Izložu un azartspēļu uzraudzības inspekcija

APPROVED
By Order No 26 issued by the head of
the Lotteries and Gambling Supervisory Inspection
on 29 December 2023

Guidelines for Gambling and Lottery Operators on the Creation of Internal Control Systems for the Prevention of Money Laundering and Terrorism and Proliferation Financing

Introduction

[1] These Guidelines lay down the basic principles that shall apply to capital companies which hold a gambling and lotteries licence issued by the Lotteries and Gambling Supervisory Inspection (hereinafter referred to as the Inspection) and which shall create an internal control system in accordance with the requirements set out in the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (hereinafter referred to as the Law).

[2] The aim of these Guidelines is to assist gambling and lottery operators with the creation of an internal control system in order to prevent the use of gambling and lotteries in money laundering or terrorism and proliferation financing; to identify, assess and understand the risks of money laundering and terrorism and proliferation financing; to act on risk management, mitigation and prevention; to define criteria for the development of common procedures.

[3] The term “money” in “money laundering” refers to any “proceeds of crime” or “criminally acquired property”, i.e., anything that a person has acquired directly or indirectly as the result of a criminal offence, such as money from drug trafficking, theft or robbery. It also includes property or proceeds that a person derives from the sale of criminally acquired property or from the benefits of such property, for

example, using money earned in drug trafficking to buy cars or real estate, or gambling with money stolen from a bank.

[4] Money laundering is:

- the conversion of proceeds of crime into other valuables, change of their location or ownership while being aware that these funds are the proceeds of crime, and if such actions have been carried out for the purpose of concealing or disguising the illicit origin of funds or assisting another person who is involved in committing a criminal offence in the evasion of legal liability;
- the concealment or disguise of the true nature, origin, location, disposition, movement, ownership of the proceeds of crime, while being aware that these funds are the proceeds of crime;
- the acquisition, possession, use or disposal of the proceeds of crime of another person while being aware that these funds are the proceeds of crime.

[5] Money laundering is divided into three stages:

- Placement;
- Layering;
- Integration.

[5.1] Placement — cash or its equivalent acquired from a criminal offence (e.g. drug trafficking) is placed in the public financial system or is taken to another country. The aim of the money launderer is to avoid authorities and to convert the proceeds of crime into other assets.

[5.2] Layering is an attempt to conceal or disguise the source and ownership of the proceeds of crime through the creation of complex financial transaction layers that complicate the audit process and ensure anonymity. The purpose of layering is to separate the proceeds of crime from the criminal activities that generated them.

[5.3] Integration deals with the integration of the proceeds of crime into the economic and financial system and their alignment with other assets therein. The integration of “clean” money into the system grants it the appearance of legally acquired or earned proceeds.

[6] Money launderers can make use of gambling at each of these stages. Land-based

gambling operations are particularly vulnerable at the placement stage due to their widespread use of cash. Operators of on-line gambling can become victims of identity theft, which in turn can facilitate anonymous movement of the proceeds of crime.

[7] A peculiar feature of the lotteries and gambling sector is its connection with the "lifestyle" spending by criminals where the proceeds of crime are used to participate in gambling or lotteries as a leisure activity or as an intermediate stage for temporary storage of money, meaning that some stages of money laundering might be omitted.

I. Risk assessment

1. Money laundering and terrorism and proliferation financing (hereinafter 'MLTPF') risk assessment includes the identification, analysis and determination of MLTPF risks.

2. The first step towards the creation of an internal control system is the performance of a risk assessment of a gambling and lottery operator (hereinafter 'Operator'), providing for an efficient use and allocation of resources. The Operator shall provide adequate and sufficient resources to manage and mitigate its inherent risks.

3. In its risk assessment the Operator shall also take into account the risks identified by the European Commission in the European Union MLTPF Risk Assessment and the risks identified in the national MLTPF risk assessment report.

4. MLTPF risks are measured using several factors. The standard risk categories used by the Financial Action Task force (hereinafter 'FATF') in the gambling and lottery sector are as follows:
    4.1. Country or geographical risk;
    4.2. Customer risk;
    4.3. Transaction risk.

5. **The country or geographical risk** assesses the customer's country of origin, since certain countries or territories represent a higher MLTPF risk than others. In addition to information that is already available on high-risk third countries, attention should be paid to other information that can help to identify countries

or territories with increased risk, thus identifying customers from such countries or territories who may pose a higher risk. Operators can use information provided by non-governmental organizations to gain an insight into the level of corruption in that particular country. The level of corruption can be analysed by making use of data non-governmental organizations have collected here: https://www.transparency.org.

6. The country or geographical risk assessment looks at the country where the customer is a citizen, does business or resides in. On-line gambling and lottery operators have to pay additional attention to the country where the customer is located (the country from which the customer connects to their game account), taking into account the additional risks posed by cross-border activities.

7. **Customer risk.** On the basis of the criteria set, Operators should determine whether the customer in question presents an increased risk and what risk mitigation measures might be applied. Customer categories the activities of which may indicate an increased risk are:
    7.1. A politically exposed person (PEP);
    7.2. A family member of a PEP;
    7.3. A person closely related to a PEP;
    7.4. Customers whose economic or personal activity is linked to high-risk professions;
    7.5. Long-term customers who make significantly larger payments than they usually do;
    7.6. New customers who pay large amount of money;
    7.7. Irregular customers, such as gambling tourists;
    7.8. Customers with negative coverage in mass media.

8. The high level of spending (threshold) is set by the Operator on the basis of information they have on the customer, meaning that it may differ between Operators.

9. **Transaction risk**. Gambling and lottery operators should consider operational aspects (products, the distribution channels thereof, accounts, player account activities) that a customer can use to facilitate MLTPF. Operators should take into account that any transaction could involve proceeds of crime. Particular attention should be paid to the following potential transaction risks in the gambling and lottery sector:
    9.1. Cash transactions in which customers can make use of land-based

gambling operations in order to change the denomination of funds (money);

9.2. The deposit and storage of funds in an on-line gambling and lottery game account;

9.3. The use of player cards to store funds;

9.4. The exchange of TITO tickets, tokens after a short game or without a game taking place;

9.5. Changing bank accounts — a customer of on-line gambling or lotteries frequently changes their bank accounts without reason;

9.6. Identity fraud or purchasing of player accounts;

9.7. The use of money mules (buying TITO tickets, winning lottery tickets or betting rate coupons);

9.8. The use of a pre-paid card;

9.9. The use of a company card;

9.10. The transfer of money (prizes) to a bank account specified by the player in "land-based games";

9.11. When a player stops playing immediately after starting and demands the return of the bet;

9.12. Solid transactions showing signs of a suspicious transaction (red flags, typologies).

Operators may also use other risk factors to determine MLTPF transaction risks.

