/herself as a foreign PEP, and that at the reception desk such a customer be submitted for signature a statement declaring that he/she is a PEP.

In addition to the procedure described above, the concessionaires may also identify PEPs on the basis of other sources. It is recommended that the concessionaires set up appropriate records showing how a foreign PEP has been identified as such. In these cases, it is not obligatory to submit the statement for signature, since it is considered that the concessionaire has obtained this information otherwise. In case of online gaming, the concessionaire must provide the option described above at its website. If a particular customer is identified as a politically exposed person, the concessionaire must apply additional measures of enhanced customer due diligence.

When assessing the money laundering and terrorist financing risks in the gaming process, the concessionaires must pay particular attention to:

- Customers who are 'high spenders' because of their cumulative spending over a longer period of time with an individual concessionaire. Similarly, usual customers who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders. In this context, the concessionaires must take into account the relative value of the monies in the country where the player obtained his/her wealth, as well as the relative value of the monies in the country where the customer is spending his/her money.
- 'VIP customers' who are provided with special facilities for playing, refreshments, food, lodging, tickets for special events. The concessionaires need to ensure that in anti-money laundering activities and combating the financing of terrorism the same measures are applied to this type of customers, particularly for due diligence, recordkeeping, suspicious transaction reporting.
- Disproportionate spenders. Concessionaires should be alert to customers engaged in high value gambling that is inconsistent with the information about the customer, and should adopt measures to obtain information about the customer's source of assets, showing the actual level of the customer's available funds, which subsequently assists in determining the player's limit.
- Casual customers whose spending pattern may be difficult to identify. This category includes tourist-players, with the exception of junket tourists.
- Customers who engage third persons in business operations (use of third parties, or anonymous or identified agents to avoid the identification at a threshold). Third parties may be used to buy chips, or to gamble on behalf of others, or cash out/redeem chips/tickets at the cashier's desk on behalf of a third person.
- The customer organises junkets. Concessionaires can become overly dependent on junket representatives, which can pose a heightened money laundering risk, especially in markets with resident populations that are too small to normally support casinos.
■ Junket operators that provide premium players may exert pressure on casinos, which may result in reducing the quality of supervision over individual spending patterns, or may try to unduly influence the control over some gaming processes. Junket organisers may engage or cooperate in lending money to players outside casinos' knowledge.

■ Customers-players who have opened up multiple player rating accounts with different names at the same concessionaire hinder the concessionaire's ability to track their gambling activities under the same customer name; in this way, the customers attempt to obscure their actual spending level and to avoid identification if the threshold is reached. Consequently, it is essential that the concessionaires introduce measures and procedures for the identification of customers opening multiple accounts with similar players' names and the same physical descriptions (e.g. age, male or female, height, weight, hair colour) to be able to more efficiently monitor customers' aggregate gambling across their casino business.

■ Customers who are unknown and purchase large amounts of chips with cash at table games, but engage in minimal or no play, and then redeem the chips for large denomination bills (e.g. EUR 500) hinder the concessionaire's ability to track their gambling activities under the same customer name; in this way, the customers attempt to obscure their actual spending level and to avoid identification if the threshold is reached.

10.2.3 Transaction risk, including financial risk

Transaction risk is influenced by products, services, games and accounts that can be used to facilitate money laundering and terrorist financing. In risk assessment, the concessionaires (also online operators) should take into account the following factors:

• **Proceeds of crime.** However money is transferred to a casino, gaming hall or betting shop, there is a risk that this money will have arisen from illegal activities, such as check fraud, credit/debit card fraud, narcotics trafficking, or theft from employers. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk.

• **Cash.** Customers may use a casino, gaming hall or betting shop to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport. This may involve certain large cash deposits transferred to customers' casino accounts with no intention to play.

• **Money lending or loan sharking.** This also involves a criminal offence known as usury. Organised crime networks often finance or support loan sharks preying on individuals who are struggling financially (often on those who are addicted to games of chance) or, for some reason, are unable to obtain credit from legal sources.

• **Use of casino deposit accounts** (safekeeping, front money, wagering). Casinos and betting shops will wish to encourage their customers to only use their deposit accounts for gambling purposes. Casinos and betting shops need to define their basic purpose of casino accounts and, through procedures, measures and internal controls, prevent customers from abusing such accounts (i.e. using such accounts to deposit and withdraw without gambling or only with minimal play).

• **Redemption of chips, tickets or tokens for gaming devices.** All casinos and gaming halls do not conduct customer due diligence for the redemption of chips, tickets or tokens, unless it triggers the reporting thresholds as provided for by the APMLFT. As a result, casinos and gaming halls should adopt procedures, measures and internal controls for the identification of large cash outs for customers using such procedures (FATF Recommendation 40 for casinos is EUR 3000).
Internet casinos (online gaming)

Since the online gaming in Slovenia may only be provided by the concessionaires that permanently organise classic games of chance and the concessionaires that already organise special games of chance in casinos, mixed gambling chains can occur, which means that the money can be transferred through land-based casinos (particularly those having introduced cashless transactions) and betting shops to the account of Internet casinos and betting shops. It is therefore imperative that Internet casinos work closely with land-based counterparts and concessionaires providing sports betting that receive the cash to ensure that customer due diligence measures are applied, including verifying the identity that the depositor is the casino account holder.