10. In order to determine the MLTPF risk to which an Operator is exposed, it shall be necessary to assess and determine the following:

10.1.1. The initial level of risk — the risk to which the Operator is exposed without applying risk management and mitigation measures;

10.1.2. The effectiveness of MLTPF risk management measures;

10.1.3. The residual risk — the risk to which the Operator is exposed after applying risk management measures.

11. The following formula shall be used to determine an Operator's inherent risk: *The initial risk — The effectiveness of MLTPF risk management measures = The residual risk*

12. When determining its initial inherent risk, the Operator shall assess the risk categories listed above (country and geographical risk, customer risk, transaction risk) as well as any additional risk indicators identified by the Operator.

13. When determining the effectiveness of its MLTPF risk management measures, the Operator shall assess the MLTPF risk measures it has applied in order to prevent MLTPF and to ensure that risk factors are being identified (such as IT systems used, policy and procedure requirements and the update thereof, quality assurance mechanisms, sufficiency and qualification of personnel, management awareness and engagement, timely implementation of audit recommendations, etc.). The Operator shall provide an assessment of every measure (e.g. adequate, inadequate, substantial improvement, minor improvement). Through the assessment of each individual measure, the Operator determines how effective the measures are as a whole.

14. The residual risk of the Operator is identified after the initial risk has been assessed and the most appropriate MLTPF risk management measures and their effectiveness have been taken into account. When calculating the residual risk according to the formula referred to in Paragraph 11, the initial risk has the highest weight because it cannot be reduced to zero regardless of how effectively the internal Control System (hereafter - ICS) operates.

15. Operators may apply risk matrices of varying detail when carrying out the risk assessment:

	MLTPF Threat				
H	M	M	MH	H	H
MH	M	M	MH	MH	H
M	ML	M	M	MH	MH
ML	ML	ML	M	M	M
L	L	ML	ML	M	M
	L	**ML**	**M**	**MH**	**H**

High (H)	Medium-High (MH)	Medium (M)	Medium-Low (ML)	Low (L)

	MLTPF Threat		
H	M	H	H
MH	L	M	H
L	L	L	M
	L	**ML**	**L**

High (H)	Medium (M)	Low (L)

16. The Operator decides which matrix to apply considering the size of its operation and its customer base. Operators with fewer customers can apply the simplified risk assessment matrix, whereas if a detailed risk breakdown is required, the risk assessment matrix featuring a more detailed risk breakdown can be used.

17. The Operator has an obligation to continuously identify, assess and manage newly discovered risks. The application of a risk assessment-based approach ensures a proportionate allocation of the Operator's resources and a more

efficient and effective use thereof.

18. The Law stipulates a regular review and update of the MLTPF risk assessment that is to be done at least once every three years. The reviewing and updating of the MLTPF risk assessment shall be more frequent when introducing new products, services or technologies.

II. Training of employees

19. The Operator shall draw up a training plan preventing of MLTPF for a period of not less than half a year, which shall be approved by the employee responsible for the fulfilment of the requirements of the Law from senior management.

20. The development of MLTPF prevention training plan should consider:
    20.1. Results of the European Union supranational risk assessment;
    20.2. Results of the risk assessment report of the MLTPF of Latvia;
    20.3. Results of the risk assessment of the Operator’s MLTPF.

21. The Operator shall determine the employees who are directly responsible for the preparation, management and organisation of MLTPF prevention training materials.

22. The Operator determines the categories of employee positions and the scope of their responsibility to prevent MLTPF.

23. The Operator shall determine the procedures and form (remote or face-to-face or hybrid) of employees training and the type of knowledge test.

24. The Operator shall retain all information regarding the training performed for the employee until the end of the employee's employment relationship, including:
    24.1. identifying data and position of the employee;
    24.2. confirmation regarding the participation of the employee in training;
    24.3. the date, duration and subject of the training;
    24.4. training materials;
    24.5. the results of the knowledge test.

25. The Operator shall determine the regularity and duration of training, ensuring the level of knowledge of employees according to their area of responsibility in preventing MLTPF.

26. The Operator shall, at least once a year, provide a theme in training - regarding the signs and detection of suspicious transactions.

27. The Operator shall determine the criteria when evaluating the results of the knowledge tests of employees (thresholds for the positive and negative results).

28. The Operator shall provide additional training for an employee if:
    28.1. the assessment of the result of the knowledge test is negative;
    28.2. detected deficiencies or violations in preventing of MLTPF in the field of responsibility of the employee.

29. The Operator provides training of new staff in the MLTPF prevention before performing their duties independently.

30. The Operator shall provide training additional to the plan if amendments to the sectoral regulatory framework are taking place, which is the basis for updating the ICS and applies to the area of responsibility of the employee or if the supervisory and control authority detects an infringement.

III. Establishment of Customer Relations and Transaction Characteristics

31. The Operator shall follow the “know your customer” principle before deciding whether to start a business relationship, continue the business relationship, terminate the business relationship. An effective application of the “know your customer” principle involves applying all stages of customer due diligence:
    31.1. Identification of the customer;
    31.2. Evaluation of the customer’s financial activity;
    31.3. Determination of the customer risk level.

32. Effective identification and management of MLTPF risks depends on the Operator’s ability to obtain comprehensive information about its customer, the

quality of policies and procedures developed, and the professional performance of its employees.

33. As part of customer due diligence, the Operator shall request and obtain from the customer any supporting information or documents and make sure that the information or documents are relevant to the particular purpose of customer due diligence (e.g. they justify the origin of the funds, provide an idea about the customer's education and experience, justify a specific transaction, etc.). The amount of information and documents obtained during customer due diligence must be reasonable and proportionate to the risks posed by the customer or their transactions.

34. The Operator is obliged to provide the capacity necessary to collect and analyse information on customer activities in all of the Operator's gambling or lottery sites (land-based or on-line) in order to gain a comprehensive picture of the risks posed by a particular customer activity.

35. Customer transaction and relationship management requires a continuous and targeted communication between personnel and the customer, which will contribute to the implementation of the Operator's procedures in the field of MLTPF and compliance with the obligations stipulated in the MLTPF Law.

36. The Operator’s relationship with the customer, as seen through the lens of PMLTPF, can be divided into three parts:
    36.1. The start of the business relationship with the customer, including verification of the customer's identity;
    36.2. The monitoring of customer transactions (transactions, money flows, etc.);
    36.3. The termination of transaction relations with the customer.

37. At all stages, the Operator shall check for signs of a suspicious transaction and, where necessary, report any suspicious activities to the relevant authority.

38. **Starting Business Relationships**. Transaction relationship is the relationship between the Operator and its customer that originates when the Operator performs an economic or professional activity and that is expected to have an

element of duration at the time when the contact is established[1]. In the area of gambling and lottery operation, a distinction exists between business relationships and occasional transaction relationships without an element of duration due to the historical model of gambling and lottery operations. For this reason, there are special conditions for launching customer due diligence laid down in the Law that apply to Operators[2].