In assessing the risk, the following factors need to be taken into consideration:

- **Multiple casino accounts** (deposit, credit, check cashing, player rating/tracking, slot club) or 'casino wallets'. A concessionaire of games of chance through the Internet may own multiple websites. Single websites can offer a range of different types of gambling; the concessionaires, therefore, need to monitor customers' aggregate position across the whole of their operations. Customers may wish to separate the different types of gambling they are conducting with the same operator, or through the same website, for legitimate reasons, e.g. to monitor their performance in different areas. Concessionaires providing gaming through the Internet should apply procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.

- Where gaming is organised via the Internet or other telecommunications means through cashless transactions that are applied by the concessionaires in casinos and gaming halls, the concessionaires should lay down limitations in their internal act regulating (for example) casino account transactions, which makes suspicious transactions considerably more difficult (e.g. each player may only open one casino account, the prohibition for issuing power of attorney to another person for casino account transactions, cash limitations in connection with the performance of financial transactions); consequently, the money laundering and terrorist financing risk is to be assessed within this particular framework.

- **Identity fraud.** Details of financial institution accounts may be stolen and used on websites. The numbers and codes of the Internet Provider (IP) are useful in preventing criminals from opening multiple casino accounts using stolen identities, using the same computer. Internet casinos are aware of these risks because of the 'charge back' system, as they have a responsibility to protect their customers from having their identities stolen when using their website.

- **Pre-paid' cards.** Using cash to fund a pre-paid card poses similar risks as cash. Internet casinos cannot make the same level of cross reference checks on some types of pre-paid cards as they are able to perform on financial institution accounts.

- **Electronic wallets (e-wallets).** E-wallets are often not licensed in reputable countries and some accept cash as deposits. However Internet casinos should be aware that when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Internet casino.

- **Games of chance involving multiple operators** (e.g. poker games, tournaments, 'pools') and the role of the platform and chip dumping in risk assessment.

- **Transfers between customers-players.** If concessionaires that provide games of chance through the Internet wish to allow inter-account transfers between their customers, they should adopt careful policies and procedures that monitor the amount of the transfer. Internet casino operators may also be aware of customers transferring money between themselves more informally without using their casino accounts, which should be taken into consideration in the casino operator's risk assessments.
In drawing up the risk analysis, the concessionaire must, in addition to the aforementioned factors, also take into account other circumstances that may impact the risk level:

- the selection of the business model of a casino, gaming hall, betting shop:
  - a large number of customers who gamble relatively small amounts of money, or
  - a small number of customers who gamble relatively large amounts of money, speed and volume of business, types of payment, and customer's payment methods,
- types of gambling offered: table games, card games, gaming machines, electronic games, types of betting;

The type of the customers: regular/permanent or irregular/occasional customers, whether a casino, gaming hall, betting shop forms part of a bigger organisation owned by the same operator, for example:
- whether the casino operator owns other land-based casinos, gaming salons and Internet casinos;
- whether the casino operator offers different types of gambling, e.g. sports betting, card games;
- for internet betting shops, whether the operator has other websites;
- for land-based casinos, gaming halls, whether they are stand-alone or integrated in the hotel's larger services, etc.;
- staffing numbers, turnover rate and experience levels,
- type and effectiveness of existing internet supervision mechanisms (e.g. audio-visual (AV), electronic, information system for monitoring, physical, security, etc.);

- slot kiosk machines for the redemption of chips, money and maximum betting threshold for individual games;
- 'VIP' rooms or other facilities designed for high spending customers, loyalty clubs and other perks provided for particular customers.

10.2.4 Monitoring of customers and transactions

The monitoring of customers and transactions is essential to ensure effective application of anti-money laundering and combating the financing of terrorism policies, procedures, internal controls and automated systems.

Monitoring methodologies and processes must take into account the size, scope and types of games of chance, staffing structure, the technological level of development, pay-in/pay-out systems, the type of information system for monitoring, etc. Casinos and gaming halls that have special surveillance departments with audio-video equipment and maintain records through which they can identify a customer should also include monitoring for potential suspicious transaction reporting in terms of anti-money laundering and combating the financing of terrorism; with the audio and video monitoring system. They should constantly observe and monitor the players, their way of playing, their spending, their behaviour at the cage, their contacts with other players, which would contribute to a more effective implementation of anti-money laundering and combating terrorist financing measures, provided staff are appropriately trained and remain alert.

Internet casinos and betting sites are dependent upon IT systems. These concessionaires need to set up such systems so as to ensure the accurate monitoring of accounts and customers and to ensure that adequate records are kept and retained. Decisions must be made about the details of the transaction records that are to be retained. A risk-based approach cannot solely rely upon IT; there must also be an element of human supervision and staff levels should be proportionate to risk levels.

10.2.5 Reporting of suspicious transactions

The concessionaires need to have systems in place that ensure that reports are made when required and once a suspicion has been formed. The concessionaires should allocate resources and provide staff on the basis of their risk assessment, focusing on those areas that present a greater vulnerability to money laundering and terrorist financing.
10.2.6 Training and awareness

Staff must be trained in accordance with their role and level/nature of responsibilities. Examples of the staff qualifications by individual organisational units: accounting staff, information technology department, finance department, fraud management department, staff who deal with high spenders, customer services staff, compliance staff and surveillance staff, etc.

For Internet casinos and betting sites, such training should be mostly addressed to information technology staff. Individuals who have responsibilities to monitor or approve transactions should receive more comprehensive training than other staff.

Applying a risk-based approach gives each concessionaire flexibility in training, taking into account the frequency of training and individual contents of knowledge delivery.