39. The obligation to conduct customer research in land-based gambling and lotteries arises from:
    39.1. when executing a transaction with the customer for the sum equal to or exceeding EUR 2,000, including if the customer wins, purchases means for participation in the game or lottery tickets, or exchanges foreign currency for this purpose, regardless of whether such transaction is executed as a single operation or as several mutually linked operations:
        39.1.1. A customer purchases means for participation in the game (cash deposit in a gaming machine, tokens, lottery tickets, TITO tickets, etc.) at a land-based gambling operation and lottery ticket point-of-sale or exchanges foreign currency for this purpose in a single operation or several mutually linked operations for a total amount of at least EUR 2,000;
        39.1.2. A customer makes pay-outs (including money from a gaming machine, token exchange, TITO ticket pay-outs, etc.) at a land-based gambling operation in a single operation or several mutually linked operations for a total amount of at least EUR 2,000.

40. The obligation to conduct customer due diligence in interactive gambling and lotteries arises prior to the establishment of a business relationship.

41. A business relationship begins if:
    41.1. The customer has registered for interactive gambling and lottery;
    41.2. The customer becomes a member of the Operator's loyalty program (for example, acquires a loyalty card).

42. In interactive gambling, the establishment of a business relationship closes when **a gambling service becomes available to the customer**.

---

[1] Section 1(3) of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing (LPMLTPF)

[2] Section 11, Paragraph one, Clause 4 of LPMLTPF

43. When starting the business relationship, the Operator shall assess:
    43.1. The initial information regarding the customer in order to identify the potential risk they pose;
    43.2. The necessity to apply appropriate customer due diligence measures.

    In case it is discovered that the customer is trying to use the Operator in order to launder proceeds of crime or there are reasonable doubts of such activity, the Operator shall report the suspicious transaction.

44. **Customer Monitoring.** If the customer meets high-risk criteria and poses an increased MLTPF risk, the Operator shall closely monitor the player's behaviour and consider the need for enhanced customer due diligence. The Operator shall define and strengthen the ICS conditions for the termination of business relationships with a customer in cases where the MLTFP risk is too high.

45. The Operators shall ensure that the customer monitoring policies and procedures, that are applicable to all products and platforms (land-based and on-line) they offer, are sufficient to manage risks to which the Operator is exposed. Monitoring of deposits and pay-outs and the scope of control measures shall be provided for in the customer monitoring policies and procedures. Land-based gambling Operators shall provide practical systems or solutions for the effective monitoring and determination of the amounts a customer spends in gaming machines, on bets and betting sites, bingo halls and casinos.

46. In order for the Operator to be able to effectively monitor the transactions performed by customers, it is necessary to collect the minimum initial information regarding the customer: the customer's identity, verification that they are not on any lists of national or international sanctions, and monitoring of the customer's transaction to check for the threshold that triggers customer due diligence.

47. The transactions of all of Operator's customers shall be subject to monitoring, not only for the purposes of checking for the EUR 2,000 customer due diligence threshold but also to enable the identification of suspicious transactions. Monitoring of customer transactions shall be carried out using a risk-based approach. High-risk customers shall be subjected to heightened monitoring and, where appropriate, enhanced customer due diligence.

48. At first suspicion of money laundering and the financing of terrorism and proliferation that is linked to a certain type of gambling or lottery operation (e.g., gaming machines), the Operator shall monitor and analyse the customer's behaviour and actions in other forms of gambling or lottery operations (e.g., gaming tables or on-line).

49. **Termination of the Business Relationship with a Customer.** The Operators shall decide on whether to terminate the business relationship or to refrain from executing transactions with the customer in the following cases:
    49.1. The Operator is aware that the customer is trying to use its services and products to legalize proceeds of crime or to finance terrorism and proliferation;
    49.2. The customer's gambling habits and information regarding the customer available to the Operator gives rise to reasonable suspicion of MLTPF activity;
    49.3. The Operator has reasonable grounds to suspect that funds involved in the transaction have originated from a criminal offence or are of unknown origin and the customer is unable to justify the origins of the funds;
    49.4. The customer does not provide the Operator with all required true information necessary for customer due diligence and the determination of customer risk level;
    49.5. The Operator believes that the MLTPF risk is too high;
    49.6. The customer uses the identity of another person.

IV. Customer Due Diligence

36. In accordance with the Law the Operator is obliged to carry out customer due diligence. The purpose of customer due diligence is to obtain information and sufficient documentation at the early stage of a business relationship with a customer, enabling the Operator to reduce the risk of being involved in MLTPF activity.

37. The Operator shall use a risk assessment-based approach in its customer due diligence and apply due diligence measures to an extent that is commensurate with the customer risk assessment. While gathering of information, the Operator shall obtain information on the origin of the customer's funds and the origin of wealth characterising the financial situation of the customer.

38. The extent of the customer due diligence depends on the degree of risk posed by the customer, the customer's country of origin, the customer's economic and personal activities, the way services are delivered, transactions carried out, the duration of the business relationship and its regularity.

39. During customer due diligence, the Operator shall establish the customer risk and assess the transactions (deposits and pay-outs) performed by the customer and the services (types of games) used by the customer, for instance — a significant amount (as defined by the Operator, considering the results of customer due diligence) is transferred by a new customer to their interactive gambling game account or used to purchase means for participation in the game in land-based gambling operations (casino tokens, betting rates, deposits in a gaming machine). In such a case, the Operator shall, on the basis of a risk assessment, obtain information attesting the origin of the funds.

40. The services provided by the Operator are the operation of gambling or lotteries, thus it is assumed that the customer enters a business relationship in order to access gambling or lottery services. The Operator shall provide in its procedures for situations where the conduct of the customer gives rise to reasonable suspicion regarding the purpose of the business relationship and how to identify such a situation.

41. The Operator shall document all the information obtained during the customer due diligence and ensure that it is revised according to the risk level and at least once every five years.

42. The risk-based approach ensures that the level and amount of information gathered and verified increases proportionally with the increase in the exposure to risk in business relationship with the customer. The Operator shall set out in its policies the levels of customer risk and the criteria for determining them, the customer due diligence measures and the extent to which these apply to customers of a particular risk level. There will be less information about a lower risk customer than a higher risk customer. PEP, PEP family members, PEP-linked persons contribute to a higher risk and demand more due diligence resources. The Operator is prohibited from establishing a business relationship and from conducting occasional transactions with persons against which international or national sanctions have been imposed.

43. The way in which information required for customer due diligence is obtained may differ. On the basis of a risk assessment, it may take the form of a customer questionnaire covering a variety of issues aimed at obtaining reasonable and sufficient information in order to identify customer risk, or information may be collected from public and reliable sources, such as commercial databases. Such requirements shall be laid down in the Operator's policies and procedures, also specifying the sources that the Operator considers to be reliable. For example, information on companies registered in the Republic of Latvia can be obtained from the Enterprise Register, including commercial databases that maintain information in the Enterprise Register, while information on foreign residents can be obtained from the database of the Enterprise Register of the relevant state, such as:

European Union Member States, Iceland, Liechtenstein, Norway	https://e-justice.europa.eu/content_find_a_company-489-en.do?clang=en
Estonia	https://www.inforegister.ee
Lithuania	https://rekvizitai.vz.lt/en/
Great Britain	https://beta.companieshouse.gov.uk/
Ireland	http://www.cro.ie/ena/online-services-company-search.aspx
Cyprus	https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchForm.aspx?sc=0
The Czech Republic	https://or.justice.cz/ias/ui/rejstrik
The Russian Federation	https://egrul.nalog.ru/#
Ukraine	https://usr.minjust.gov.ua/ua/freesearch

44. Types of customer due diligence: **standard and enhanced customer due diligence.** Standard due diligence differs from enhanced customer due diligence in that standard due diligence features no risk-increasing circumstances and only a minimum amount of information is verified, and the information required for customer due diligence is of a different level of detail.