Concessionaires should review their workforce, available resources and implement training programmes for anti-money laundering and combating terrorist financing that are tailored to the appropriate staff responsibility and specified duties.

10.2.7 Internal controls

When devising internal controls, the concessionaires should consider their overall operation. The management should ensure that the commitment of both staff and their business partners to anti-money laundering and combating terrorist financing is visible, including their personal responsibility to ensure that, as regards anti-money laundering and combating terrorist financing, there are adequate systems and controls in place. The concessionaire's management is in a position to influence the culture of their organisation, including a culture of compliance with the guidelines for the prevention of money laundering and terrorist financing.

The concessionaires should set up a framework of internal controls (e.g. policies, procedures, processes) for all divisions designed for operations against money laundering and terrorist financing. The internal control for anti-money laundering and combating terrorist financing should cover all related activities and programmes, such as reporting suspicious activity, reporting currency transactions, customer due diligence, records retention, and compliance with the guidelines for the prevention of money laundering and terrorist financing. Internal controls should also include account opening and documentation procedures, and management information/monitoring systems adequate to detect and report suspicious activity in a timely manner to authorities. In addition, internal controls should mitigate the inherent risk of any high-risk account, customer, or service as well as transactions to or from a high-risk country (e.g. sanctioned country, non-cooperative country) that could be misused for money laundering or terrorist financing.

The concessionaire's internal controls should be commensurate with:
• the complexity, organisation, and relative size of the business;
• the establishment of a function of compliance with the guidelines for the prevention of money-laundering and terrorist financing;
• risks posed by the types of gambling and financial services offered as well as the volume of business. These procedures include:
  • measures for addressing higher risk customers and their transactions and accounts and ensuring adequate supervision with adequately trained staff;
  • use of appropriate automated systems;
  • regular review and update of the risk assessment.

The concessionaires should conduct independent internal controls, external testing for anti-money laundering and combating terrorist financing programmes with a scope and frequency commensurate with the risks of money laundering and terrorist financing they face, as well as the services provided to ensure comprehensive procedures to detect suspicious activities. Internal control of transactions of casinos, gaming halls and concessionaires operating sports betting should cover:
• customer/staff ratios particularly at busy periods;
• communication of persons responsible for the internal control of transactions within the gaming floor and between individual organisation sections;
• the manner of informing the customer of the relevant threshold (EUR 15000) and of what type of checks will need to be undertaken if the threshold is reached, and what additional data the customer needs to provide.

Where permitted by other legislation, the concessionaires should become users of or subscribe to:

• a national and/or international reporting agency that provides data for the identification of customers (whether the customer applied for credit in another country's casino, data on outstanding debts in other casinos);

• public on-line databases that do not require a subscription;

• 'data mining' agencies that document data on criminal offences, employers, occupations, asset locations, and civil actions such as bankruptcies, judgements, etc.;

• organisations that provide customer due diligence from various business, government, legal, newspaper documents, as well as organisations providing customers' personal information (e.g. name, date and place of birth, address, etc.).

11. ANTI-MONEY LAUNDERING REGULATIONS

• Prevention of Money Laundering and Terrorist Financing Act (Ur. l. RS, no. 60/07);
• Rules on the method for reporting information to the Office of the Republic of Slovenia for Money Laundering Prevention (Ur. l. RS, no. 10/08);
• Rules on exercising internal control, authorised person, storage and protection of information, and management of records with respect to organisations, lawyers, law firms and notaries (Ur. l. RS, no. 10/08);
• Rules on determining the list of equivalent third countries (Ur. l. RS, no. 10/08);
• Rules laying down the conditions to be met by a person in order to be allowed to act as a third party (Ur. l. RS, no. 10/08);
• Rules laying down the conditions under which a person may be considered a customer who represents a low risk of being involved in money laundering or terrorist financing (Ur. l. RS, no. 10/08);
• Rules laying down the conditions for identifying a customer and verifying the customer's identity on the basis of the customer's qualified digital certificate (Ur. l. RS, no. 10/08).

12. ANNEXES

Annex 1 – LIST OF INDICATORS FOR DETECTING SUSPICIOUS TRANSACTIONS FOR TERRORIST FINANCING APPLICABLE TO CONCESSIONAIRES OFFERING GAMES OF CHANCE

A list of indicators is based on two principles: knowledge about the customer and knowledge about the customer's business operations. Knowledge about the customer provides the basis for establishing whether there are grounds for a suspicion of money laundering under Article 245 of the Penal Code (KZ-1). There are grounds for suspicion in respect of any transaction that is not in line with the customer's ordinary course of transactions in games of chance. When dealing with an unknown customer, the indicators not relating to the knowledge of a customer should be taken into account.

When establishing whether there are grounds for a suspicion of money laundering in respect of transactions carried out by individual customers, the indicators should be examined individually or jointly (if there are several indicators present). If only one indicator pointing to a suspicious transaction is present, it may be sufficient to submit data to the Office in some cases, while in other instances this would only be a warning that a transaction and a related customer need to be carefully examined with a view to uncovering other indicators.

Persons under obligation must prepare the indicators to detect suspicious transactions in accordance with the first paragraph of Article 51 of the APMLFT. The UNPIS and the associations and societies, whose members are persons under obligations under the APMLFT, participate in drawing up the list of indicators.
These indicators include the lists of natural and legal persons associated with terrorism and terrorist financing subject to the sanction of assets freeze imposed by the UN Security Council and the EU in the framework of its common foreign policy.

The list of the Security Council of the United Nations is published on the website:  

The list of the European Union\(^2\) is published on the website:  
1. INDICATORS RELATING TO CASINO ACCOUNTS

- A natural person opens multiple casino accounts to receive small payments.
- An account is opened by a natural person involved in the activities of an organisation or a foundation supporting the objectives and demands of a terrorist organisation.
- An account is opened by a natural person which might be linked to a terrorist organisation.

2. INDICATORS RELATING TO THE ESTABLISHMENT OF A BUSINESS RELATIONSHIP

- A natural person establishes several business relationships on the basis of which a number of minor transactions are concluded which are related to games of chance.
- A business relationship is established by a natural person involved in the activities of an organisation or a foundation supporting the objectives and demands of a terrorist organisation.
- A business relationship is established by a natural person which might be linked to a terrorist organisation.

3. INDICATORS RELATING TO CUSTOMERS

- A customer wishes to enter a business relationship that is inconsistent with his/her objectives.
- There is no logical connection between the executed transactions and the customer's activity.
- Statements and data presented in the identification procedure are inconsistent (erroneous reference to residence, nationality, last name, date of birth, etc.).
- A customer comes from (has permanent or temporary residence) a country or region that supports terrorism of terrorist financing.
- A customer is subject to the sanction of assets freeze imposed by the United Nations Security Council or the European Union and appears on their respective lists.

4. INDICATORS RELATING TO TRANSACTIONS

- One person carries out several transactions in the same branch office with a clear intention to use several cashier's desks.
- A deposit of uncounted cash — after the money is counted, the deposit is made into an account in the amounts not subject to the identification or reporting requirement.
- The use of product associated with a high fee payment (e.g. Western Union, MoneyGram).
- A customer uses products (securities, checks, etc.) bearing informal inscriptions, initials or signs in transactions.

Annex 2 – LIST OF INDICATORS FOR DETECTING SUSPICIOUS TRANSACTIONS FOR MONEY LAUNDERING APPLICABLE TO OPERATORS AND CONCESSIONAIRES OFFERING GAMES OF CHANCE

A list of indicators is based on two principles: knowledge about the customer and knowledge about the customer's business operations. Knowledge about the customer provides the basis for establishing whether there are grounds for a suspicion of money laundering under Article 245 of the Penal Code (KZ-1). There are grounds for suspicion in respect of any transaction that is not in line with the customer's ordinary course of transactions when participating in games of chance. When dealing with an unknown customer, indicators that do not relate to knowledge about the customer should be taken into account.
When establishing whether there are grounds for a suspicion of money laundering regarding transactions carried out by individual customers, the indicators should be examined individually or jointly (if there are several indicators present). If only one indicator of a suspicious transaction is present, it may be sufficient to submit the data to the Office in some cases, while in other instances this would only be a warning that a transaction and a related customer need to be carefully examined with a view to uncovering other indicators.

Persons under obligation must prepare the indicators for detecting suspicious transactions in accordance with the first paragraph of Article 51 of the APMLFT.

1. INDICATORS OF MONEY LAUNDERING USING CASINO ACCOUNTS

- Frequent deposits of cash, cheques, wire transfers into casino accounts in a casino, gaming hall.
- Funds withdrawn from the casino account shortly after being deposited.
- Significant casino account activity within a short period of time.
- Casino account transactions conducted by persons other than the account holder.
- Funds credited into the casino account from country of concern.
- Large amounts of cash deposited from unexplained sources.
- Associations with multiple casino accounts under multiple names.
- Transfer of funds from/to a foreign casino/bank account.
- Structuring of deposits/withdrawals or wire transfers.
- Using third parties to undertake wire transfers and structuring of deposits.
- Use of an intermediary to make large cash deposits.
- Use of false or stolen identities to open casino accounts.
- Difficulties with customer due diligence.

2. INDICATORS RELATING TO A TRANSACTION

- A customer purchases chips or tickets and after a short time of gaming activity, or not with gaming activity, exchanges them for cash at the cashier's desk.
- Visible increase in chip or ticket purchases and other increased spending in a casino, gaming hall, which is in disproportion with the usual business operations of a customer.
- A customer purchases chips and tickets successively at various cashier's desks, gaming tables.
- A customer using a large amount of cash through purchases of chips or tickets at various cashier's desks (i.e. 'smurfing').
- A customer often exchanges winnings for cash or often purchases or exchanges chips or tickets at the cashier's desks.
- A customer takes large amounts of chips or tickets from a casino or gaming hall, and exchanges them the next day or in consecutive days.

2. INDICATORS RELATING TO A CUSTOMER

- Use of false or foreign identification documents.
- A person refuses to identify himself with all the requested data or provides false data.
- A person cancels the transaction when learning of customer due diligence obligation.
- A person exhibits unusual behaviour (obviously tense, nervous, etc.).
- A person is accompanied by suspicious people in the casino or gaming hall.
- A person has already been sanctioned or criminal charges have been filed against the person (this is known from the media or notifications provided by the Office, the Bank of Slovenia, etc.);
- A customer requests the certificate of the winning.
- A customer sends another person to perform the transaction at the cashier's desk.
- A person comes from a country known for being a drug producer or tax haven (off-shore centres): countries of the Middle and Far East (e.g. Turkey, Afghanistan, Pakistan, Lebanon), countries of the Golden Triangle (Myanmar, Laos, Thailand), countries in the South America (e.g. Peru, Columbia, Mexico), countries of North and Central Africa (Morocco, Tunisia, Nigeria).
3. **INDICATORS RELATING TO VALUE INSTRUMENTS**