45. A standard customer due diligence shall be carried out in cases where the customer has a low MLTPF risk (the customer's expenses are reasonable, consistent with the information the Operator has obtained on the person and commensurate with their income) and the customer does not trigger any conditions for performing an enhanced customer due diligence, no risk-increasing factors affecting the customer's risk profile have been identified, the

monitoring of transactions does not reveal any signs of potentially suspicious transactions or activities that are atypical for the customer. The Operator shall ensure that the key information necessary for customer due diligence is updated at least once every five years. The level of detail of the information to be obtained in the case of standard due diligence is lower than that of information obtained during an enhanced due diligence. For example, when obtaining information on a customer's economic or personal activities, it is sufficient to ascertain the customer's occupation, employer, profession.

46. The Operator shall ensure that it is able to justify how the information or documents obtained pertain to the information required for customer due diligence. The information and documents obtained during customer due diligence shall provide assurance that the Operator is aware of customer risks and takes appropriate measures to manage those risks.

47. The Operator may adopt procedures aimed at reducing the level of customer risk by defining the amount of information that has to be verified in order to assure its credibility and the effectiveness of the monitoring measures. The responsible person shall coordinate the threshold for mitigating customer risk with a representative of senior management.

48. The Operator shall identify indicators that signify changes in the customer risk level during business relationship monitoring. The Operator shall ensure that the customer risk level is updated in accordance with the latest information on the customer. For example, when a customer, who was initially rated as a low-risk customer, reaches a certain amount of transactions the customer is classified as high-risk and subjected to relevant customer due diligence measures.

49. The Operator shall carry out an enhanced due diligence of customers who were initially or eventually rated as high-risk customers. Enhanced customer due diligence consists of the following actions:
    49.1. To use additional due diligence measures;
    49.2. To obtain and assess additional information regarding the customer;
    49.3. To assess the compliance of the transactions executed by the customer with the economic activity indicated;
    49.4. To assess the origin of the funds and wealth of the customer;
    49.5. To ascertain (verify) the veracity of the information obtained;

49.6. To receive a consent from the senior management of the Operator for the commencement or continuation of a business relationship;

49.7. To perform in-depth supervision of a business relationship[3];

Verification of the source of income is mandatory for PEP, PEP family members, persons closely associated to a PEP and in case of business relationships with customers coming from high-risk third countries.

50. Customer Due Diligence Requirements. The Operators shall carry out customer due diligence in the following cases:

50.1. When executing a transaction with the customer in a land-based gambling operation and lottery ticket point-of-sale for the sum equal to or exceeding EUR 2,000, including if the customer wins, purchases means for participation in the game or lottery tickets, or exchanges foreign currency for this purpose, regardless of whether such transaction is executed as a single operation or as several mutually linked operations;

50.2. The customer has registered for interactive gambling or lottery;

50.3. The customer becomes a member of the Operator's loyalty program (for example, acquires a loyalty card);

50.4. If there are suspicions of money laundering, terrorism and proliferation financing or an attempt of such actions;

50.5. If there is information on mass media regarding a possible criminal offence or possible corruption.

51. The Operator shall carry out customer due diligence of existing customers in the following cases:

51.1. During the application of a risk-based approach;

51.2. If the previously gathered customer due diligence data of an existing customer changes in a way that may influence the risk assessment of this customer.

52. When deciding whether the use of customer due diligence measures for existing customers is appropriate the Operator shall also take into account following:

52.1. Any indication that the identity of the customer has

[3] Section 22, Paragraph one of the LPMLTPF

changed;

52.2. Any transactions that appear unusual considering the Operator's knowledge of the customer (e.g. untypically large deposits or bets, number of bets, gambling at hours unusual for the customer, etc.);

52.3. Other circumstances that could affect the Operator's assessment of the customer risk level.

53. **Customer due diligence measures.** Customer due diligence measures are:

53.1. The initial identification of the customer and the verification of acquired identification data if the Operator has not previously identified the customer;

53.2. The further verification of the customer's identity using data obtained during the initial identification of the customer;

53.3. The monitoring of business relationships;

53.4. The storage, regular assessment and updating of documents, personal data and information regarding customers obtained over the course of customer due diligence.

54. The verification of documents or information obtained during customer due diligence must be based on data obtained from a reliable source, that is independent from the person under examination. Documents issued or made available by an official authority shall be considered to be independent from the person, even if these have been provided or made available to the Operator by the person under examination.

55. The Operator shall verify that the personal identification document is valid using available public registers of the respective country (e.g., the Register of Invalid Documents). One of the reasons why there is an obligation to check personal identification documents against the Register of Invalid Documents is to make sure the person indicated in the submitted document is alive and that services provided by the Operator are not being used by a third party. During this verification, the Operator shall compare and verify the number of the personal identification document submitted by the customer and make sure that the document has not been stolen, lost, destroyed, annulled, is not being used by a third party, has not expired, etc.

56. For a customer with a personal identification document issued abroad, the Operator can use national databases of the respective country if any are

available (e.g. in Russia – http://services.fms.gov.ru/info-service.htm?sid=2000 , in Ukraine – https://nd.dmsu.gov.ua/). When verifying the authenticity of the personal identification document presented by the customer, the Operator may refer to publicly available information (e.g. http://www.consilium.europa.eu/prado/en/search-by-document-country.html) or commercial databases offering information on the types of personal identification documents in different countries.

57. The Operator has an obligation to update customer personal identification document data of all of the Operator's customers. The update frequency and the type and amount of information to be obtained depends on the MLTPF risk assessment.

58. The information can be considered to be "obtained from a reliable source, that is independent from the person whose identity is being verified" if:
    58.1. it is obtained during a remote identification procedure, including by secure electronic signature, video identification and other technological solutions[4]; and
    58.2. this process is protected from fraud and abuse and can provide reasonable assurance that the person claiming a certain identity is actually the person with that identity.

59. These requirements apply to both land-based and on-line Operators.

60. An Operator who operates different types of gambling or lotteries does not need to repeat customer due diligence if the customer visits another gambling facility of the same Operator, provided that access is given to the customer due diligence records held by the Operator. The Operator shall ensure that all its gambling venues have the necessary facilities for processing information and updating records. The ICS shall contain detailed information on how it will be managed by the Operator.

61. When determining the extent and frequency of customer due diligence, the Operator shall also take into account the following indicators affecting the risk:
    61.1. The purpose of the business relationship;

[4] Cabinet Regulation No. 392 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer"

61.2. The amount deposited by the customer or the amount of transactions executed by the customer;
61.3. The duration of the business relationship;
61.4. The regularity of transactions.

62. During a business relationship with the customer in the gambling and lottery sector the Operator considers participation in gambling and lottery activities to be the purpose of such relationship, so whenever there are indications that the purpose of a transaction is not gambling or lottery, additional checks shall be carried out and, if necessary, the transaction shall be terminated or refrained from and/or the case shall be reported to the FIU.

63. The Operator shall gain assurance that information sources used to conduct customer due diligence are reliable and sufficient for risk mitigation. For example, information from a publicly available source, such as the press, can be used for customer due diligence. The Operator shall however not rely too much on only one source of information and shall make use of other databases and information sources when performing customer due diligence.

64. The Operators have to be able to demonstrate to control and supervisory authorities that the amount of customer due diligence activities is adequate and sufficiently reliable, taking into account MLTPF risks, including risks:
64.1. identified in the Operator's risk assessment;
64.2. indicated in the MLTPF risk assessment summary report.

65. **Timing of the Customer Risk Assessment.** The Operator shall only proceed with the business relationship with the customer after the completion of the risk assessment and the establishment of the customer risk level.

66. **Transaction Monitoring.** The Operators shall provide for constant monitoring of the business relationship after it has been established, including:
66.1. the monitoring of transactions over the entire course of the relationship in order to verify that transactions correspond to the information the Operator has at its disposal regarding the customer, the customer's personal or economic activity and customer's risk profile;

66.2. the monitoring of the customer's actions and transactions in order to check for signs of suspicious transactions.

67. The Operator shall take note of customers and their gambling habits, taking into account the information already known about the customer and, where appropriate, collects and stores additional information, for example, on the origin of the customer's funds.

68. **Enhanced Customer Due Diligence and Transaction Monitoring.** The Operator shall apply enhanced customer due diligence, in addition to the customer due diligence measures set out in the Law[5], in order to manage and mitigate customer-related MLTPF risks that can occur in the following cases:

68.1. The customer is a resident of a high-risk third country or the customer's country of origin is a high-risk third country;

68.2. Upon establishing and maintaining a business relationship or executing an occasional transaction with a customer who has not participated in the onsite identification procedure in person, except in the case when the following conditions are fulfilled:

68.2..1. The Operator ensures adequate measures for mitigating MLTPF risks, including drafting of policies and procedures and carrying out of staff training on the performance of remote identification;

68.2..2. The customer identification, by means of technological solutions including video identification or secure electronic signature, or other technological solutions, is being performed to the extent and in accordance with the procedures stipulated by the Cabinet[6].

68.3. Upon establishing and maintaining a business relationship or executing an occasional transaction with a customer — PEP, a family member of a PEP, or a person closely associated to a PEP;

[5] Section 11^1 of LPMLTPF

[6] Cabinet Regulation No. 392 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer"

68.4. The customer executes untypically large transactions, complex transactions, seemingly mutually linked transactions or transactions which do not seem to have an economic purpose;

68.5. In other cases, upon establishing and maintaining a business relationship or executing an occasional transaction with a customer if there is an increased MLTPF risk.

69. When carrying out transactions with customers from a high-risk third country the Operator shall take the following enhanced customer due diligence measures:

69.1. Obtain and assess additional information regarding the customer, as well as ascertain the veracity of the additional information obtained;

69.2. Obtain and assess additional information regarding the intended nature of the business relationship;

69.3. Obtain and assess information regarding the origin of the funds and wealth of the customer;

69.4. Obtain and assess information regarding the justification of the intended or executed transactions;

69.5. Receive a consent from the senior management for the commencement or continuation of the business relationship;

69.6. Perform in-depth supervision of the business relationship by increasing the number and frequency of controls applied and specifying the types of transaction for which reverification is necessary.

70. In cases where a customer executes untypically large transactions, complex transactions, seemingly mutually linked transactions or transactions which do not seem to have an economic purpose, the reinforced measures shall include:

70.1. A verification of the nature and purpose of the transaction;

70.2. The monitoring of the activities and transactions of the customer in order to ascertain that the transactions are not considered suspicious.

71. Depending on the situation, additional enhanced customer due diligence measures can also be applied such as:

71.1. Searching for additional independent and reliable sources to verify the information submitted by the customer to the Operator;
71.2. Performing additional measures to better understand the history, ownership and financial position of the customer;
71.3. Taking further measures to ensure that the transaction is consistent with the purpose of the business relationship;
71.4. Strengthening the monitoring of business relationships, including reinforced transaction controls.

72. When assessing whether there is increased MLTPF risk in a particular situation and the extent of customer due diligence necessary for risk management and mitigation the Operator shall take into account the following risk-increasing factors:
72.1. The business relationship is carried out under unusual circumstances;
72.2. The customer is affiliated with a higher risk jurisdiction:
72.2..1. A high-risk third country;
72.2..2. A country or territory with a high corruption risk;
72.2..3. A country or territory with a high level of criminal offences as a result of which proceeds from crime may be obtained;
72.2..4. A country or territory on whom financial or civil legal restrictions have been imposed by the United Nations Organisation, the United States of America or the European Union;
72.2..5. A country or territory which provides financing or support to terrorist activities or in the territory of which such terrorist organisations operate that are included in lists of countries or international organisations recognised by the Cabinet which have prepared lists of persons suspected of engaging in terrorist activities or in the production, storage, transportation, use or distribution of weapons of mass destruction.
72.3. The customer makes large-scale cash transactions;
72.4. The customer uses services, products or delivery channels thereof that favour anonymity;

72.5. The customer uses services, products or delivery channels thereof that restrict the possibilities of customer identification or acquiring knowledge inherent to its personal and economic activity;

72.6. The customer receives payments from an unknown third party;

72.7. The customer uses new services, products or delivery channels thereof, or new technologies.

73. **Customer Due Diligence Threshold and its Identification.** The Operator has an obligation to carry out a mandatory customer due diligence if a customer's transactions with the Operator conform with Clauses 27 and 28 of these guidelines. The customer due diligence threshold is set for a single transaction or linked transactions. Customers can carry out a number of linked transactions each of which is less than EUR 2,000 but that reach or exceed the threshold as an aggregate. The Operator shall take into account that the customer can consciously make pay-outs in a number of transactions in order to circumvent the threshold and avoiding customer due diligence.

74. The Operator shall develop a secure and reliable system for establishing the threshold with the help of IT solutions, as well as define the scope of customer due diligence activities in relation to the customer risk level.

75. The Operator shall ensure that the amount of money or means for participation in the game that a customer deposits in (inserts) and pays-out from (receives) a gaming machine cannot exceed EUR 2,000 if the Operator is not present (without customer due diligence). This requirement applies to gaming machines located in land-based gambling venues, such as gambling halls and casinos.

76. The Operator shall equip itself with technological systems or tools to monitor the transactions executed by customers and to provide assurance that all customers who reach the customer due diligence threshold are identified in a timely manner and are subject to an appropriate customer due diligence measure.

77. The Operator shall apply the most efficient procedures for identifying customers, detecting the customer due diligence threshold, and preventing

transactions with persons who are subject to international and national sanctions.

78. One of the main tasks of the Operator is to monitor the deposits and pay-outs of each customer, including exchange of tokens, spending on gaming machines and prize pay-outs.