- Customers claiming gaming machine credits/pay outs with no jackpot.
- Customers frequently inserting substantial amounts of banknotes in gaming machines that have high pay out percentages and do not play 'max bet', thereby accumulating gaming credits with minimal bets.
- Frequent even-money betting (e.g., in roulette, baccarat, or craps, etc.).
- Customer's intention to win is absent or secondary.
- Two or more customers frequently betting against one another on even-money games.
- A customer in possession of large amounts of coinage or bills.
- A customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque.
- Chip cash out is same/similar to chip purchase.
- Requests for credit transfers to other casinos, gaming halls.
- Use of multiple names to purchase chips, tickets.
- Use of various credit cards to purchase chips, tickets.
- Use of personal cheques, bank cheques and traveller's cheques to purchase casino chips.
- A customer purchases chips and leaves the casino shortly after.
- Vouchers, tickets, cashed out prior to date of redemption.
- Frequent purchase of certificates of the game of chance performed in the casino, gaming hall.
- Unexplained income inconsistent with financial situation/customer profile.
- Rapid increase in frequency of transactions for regular account holder.
- Cash out of chips brought into the casino after a longer period and not at the time when they were won or bought (chips in possession of a third party).

4. **INDICATORS RELATING TO THE USE OF STRUCTURING/REFINING METHODS**

- Cheque issued to a family member of the person.
- Third party present for all transactions but does not participate in the game of chance.
- Transferring funds into third-party accounts.
- Transactions on casino accounts conducted by persons other than the account holder.
- Use of third parties to purchase gaming chips.
- Cash handed to third party after cash out.
- Use of third party to conduct betting.
- High volume of transactions within a short period.
- Exchanging large quantities of coins (from non-gaming proceeds) for paper currency.
- Frequent transactions just under reporting thresholds.
- Frequent 'buy in' and 'cash out' transactions just under reporting thresholds.
- Cash deposits/withdrawals just under reporting thresholds.
- Wire transfers/currency exchanges just under reporting thresholds.
- Requests for winnings in separate chip amounts under reporting threshold.
- A customer moving from table to table or room to room before the betting amounts reach the reporting threshold.
- Opening a casino account or purchasing casino chips with small denominations bills.
- Frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa.
- Inserting banknotes in gaming devices with no gaming activity, and pressing the 'cash out' button, which generates a TITO ticket, and redeeming the ticket at the cashier's desk.

5. **INDICATORS OF MONEY LAUNDERING USING WINNINGS**

- Frequent claims for winning jackpots.
- Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash.
- Customers watching/hanging around jackpot sites, progressive systems, but not participating in gambling.
- Multiple chip or ticket cash outs on the same day.
• Customers frequently claiming a high level of gaming machine pay outs.
• Purchasing and cashing out casino chips/tickets with no gaming activity.
• Requests for winnings in separate cash or chip amounts under reporting threshold.
• Frequent 'cash out' transactions without corresponding 'buy in' transactions.
• Cashing in winnings in a multiple combination of chips, tickets and cash.

6. INDICATORS OF MONEY LAUNDERING USING CURRENCY EXCHANGE

• Multiple currency exchanges.
• Dramatic increases in size and frequency of currency exchange transactions for regular account holders.
• Currency exchange for no reasonable purpose.
• Currency exchanges with low denomination bills for high denomination bills.
• Currency exchanges carried out by third parties.
• Large, one-off, or frequent currency exchanges for customers not known to the concessionaire.
• Currency exchanges with little or no gambling activity.
• Structured currency exchanges.

7. INDICATORS OF EMPLOYEE COMPLICITY

• Contact between players and the concessionaire's staff outside of the gaming floor.
• Supposed winnings do not correspond with recorded winnings.
• Increases in size and frequency of currency exchange transactions for regular casino account holders.
• Large amounts of cash from unexplained sources.
• Associations with multiple accounts under multiple names.
• Transactions on casino accounts conducted by persons other than the account holder.
• Cheque issued to a family member of the person.
• Multiple individuals sending funds to a single casino account holder.
• Third party present for all transactions but does not participate in the actual transaction.
• Use or third parties to undertake wire transfers.
• Use of agents to move funds across borders.
• Use of third parties to purchase gaming chips.
• Use of third party to conduct betting.
• Wire transfers from third parties in tax haven countries.
• Cash handed to third party after cash out.
• Reception staff allow a person to enter on the basis of a false identification document even if familiar with the person's true identity.
• Issuing false certificates to players of winning the jackpot.

8. INDICATORS OF MONEY LAUNDERING USING CREDIT/DEBIT CARDS

• Purchasing casino chips, tickets, using credit cards.
• Purchasing casino chips using credit cards.
• Purchasing and cashing out casino chips/plaques with no gaming activity.
• A customer purchases chips and leaves the casino or gaming hall shortly after.
• Use of stolen or fraudulently obtained credit cards.
• Use of multiple credit/debit cards to purchase casino chips.
• Use of third parties to purchase chips using credit/debit cards.
• Structuring of credit card transactions.
• Conducting debit card transactions up to the maximum limit.
• Customer due diligence challenges.
9. **INDICATORS OF MONEY LAUNDERING THROUGH JUNKET OPERATIONS**

- Players refuse to provide identification.
- Use of third parties to purchase chips.
- Junket chips redeemed without any gambling activity.
- Source of funds for buy-in not disclosed.
- Source of funds for buy-in indirectly from companies.
- Junket agents issuing cheques to casinos competitive with those with which the contract has been signed.
- Junket agents transferring funds to players with no proof of winnings.
- Player frequently requesting cheques from junket operators below the reporting threshold.