79. The Operator shall ensure that every single gambling and lottery operation has appropriate procedures for detecting the customer due diligence threshold, taking into account the assessed MLTPF risk and the average turnover in each gambling and lottery operation.

80. Operators shall terminate business relationship with a customer and document this event if it is not possible to carry out the required customer due diligence measures. In such an event, the necessity to report a suspicious transaction to the FIU should be assessed.

81. **Identification and Identity Verification**. Customer Due Diligence consists of several stages, one of which is identification. The Operator shall identify the customer and then verify their identity when the transaction threshold is reached or upon establishing a business relationship. Customer identification includes the following activities:

    81.1. The Operator shall establish the customer's identification data, such as the customer’s first name, surname and identity code;

    81.2. Inspection of the information the customer has provided about themselves, by obtaining and verifying documents or information that justify the identity

    81.3. The Operator shall compare the information regarding the customer with the identification documents presented (passport, ID card).

82. When identifying a natural person, the Operator shall compare the visual likeness of the customer to the photograph included in the presented personal identification document and ascertain that the document does not bear any signs of falsification. If doubts arise and the Operator cannot verify that the customer who presents the personal identification document is the person in the photograph of the document, or the Operator cannot verify that the document does not bear any signs of falsification, it shall refrain from

engaging with such a customer and, following the requirements of the Law, report this to the FIU in case of suspicion.

83. A resident natural person is identified by checking its identity on the customer's personal identification document, which includes information about the customer's first name, surname, identity code[7].

84. The identification of a foreign resident customer can be performed by means of a document recognized as valid for entering the Republic of Latvia, that includes the customer's first name, surname, date of birth, photograph, as well as the number and date of issue of the identity document, the issuing country and body.[8]

85. In cases where a person has the right to enter and reside in the Republic of Latvia with a valid personal identification document and a valid visa or residence permit issued by the Republic of Latvia, the Operator shall make a copy of the personal identification document, as well as of the visa or residence permit since it recognizes the customer's right to enter the country.

86. In cases where the identity document of a third-country national is a residence permit issued by the Republic of Latvia (a temporary residence permit or a permanent residence permit) in accordance with laws and regulations governing the movement of persons, their identification can be carried out on the basis of the residence permit.

87. During the customer due diligence, it is useful to obtain information about the source and level of income of the customer, such as his occupation. This information can help the Operator to assess whether the amounts the customer spends on gambling or lottery are commensurate with their income or give rise to suspicion.

88. **Remote Identification**. Remote identification can only be employed by on-line gambling or lottery Operators for customers who intend to use the Operator's services — on-line gambling or lottery (interactive gambling or

[7] Cabinet Regulations No. 134 of 21.02.2012 "Regulations Regarding Personal Identification Documents";

[8] Cabinet Regulation No 215 of 29.04.2003 "Procedures for Recognition of Travel Documents of Aliens"

lottery), in accordance with the procedure prescribed by the Cabinet of Ministers[9].

89. The Operator can use remote customer identification if they have been assessed for MLTPF risk, an ICS has been established, staff has received training, the customer has been informed about the remote identification process and their rights and obligations within it, technological solution security requirements have been set in accordance with MLTPF risk.

90. The Operator shall not carry out remote identification of customers or shall interrupt it if circumstances are found which indicate that the risk-based approach has shown the customer to pose a high MLTPF risk, discrepancies are found in information obtained during customer due diligence, the security of the remote identification process has called into doubt.

91. Using the risk-based approach, the Operator shall apply one or more of the following types of remote identification during customer due diligence:
    91.1. A secure electronic signature that provides a qualified electronic identification of increased security;
    91.2. Video identification;
    91.3. The acquisition of natural person identity data from a credit institution or payment institution by means of an identification payment or other method which allows the customer's first name, surname and identity code to be obtained from a credit institution or payment institution;
    91.4. Comparison of the personal identification document photograph with the photograph of an electronic self-portrait.

92. **Origin of Funds and Origin of Wealth.** Verification of the origin of the customer's funds and wealth is a measure based on risk assessment. Depending on the MLTPF risk posed by the customer, the Operator shall determine the measures to be applied and is obliged to demonstrate that the measures it has taken (such as clarifications from the customer, documents obtained or publicly available information) are appropriate and proportionate to the risk inherent to the customer.

[9] Cabinet Regulations No 392 of 03.07.2018 "Procedures by which the Subject of the Law on the Prevention of Money Laundering and Terrorism Financing Performs the Remote Identification of a Customer"

93. The Operator shall verify the origin of the funds used in the customer's transactions and it cannot in all cases (irrespective of risk) rely solely on publicly available information regarding the customer's financial situation to conclude that the customer's funds do not originate from MLTPF. The fact that the customer is financially well-positioned does not exclude the possibility that the funds received in the customer's account or on their behalf or for their benefit have illegal origin and could be linked with MLTPF activities. Information obtained from public resources on the financial situation of the customer may in certain cases be assessed only as additional information and may not in all cases serve as a basis for drawing conclusions on the legality of the funds.

V. Detection and Reporting of Suspicious Transactions and Threshold Declaration Transactions

94. **Suspicious Transaction**. The Operator shall establish a procedure to assist its employees in detecting a transaction or activity which gives rise to reasonable suspicion that the funds involved are direct or indirect proceeds of crime or are linked with terrorism and proliferation financing or an attempt of such activities. The arrangements for detecting, documenting and circulating information about such a transaction shall be determined by the Operator.

95. In order to provide for an internal reporting system that will help to identify and report suspicious transactions, it shall be ensured that:

95.1. employees shall report to the employee responsible for PMLTPF if they have information or reasonable grounds to suspect that a person or customer is involved in money laundering or terrorist or proliferation financing or in an attempt of such activities;

95.2. the employee responsible for PMLTPF shall review each internal report and decide whether there are grounds for reporting it to the FIU;

95.3. employees shall be adequately trained in the performance of their duties, have the necessary skills to identify the characteristics of a suspicious transaction and to prepare an

internal report on a suspicious transaction to be submitted to the employee responsible for PMLTPF.

96. The characteristics of a suspicious transaction can be divided into two categories:

96.1. Customer-specific characteristics:

96.1.1. Problems with customer identification (the customer is unwilling to provide identification information or provides a minimal amount of it, provides fictitious information, provides information that is difficult to verify, there is reasonable suspicion that the personal identification document is a forgery);

96.1.2. The customer is nervous for no obvious reason;

96.1.3. The customer has minders who are observing them;

96.1.4. The customer brings money they have not counted;

96.1.5. The customer carries out a large number of small identical transactions that suggests a deliberate attempt of avoiding the threshold declaration;

96.1.6. There is reasonable suspicion that the customer or beneficial owner could be associated with terrorism even though they are not included on the list of terrorists and there are no previous reports about them in the FIU;

96.1.7. The customer gambles without a clear intention to win;

96.1.8. The customer seeks to establish contact with the Operator's employee or employees (outside working hours);

96.1.9. The customer connects to their interactive gambling or lottery account from high-risk countries;

96.1.10. The customer connects to an interactive gambling or lottery account from several countries over a short period of time.

96.2. Customer transaction-specific characteristics:

96.2.1. The customer carries out an untypical transaction (an uncharacteristically large amount of transactions – the exchange of bills (banknotes) for coins, means for participation in the game);

96.2.2. There is reasonable suspicion that the transaction involves the use of proceeds of crime;

96.2.3. The customer carries out a transaction that does not correspond to his financial situation;

96.2.4. The customer acts recklessly with large amounts of money;

96.2.5. The customer uses forged or non-conforming documents;

96.2.6. The customer uses loyalty (bonus) cards of other persons;

96.2.7. The customer carries out atypical actions or attempts fraudulent activities;

96.2.8. The customer becomes defensive when questioned or makes too many excuses;

96.2.9. The customer avoids customer identification and due diligence measures required by law;

96.2.10. The customer conceals the amount of money they paid to gamble in order to make the identification of the transaction and the total amount of mutually linked operations more difficult;

96.2.11. The transaction is linked to another suspicious transaction that has already been reported to the FIU;

96.2.12. The transaction has no apparent legal purpose;

96.2.13. The suspicious transaction is reported in other sources (mass media, police, internal security service, credit institutions);

96.2.14. Cases where a third party pays an amount of money so that the customer can participate in gambling;

96.2.15. The customer regularly makes bets below the threshold of EUR 2,000 or close to the threshold;

96.2.16. The customer attempts to make a deposit/pay-out to a third party;

96.2.17. The customer attempts to pay with/use a bank card of another person;

96.2.18. The customer has a large amount of TITO tickets (with different dates) or casino tokens they want to exchange for money;

96.2.19. The exchange of the customer's means for participation in the game against money does not correspond to the game they played;

96.2.20. The customer deposits money into their interactive gambling account, but does not participate in gambling;

96.2.21. The denomination of banknotes is untypical for the customer;

96.2.22. The packaging of banknotes is untypical for the customer;

96.2.23. A transaction in which low denomination coins or banknotes are exchanged for banknotes with a higher denomination (or vice versa) or for other banknotes with the same denomination;

96.2.24. In other cases, as defined in the internal control system.

97. This list of characteristics of a suspicious transaction is not exhaustive and the Operator can add other characteristics that give rise to suspicion. The detection of one or several suspicious transaction characteristics does not necessarily mean that the transaction in question is suspicious (it can serve as an indicator) – the characteristics must be assessed to ensure that reports to the FIU are timely, of high quality and contain a detailed description why the transaction is considered to be suspicious.

98. All suspicious cases shall be documented or electronically recorded by an employee of the Operator and then included in the internal suspicious transaction report. The report shall include details of the suspected customer and information justifying the suspicion of money laundering or terrorism or proliferation financing. All internal information searches or requests made in connection with the report must also be documented or electronically recorded. This information may be necessary to supplement the initial report or as evidence of good practice.

99. An employee of the Operator is considered to have completed their reporting obligation as soon as they have duly reported their suspicions to the employee responsible for PMLTPF or to the person to whom the obligation to receive internal reports has been delegated.

100. If the employee responsible for PMLTPF confirms the internal report of a suspicious transaction provided by the Operator's employee or identifies a suspicious transaction in the course of their own duties, they shall immediately report the suspicious transaction to the FIU in accordance with the reporting procedure.

101. If the employee responsible for PMLTPF decides not to report a suspicious transaction to the FIU, they must clearly document or electronically record and store the reasons for not doing so.

102. **Threshold Declaration.** The Operator shall provide for a procedure for identifying any transaction of EUR 2,000 or more. The threshold declaration transaction includes the following transactions:

102.1. The prize paid to the customer;

102.2. Payments to the customer;

102.3. The purchase of means for participation in the game done by the customer;

102.4. The sale of means for participation in the game done by the customer;

102.5. The exchange of means for participation in the game done by the customer;

102.6. Currency exchange done by the customer in order to purchase means for participation in the game;

102.7. Contributions made by the customer into interactive gambling or lottery game account;

102.8. Withdrawal by the customer of funds from the interactive gambling or lottery game account.

103. The threshold declaration for each transaction which amounts to EUR 2,000 shall be submitted to the FIU once a week and cover the time period since the submission of the previous threshold declaration.

104. The Operator shall maintain records of suspicious transaction reports and threshold declarations reported to the FID and make them available to the Inspection.

VI. Record Keeping

105. The purpose of record keeping is to provide law enforcement authorities responsible for control and supervision with sufficient evidence to conduct financial investigations. The Operator’s record keeping policy and procedure shall include entries in the following areas:

105.1. Information on how compliance has been monitored by the designated official;

105.2. Delegation of tasks of the employee responsible for PMLTPF;

105.3. Reports of the employee responsible for PMLTPF to senior management;

105.4. Customer identification and verification information;

105.5. Transaction monitoring data;

105.6. Due diligence information on the Operator's business partners;

105.7. Employee training records;

105.8. Suspicious transaction reports.

106. The continuous monitoring of customer transactions is a mandatory requirement for Operators and includes a thorough review of all transactions carried out over the course of the relationship (including an evaluation of the appropriate use of funds) to ensure that transactions are consistent with the Operator's knowledge of the customer, the customer's personal and economic activities and risk profile.

107. Regular customers shall be subject to a more thorough review and their level of activity shall be assessed by reference to information already known about them and, where necessary, additional information on their source of funds shall be collected and stored.

108. Occasional customer transactions shall be monitored with the aim of identifying the customer due diligence threshold and the audit trail shall be retained when the due diligence threshold is reached.

109. The Operator shall store all documents or copies thereof obtained during the customer due diligence. The Operator shall use copies of identification documents to demonstrate the basis upon which identification was done and for future reference to ascertain that the customer who has arrived at the gambling operation is the same person (for example, the Opera ensures before the game starts that the customer who presents the personal identification document is the same person that is already identified as the Operator's customer by comparing the customer's personal data shown in the personal identification document with the data contained in the copy of the identification document held by the Operator). If the Operator can provide information in the system on who completed the customer identification and scanned this document and when this was done, it is acceptable that the identification documents are scanned instead of copied.

110. The Operator shall provide for an update or revision of the due diligence documents after a certain period of time or under certain circumstances. For example, the Customer has not used the services of the Operator for a long time, or the Operator has learned that the status of the customer has changed (PEP, PEP family member or a person closely associated with a PEP).

111. Land-based gambling Operator must ensure that the customer's transactions are monitored not only during the customer's transactions at the gambling operation’s cash desk but also during transactions in gambling equipment (gaming machines, casino tables, betting terminals), with a clear description of its ICS procedure arrangements for the monitoring of transactions at the gambling operation (for example, through the creation of registers or systems in which customer transactions are recorded).

112. It is allowed to use information technology solutions and existing information systems that enable Operators to identify a player, remotely monitor player transactions, link cash flow (deposits, pay-outs and prizes) with a person and accurately record the moment when the EUR 2,000 threshold is reached or a transaction with a PEP begins.