**Annex 3 – LIST OF INDICATORS FOR DETECTING SUSPICIOUS TRANSACTIONS APPLICABLE TO OPERATORS AND CONCESSIONAIRES OFFERING GAMES OF CHANCE THROUGH THE INTERNET OR OTHER TELECOMMUNICATION MEANS**

A list of indicators is based on two principles: knowledge about the customer and knowledge about the customer's business operations. Knowledge about the customer provides the basis for establishing whether there are grounds for a suspicion of money laundering under Article 245 of the Penal Code (KZ-1). There are grounds for suspicion in respect of any transaction that is not in line with the customer's ordinary course of transactions when participating in games of chance. When dealing with an unknown customer, indicators that do not relate to knowledge about the customer should be taken into account.

When establishing whether there are grounds for a suspicion of money laundering in respect of transactions carried out by individual customers, the indicators should be examined individually or jointly (if there are several indicators present). If only one indicator pointing to a suspicious transaction is present, it may be sufficient to submit data to the Office in some cases, while in other instances this would only be a warning that a transaction and a related customer need to be carefully examined with a view to uncovering other indicators.

Persons under obligation must prepare the indicators for detecting suspicious transactions in accordance with the first paragraph of Article 51 of the APMLFT.

1. **INDICATORS RELATING TO A CUSTOMER**

- A customer is unwilling to produce personal identification documents when requested by the authorised persons or produces for inspection personal documents for which a suspicion exists that they are false, or the documents do not belong to the customer.
- A customer refuses to open a casino account when learning of identification obligation.
- A customer exhibits unusual behaviour (obviously tense, nervous, etc.) when opening the account.
- In the course of establishing a business relationship, it is found that a customer is ‘known’ to have a criminal past (notifications by the Office or media).
- A customer appears to be trying to avoid identification or states false data.
- A customer offers material or non-material benefit to avoid identification.
- A customer is accompanied by suspicious people.
- A customer comes from a country appearing on a list of countries that, according to the information provided by international organisations and associations (FATF, EU, Council of Europe) fail to observe standards in the field of preventing and detecting money laundering or are known for producing or trafficking in drugs.
2. **INDICATORS RELATING TO A TRANSACTION**

- A player registers in the Internet casino with multiple accounts open under multiple names.
- A player conducts large casino account transactions.
- A player conducts an unusually large number of casino account transactions in a short period of time.
- A player makes credit on the casino account mainly or solely with deposits, but does not participate in any online game.
- A player gradually withdraws from his/her casino account funds that were mainly created with deposits.
- A player deposits large amounts into the casino account or into several casino accounts.

**Annex 4 – INDICATORS FOR DETECTING SUSPICIOUS TRANSACTIONS REGARDING SPORTS BETTING OPERATORS**

A list of indicators is based on two principles: knowledge about the customer and knowledge about the customer's business operations. Knowledge about the customer provides the basis for establishing whether there are grounds for a suspicion of money laundering under Article 245 of the Penal Code (KZ-1). There are grounds for suspicion in respect of any transaction that is not in line with the customer's ordinary course of transactions when participating in games of chance. When dealing with an unknown customer, indicators that do not relate to knowledge about the customer should be taken into account.

When establishing whether there are grounds for a suspicion of money laundering in respect of transactions carried out by individual customers, the indicators should be examined individually or jointly (if they are present). If only one indicator pointing to a suspicious transaction is present, it may be sufficient to submit data to the Office in some cases, while in other instances this would only be a warning that a transaction and a related customer need to be carefully examined with a view to uncovering other indicators.

Persons under obligation must prepare the indicators for detecting suspicious transactions in accordance with the first paragraph of Article 51 of the APMLFT.

1. **INDICATORS RELATING TO A CUSTOMER**

- A customer is unwilling to produce personal identification documents when requested by the authorised persons or produces for inspection personal documents for which a suspicion exists that they are false, or the documents do not belong to the customer.
- A customer appears to be trying to avoid identification or states false data.
- A customer offers material or non-material benefit to avoid identification.
- A customer cancels the transaction when learning of identification obligation.
- In the course of transaction, a customer exhibits unusual behaviour (obviously tense, nervous, etc.).
- Upon the arrival of the customer, the authorised person establishes that the customer is 'known' as a person with criminal record (notifications by the Office or media).
- A customer encourages the authorised person that the amount which is to be paid-out be broken down to smaller amounts to avoid identification, or to state false data about the customer on the identification form.
- A customer is accompanied by suspicious people.
- A customer comes from a country appearing on a list of countries that, according to the information provided by international organisations and associations (FATF, EU, Council of Europe), fail to observe standards in the field of preventing and detecting money laundering or are known for producing or trafficking in drugs.

2. **INDICATORS RELATING TO A TRANSACTION**

- A customer requires the pay out of winnings on the basis of a large number of winning betting slips, or the pay-out amount based on winning betting slips exceeds EUR 15 000.
- Rapid increase in the volume of transactions by a 'known customer', increase in the number of winning betting slips or deposits made in a shorter period of time.
• The spending/betting pattern of a 'known customer' changes noticeably.
• Simultaneous transactions conducted by several persons, which are clearly linked in order to break the total pay-out amount into smaller amounts with a view to avoiding identification.
• A customer's purchases, in a short period of time, a large volume of betting slips in smaller amounts for the obvious reason of avoiding identification.
• The transactions for the player are made by a third person.