113. The Operator must provide for that IT solutions (registers) or information systems referred to in Clause 112 can store audit trails and find

information on who and when has created entries in the register, as well as on what information has been changed (changelog).

114. For five years after the termination of the transaction or the execution of an occasional transaction the Operator shall keep all information obtained during the customer due diligence, information on all payments made by the customer, correspondence with the customer.

115. After the expiry of the five-year storage period, the Operator shall destroy the documents and information it has regarding the person. The Operator shall establish a procedure for the destruction of documents and information of its ICS.

116. Law enforcement authorities and the Inspection can extend the storage period of documents and information by a maximum of five years.

117. The Operator may choose the type of storage and processing of documents and information that is most appropriate for its activity and volume — original documents, photocopies of original documents, video, scanned copies, in an electronic format.

118. Processing of personal data of natural persons is only permitted for the purpose of preventing money laundering and terrorism and proliferation financing (PMLTPF).

VII. Persons Responsible for Fulfilment of PMLTPF Requirements

119. Persons responsible for the fulfilment of PMLTPF requirements:

119.1. An employee or several employees specially authorised by the Operator;

119.2. A representative of senior management (a member of the board, official or employee).

120. The level of knowledge of persons responsible for the fulfilment of PMLTPF requirements must be sufficient to enable them to take appropriate decisions in the field of PMLTPF.

121. Mandatory assessment requirements for candidates to the post of person responsible for the fulfilment of PMLTPF requirements:

121.1. Impeccable reputation;

121.2. Must not been punished for committing an intentional criminal offence against the state, property or administrative order, or for committing an intentional criminal offence in national economy or while in service in a state authority, or for committing a terrorism related criminal offence, or who has been punished for such offences, however, the criminal record thereon has been set aside or extinguished;

121.3. To whom sanction (except for a warning) regarding a violation of the laws and regulations in the field of the prevention of money laundering and terrorism and proliferation financing or international and national sanctions has not been imposed or to whom such sanction has been imposed, however, at least one year has passed since the day of its application;

122. The Operator can define additional requirements for the candidate.

123. The main factors affecting reputation are actions in accordance with laws and regulations, information on the person's previous personal or commercial activities, inspections carried out by public authorities. When assessing the reputation, the related persons - family members, persons known to be in business or other close relationship, shareholders or members of the same commercial company - also have to be assessed. It should be noted whether there is any publicly available negative information on the person and their related persons that might imply a link to MLTPF. Publicly available information must be objective and verifiable.

124. Within 30 days of receiving a gambling operation license, the Operator shall notify the Inspection of the persons responsible for the fulfilment of PMLTPF requirements.

125. The Operator shall issue an order designating the persons responsible for the fulfilment of PMLTPF requirements and inform the Inspection of the persons designated or any changes among the responsible persons within 30 days after the status of the person responsible for the fulfilment of PMLTPF requirements was acquired.

126. A person specially authorised by the Operator shall carry out the assessment of requirements for candidates to the post of person responsible for the fulfilment of PMLTPF requirements and document it in accordance with the procedure defined by the Operator.

127. The Operator shall clearly define in its ICS procedures the allocation of powers and responsibilities within the PMLTPF field to persons responsible for the fulfilment of PMLTPF requirements.

128. The Operator shall provide for the supervision of the activities of the person responsible for the fulfilment of PMLTPF requirements in order to prevent the risk that an employee makes unilateral decisions on matters regarding the Operator's activities in the PMLTPF field.

129. The persons responsible for the fulfilment of PMLTPF requirements have the following duties:

129.1. The development and updating of ICS policies and procedures;

129.2. Staff training;

129.3. Drafting of internal reports;

129.4. Reporting suspicious transactions to the FIU;

129.5. Submitting threshold declarations to the FIU;

129.6. The development and maintenance of internal registers;

129.7. The examination and evaluation of anonymous employee reports.

130. A representative of senior management shall ensure the supervision of the fulfilment of requirements laid down in the PMLTPF law, and the compliance of the responsible person and the entire staff with the practical implementation of PMLTPF requirements. The representative of senior management shall be entitled to establish procedures for the implementation of this supervision.

131. The senior management representative shall make independent decisions on the commencement or termination of transactions with high-risk customers, including PEP and persons associated with PEP, as well as with other high-risk customers. The decision-making procedure, its extent, frequency and the risk threshold that triggers the involvement of the senior

management representative shall be determined by the Senior Management of the Operator and based on proposals from the Senior management representative.

132. The Senior management representative shall be primarily guided by considerations of the PMLTPF field when performing duties in the board and adopting board decisions.

133. The Senior management representative shall ensure that the person responsible for the fulfilment of PMLTPF requirements submits an annual report on the functioning of the ICS and its effectiveness, shortcomings identified and corrected, as well as on proposals for the improvements in the PMLTPF work. The Senior management shall determine how often and how much information has to be reported.

VIII. Cooperation with Non-Governmental Organizations

134. The Operator shall carefully assess the existing MLTPF risks before launching a cooperation with non-governmental organizations (hereafter — NGO). Considering that the range of activities of NGOs includes also the collection of funds for a specific goal through charitable contributions and donations, and the collected funds are then transferred to third parties. In cases where the actual beneficiary and the purpose of use is unknown there are significant TF and MLTPF risks.

135. NGOs can be involved in several or any of the stages in the MLTPF scheme.

135.1. Collection of funds — NGOs can be involved in the collection of funds from natural persons, legal persons and other NGOs, including individuals and organizations;

135.2. Money laundering — NGOs can be involved in ML by merging such funds with legally collected funds, by depositing funds in credit institution accounts, making transfers or other financial activities;

135.3. Distribution of funds — laundered funds are channelled to persons or organizations linked to MLTPF by means of,

among other things, fictitious contracts, invoices and other documents, as well as to the benefit of persons or organizations linked to MLTPF.

136. The MLTPF scheme may feature one or several NGOs, including their branches and representative offices both at local and international level. The risk group consists mainly of NGOs whose representatives (the beneficial owners (BO), executive representatives) are residents of high-risk countries or countries with weak MLTPF regulation, or the NGO's activities are in some way related to such countries.

137. When an Operator intends to cooperate with an NGO, it shall develop and include in its PMLTPF system ICS arrangements and procedures that are based on an assessment of TF and MLTPF risk, as well as procedures for controlling the use of charitable contributions and donations collected during this cooperation.

138. Before starting a transaction with and NGO, the Operator shall identify the BO, assess the reputation of the NGO and the status of the NGO, check whether it has been awarded the status of a public benefit organization, the type of charitable contributions (cash or non-cash), the type of NGO activity (culture, sport, recreation, religion, protection of rights and interests, etc.).

139. Regarding transactions with an NGO (charitable contributions, donations, etc.) the Operator shall provide in its ICS for procedures aimed at controlling the use of the funds allocated (verifying that the goal was achieved) and obtain documentary assurance and evidence of cash flows in order to ascertain that the funds of charitable contributions or donations were not used in the field of MLTPF.

IX. Final provisions

140. These guidelines enter into force on 29 December 2023.