3. INDICATORS RELATING TO EMPLOYEES WITH THE SPORTS BETTING OPERATORS AND AUTHORISED DEALERS

• Suspicious behaviour or operation (e.g. extravagance, reluctance to go to vacations, linking of personal and business relations with the customers).
• An employee avoids reporting a customer or a transaction in respect of which there are grounds to suspect money laundering despite being aware of the facts in support of money laundering.
• A deliberate violation of internal instructions, procedures and rules on money laundering by the employees and authorised dealers.
• Employees or authorised dealers avoid reporting to the authorised person for money laundering prevention.

Annex 5 – Reporting Questionnaire on transactions or customers giving rise to a suspicion of money laundering or terrorist financing (Questionnaire II),

REPORTING QUESTIONNAIRE ON TRANSACTIONS OR CUSTOMERS IN RESPECT OF WHICH THERE ARE GROUNDS FOR SUSPICION OF MONEY LAUNDERING OR TERRORIST FINANCING (QUESTIONNAIRE II)

A. TRANSACTION DATA

1. Transaction: a. □ has been carried out b. □ has not been carried out yet

2. Date and time of the transaction (DDMMYYYY HH:MM):

3. Transaction execution method:
   a. □ receipt
   b. □ delivery
   c. □ currency exchange
   e. other (specify):

4. Purpose of transaction:

5. Amount:

6. Currency:

7. Amount:

8. Currency:

9. Amount in EUR:
### B. NATURAL PERSON REQUESTING OR CARRYING OUT THE TRANSACTION

10. Transaction is carried out by:  
   a. □ one person  
   b. □ two or more persons (see appendix to the questionnaire)

11. Last name:  
12. First name:

13. Permanent or temporary place of residence:

14. Date of birth (DDMMYYYY)):  
15. Place of birth:  
16. Tax number:

17. Documents to verify identity:  
   a. □ identity card  
   b. □ passport  
   c. □ driving licence  
   d. □ other (specify):

18. Document no.:  
19. Issued by:

20. Person carries out the transaction:  
   a. □ in his/her own name  
   b. □ as an authorised person

21. The person:  
   a. □ is employed by the customer for whom the transaction is carried out.  
   b. □ is not employed by the customer for whom the transaction is carried out.

### C. CUSTOMER FOR WHOM THE TRANSACTION IS CARRIED OUT

22. Transaction is carried out in the name or on behalf of:  
   a. □ one customer  
   b. □ two or more customers (see appendix to the questionnaire)

23. Customer is:  
   a. □ legal entity  
   b. □ natural person  
   c. □ society  
   d. □ sole proprietor  
   e. □ other (specify):

If the customer is a legal entity, society, sole proprietor or other person:

24. Company name:  
25. Registered office:

If the customer is a legal entity, society, sole proprietor or other person:

24. Company name:  
25. Registered office:  
26. Registration no.:

If the customer is a natural person:

27. Last name:  
28. First name:

29. Permanent or temporary place of residence:

30. Date of birth (DDMMYYYY)):  
31. Place of birth:  
32. Tax number:

33. Documents to verify identity:  
   a. □ identity card  
   b. □ passport  
   c. □ driving licence  
   d. □ other (specify):

34. Document no.:  
35. Issued by:
### D. CUSTOMER TO WHOM THE TRANSACTION IS DIRECTED (RECIPIENT)

<table>
<thead>
<tr>
<th>36. Transaction is directed to:</th>
<th>37. Recipient is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. □ one recipient</td>
<td>a. □ legal entity</td>
</tr>
<tr>
<td>b. □ two or more recipients (see appendix to questionnaire)</td>
<td>b. □ natural person</td>
</tr>
<tr>
<td></td>
<td>c. □ society</td>
</tr>
<tr>
<td></td>
<td>d. □ sole proprietor</td>
</tr>
<tr>
<td></td>
<td>e. □ other (specify):</td>
</tr>
</tbody>
</table>

If the recipient is a legal entity, society, sole proprietor or other person:

<table>
<thead>
<tr>
<th>38. Company name:</th>
<th>39. Registered office:</th>
</tr>
</thead>
</table>

If the recipient is a natural person:

<table>
<thead>
<tr>
<th>40. Last name:</th>
<th>41. First name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>42. Place of residence:</td>
<td></td>
</tr>
</tbody>
</table>

### E. SENDER

Organisational unit where the transaction was requested or carried out:

<table>
<thead>
<tr>
<th>43. Name:</th>
<th>44. Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>45. Registration no.:</td>
<td></td>
</tr>
</tbody>
</table>

Person who identified the customer and verified the customer’s identity:

<table>
<thead>
<tr>
<th>46. Last name:</th>
<th>47. First name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>48. Signature:</td>
<td></td>
</tr>
</tbody>
</table>

Organisation referred to in Article 4 of the APMLFT:

<table>
<thead>
<tr>
<th>49. Name:</th>
<th>50. Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>51. Registration no.:</td>
<td></td>
</tr>
</tbody>
</table>

Organisation’s authorised person, or his/her deputy, as referred to in Article 4 of the APMLFT:

<table>
<thead>
<tr>
<th>52. Last name:</th>
<th>53. First name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>54. Date:</td>
<td>55. Signature:</td>
</tr>
</tbody>
</table>

56. Information has already been transmitted (DDMMYYYY HH:MM):

a. □ by telephone
a. □ by fax
**F. DATA PROVIDING GROUNDS FOR SUSPICION**

57. The person or transaction gives grounds to suspect:  
   a. □ money laundering  
   b. □ terrorist financing

58. Date the account was opened or the business relationship established (DDMMYYYY):

59. The reason and/or purpose and the intended nature of the business relationship (opening of account or other business relationship) and information on the customer's activities (specify):

60. Information about the source of the assets or property that are the subject of the transaction (specify):

61. Grounds to suspect money laundering/terrorist financing:

**G. DATA ON THE CUSTOMER'S BENEFICIAL OWNER**

62. For companies:  
   a. □ The person owns _________% of the interest, shares or voting or other rights, on the basis of which he/she participates in the management of the company.  
   b. □ The person's equity participation in the company amounts to _________%.  
   c. □ The person has the controlling position in the management of the company's assets.  
   d. □ The person indirectly provides funds to the company and, on these grounds, has the opportunity to exercise control of or influence the legal entity's decisions concerning the funding and business operations.

For other legal entities, such as institutions and similar foreign law entities:  
   a. □ The person is the ____% beneficiary of the proceeds of the property under management.  
   b. □ The establishment and operation of a legal entity or similar foreign law entity is in the person's interest.  
   c. □ The person exercises direct or indirect control over _________25% of the property of a legal entity or similar foreign law entity.

63. The natural person is:  
   a. □ the owner or manager of the customer (legal entity or foreign law entity)  
   b. □ the owner or manager of another legal entity that owns the customer.

64. Last name:  
65. First name:

66. Permanent or temporary place of residence:

67. Date of birth (DDMMYYYY):  
68. Place of birth:
APPENDIX TO QUESTIONNAIRE

A. TRANSACTION DATA

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

B. NATURAL PERSON REQUESTING OR CARRYING OUT THE TRANSACTION

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Last name:</td>
<td>12. First name:</td>
</tr>
<tr>
<td>13. Permanent or temporary place of residence:</td>
<td></td>
</tr>
<tr>
<td>14. Date of birth (DDMMYYYY)):</td>
<td>15. Place of birth:</td>
</tr>
<tr>
<td>a. □ identity card</td>
<td></td>
</tr>
<tr>
<td>b. □ passport</td>
<td></td>
</tr>
<tr>
<td>c. □ driving licence</td>
<td></td>
</tr>
<tr>
<td>d. □ other (specify):</td>
<td></td>
</tr>
<tr>
<td>19. Issued by:</td>
<td></td>
</tr>
</tbody>
</table>

C. CUSTOMER FOR WHOM THE TRANSACTION IS CARRIED OUT

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23. Customer is:</td>
<td></td>
</tr>
<tr>
<td>a. □ legal entity</td>
<td></td>
</tr>
<tr>
<td>b. □ natural person</td>
<td></td>
</tr>
<tr>
<td>c. □ society</td>
<td></td>
</tr>
<tr>
<td>d. □ sole proprietor</td>
<td></td>
</tr>
<tr>
<td>e. □ other (specify):</td>
<td></td>
</tr>
</tbody>
</table>
If the customer is a legal entity, society, sole proprietor or other person:

<table>
<thead>
<tr>
<th>24. Company name:</th>
<th>25. Registered office:</th>
</tr>
</thead>
</table>

26. Registration no.:

If the customer is a natural person:

<table>
<thead>
<tr>
<th>27. Last name:</th>
<th>28. First name:</th>
</tr>
</thead>
</table>

29. Permanent or temporary place of residence:

<table>
<thead>
<tr>
<th>30. Date of birth (DDMMYYYY):</th>
<th>31. Place of birth:</th>
<th>32. Tax number:</th>
</tr>
</thead>
</table>

33. Documents to verify identity:
   a. □ identity card
   b. □ passport
   c. □ driving licence
   d. □ other (specify):

34. Document no.:

35. Issued by:

D. CUSTOMER TO WHOM THE TRANSACTION IS DIRECTED (RECIPIENT)

| 37. Recipient is: a. □ legal entity
   b. □ natural person
   c. □ society
   d. □ sole proprietor
   e. □ other (specify): |
|-----------------------|---------------------|

If the recipient is a legal entity, society, sole proprietor or other person:

<table>
<thead>
<tr>
<th>38. Company name:</th>
<th>39. Registered office:</th>
</tr>
</thead>
</table>

If the recipient is a natural person:

<table>
<thead>
<tr>
<th>40. Last name:</th>
<th>41. First name:</th>
</tr>
</thead>
</table>

42. Place of residence:

The method for completing the above reporting questionnaires is prescribed in the Instructions on the method for filling out the reporting questionnaires appended to the Rules on the method for reporting information to the Office of the Republic of Slovenia for Money Laundering Prevention (Ur. l. RS, no. 10/08) and is also available on the webpage of the Office http://www.uppd.gov.si/slov/zakonodaja/obrazci APMLFT.htm).
13. **SOURCES**


2. Prevention of Money Laundering and Terrorist Financing Act (Ur. l. RS, no. 60/07);
3. Gaming Act (Ur. l. RS, no. 134/03 – official consolidated text);
4. Rules on exercising internal control, authorised person, storage and protection of information, and management of records with respect to organisations, lawyers, law firms and notaries (Ur. l. RS, no. 10/08);
4. Rules laying down the conditions under which a person may be considered a customer who represents a low risk of being involved in money laundering or terrorist financing (Ur. l. RS, no. 10/08);

Further information is available on the following webpages:
