# CYPRUS GAMING AND CASINO SUPERVISION COMMISSION

## DIRECTION ISSUED PURSUANT TO ARTICLE 59(4) OF THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAWS OF 2007 (188(I)/2007) AND REGULATION 18(3) OF CASINO OPERATIONS AND CONTROL (GENERAL) REGULATIONS OF 2016 (R. 97/2016)

**VERSION 4.0**

**Reg. F. 12.04.017**

**Approved by the Board of Directors, 07 November 2025**

3, Thaleias Str., 1st Floor, 3011 Limassol|
P.O.Box 70004, 4160 Polemidia, Limassol, Cyprus
Tel.: +357 25573800, Fax: +357 25573801
Email: info@cgc.org.cy
www.cgc.org.cy

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

# Contents


DEFINITIONS.....5

INTRODUCTION.....10

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT.....11

Risk based approach.....11

Business Wide Risk Assessment.....12

Customer Risk Assessment.....12

RISK MANAGEMENT.....15

Design and implementation of internal controls to manage and mitigate the risks.....15

Responsibility for addressing risk.....16

BOARD OF DIRECTORS & SENIOR MANAGEMENT DUTIES AND RESPONSIBILITIES.....18

Role of the Anti-Money Laundering Compliance Officer.....21

Appointment of Anti-Money Laundering Compliance Officer ("AMLCO").....21

Duties of the AMLCO.....22

Internal Audit.....29

Education and training of employees.....29

Evaluation of integrity of employees.....31

CUSTOMER DUE DILIGENCE.....32

General requirements.....32

Application of Customer Due Diligence measures.....32

Timing of Customer Due Diligence measures.....34

Customer relationships.....34

Establishment of a business relationship.....35

Occasional transactions.....36

Business to Business relationships (including Junkets).....37

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

**Identification and verification** ..... **37**

Natural persons ..... 38

Legal entities ..... 40

Unincorporated businesses, partnerships and other persons with no legal substance ..... 41

**Identification of beneficial owners** ..... **42**

**Assessing and obtaining information on the purpose and intended nature of the business relationship** ..... **42**

**Ongoing monitoring** ..... **43**

**Simplified (customer) Due Diligence** ..... **45**

**Enhanced (customer) Due Diligence** ..... **47**

Politically Exposed Persons (PEPs) ..... 48

Unusual transactions ..... 49

High-risk third countries ..... 49

Other high-risk situations ..... 50

**Cash Deposits** ..... **51**

**Certificate of Winnings** ..... **56**

**Cashing out** ..... **56**

**Reliance on third parties** ..... **57**

**Transactions and products that favour anonymity** ..... **59**

**Prohibition of opening or maintaining anonymous or numbered accounts** ..... **59**

**Requirements to cease transactions or terminate relationship** ..... **60**

**Safety deposit boxes** ..... **60**

**RECORD KEEPING & DATA PROTECTION** ..... **62**

**General requirements** ..... **62**

**Supporting records (gaming machines)** ..... **64**

**Data Protection** ..... **64**

**SUSPICIOUS ACTIVITIES AND REPORTING** ..... **66**

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Internal reporting.....66

Evaluation and determination by the AMLCO.....67

External reporting to MOKAS .....67

WHISTLEBLOWING .....69

FINANCIAL SANCTIONS .....70

SUBMISSION OF DATA AND INFORMATION .....73

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## DEFINITIONS

"AML/CTF" means Anti-Money Laundering and Counter-Terrorism Financing.

"AMLCO" means the Anti-Money Laundering Compliance Officer of the Operator.

"Beneficial Owner" means any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted and includes at least:

A. <u>In the case of corporate entities:</u>

(i) the natural person who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that corporate entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

Provided that

(a) an indication of direct shareholding shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person; and

(b) an indication of indirect ownership shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person or persons.

Provided further that the control by other means can be verified, inter alia, based on the criteria provided for in section 142 (1) (b) and section 148 of the Companies Law;

(ii) the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under subparagraph (i) of the present paragraph is identified, or if there is any doubt that the person identified is the beneficial owner:

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

B. In the case of trusts:

(i) the settlor;

(ii) the trustee or commissioner;

(iii) the protector, if any;

(iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; and

C. In the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the person referred to in paragraph B.;

"Board of Directors" means the board, committee and/or body of the Operator that has the power to set the strategy, objectives, and general direction of the Operator and oversees and monitors management decision-making, including a person who effectively directs the business activities of the Operator.

"Business relationship" means business, professional or commercial relationship between the customer and the Operator, which is linked to the professional activities of the Operator and which is expected, at the time when the contact is established, to have an element of duration.

"Cash" means

a) currency;

b) bearer-negotiable instruments;

c) (Commodities used as highly-liquid stores of value; and

d) prepaid cards as defined in Article 2(1), point (a), of Regulation (EU) 2018/1672 of the European Parliament and of the Council.

"Cash declaration" means the declaration has to be made in accordance with Article 5 of the Control of Cash Entering or Leaving the European Union and the Exercise of Intra-Union Controls on Cash law of 2022 (N. 63(I)/2022).

"Commission" means the Cyprus Gaming and Casino Supervision Commission established and operating pursuant to the Casino Operations and Control Law of 2015 (L. 124(I)/2015).

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

"Control of Cash Entering or Leaving the European Union and the Exercise of Intra-Union Controls on Cash law of 2022 (N. 63(I)/2022)" is the Law of the Republic of Cyprus enacted for the purpose of effectively implementing certain provisions of Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union, and repealing Regulation (EC) No 1889/2005.

"Crypto Asset" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically, and it is not-

a) Fiat currency, or

b) Electronic money, or

c) Financial instruments, as these are specified in Part III of the First Appendix to the Investment Services and the Activities and Regulated Markets Law.

"Customer" means a person which aims to establish a business relationship or performs an occasional transaction with the Operator.

"EU Directive" means Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of Money Laundering and Terrorist Financing.

"High-risk third country" means a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers, and which has strategic deficiencies in its national AML/CTF regime that pose significant threats to the financial system of the European Union, and a third country which is classified by the Operator as high risk, according to the risk assessment referred to in Article 58a of the Law.

"Junket operator" has a meaning given to this term by the Casino Operations and Control Law of 2015 (L. 124(I)/2015).

"MOKAS" means the Unit for Combating Money Laundering of the Republic of Cyprus established according to section 54 of the Prevention and Suppression of Money Laundering Activities Law.

"Occasional transaction" means any transaction other than a transaction which takes place during a business relationship.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

"Operator" means a person holding the integrated casino resort license and is licensed to operate the temporary, satellite casinos and integrated casino resort in the Republic of Cyprus.

"Person" means both natural person and legal entity.

"Politically Exposed Person (PEP)" means a natural person who is or who has been entrusted with prominent public function in the Republic or in another country, an immediate close relative of such person as well as a person known to be a close associate of such person:

Provided that, for the purpose of the present definition, 'prominent public function' means any of the following public functions:

(a) heads of State, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies;

(b) members of the governing bodies of political parties;

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(d) members of courts of auditors or of the boards of central banks;

(e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(f) members of the administrative, management or supervisory bodies of State-owned enterprises;

(g) directors, deputy directors and members of the board or equivalent function of an international organisation;

(h) mayor;

Provided further that no public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials;

Provided furthermore that "close relatives of a politically exposed person" includes the following:

(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;

(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(c) the parents of a politically exposed person;

Provided even furthermore that 'persons known to be close associates of a politically exposed person' means natural person:

(a) who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;

(b) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

"Senior Management" means an officer or employee of the Operator with sufficient knowledge of the Operator's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the board of directors.

"Source of funds" means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

"Source of wealth" means the origin of the customer's total wealth, for example inheritance or savings.

"The Law" or "AML Law" means the Prevention and Suppression of Money Laundering Activities Laws of 2007 (L.188 (I)/2007) as amended.

"Third Country" means a country not member of the European Union or contracting party to the agreement of the European Economic Area signed in Porto on the 2nd of May 1992 and adjusted with the Protocol signed in Brussels on 17 May 1993, as amended.

"Transaction" means gambling transaction and/or financial transaction of the casino related to casino gambling.

Without prejudice of the abovementioned provisions, terms not defined in this Direction shall have the meaning given to them by the Law.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## INTRODUCTION

1. Under the provisions of the Prevention and Suppression of Money Laundering Activities Law (hereinafter referred to as the "Law" or the "AML Law"), the Cyprus Gaming and Casino Supervision Commission (hereinafter referred to as the "Commission") is the competent supervisory authority for casino gambling and financial activities and transactions of the casino related to casino gambling within the Republic of Cyprus, and has the duty of monitoring, evaluating and supervising the implementation of the AML Law and of the Directions issued to the Operator.

2. The present Direction is issued in accordance with the powers vested in the Commission by virtue of Article 59 of the AML Law and Regulation 18(3) of the Casino Operations and Control (General) Regulations.

3. This Direction, as explicitly stated in the AML Law, is directly legally binding and compulsory for the Operator and has been prepared with the aim of specifying the details and the manner of application of the AML Law by the Operator. The Direction requires the adoption and implementation of procedures and systems to effectively address and prevent the risks of committing or attempting to commit the money laundering and terrorist financing offence.

4. It is stressed out that the present Direction contains the minimum requirements and obligations of the Operator and does not purport to be and should not be considered a guide as to how the Operator will conduct its business to meet its obligations under the Law. The Commission expects that the Operator designs and implements its own mechanisms, control systems and internal policies and procedures emanating from its business wide risk assessment and risk management approach in order to achieve compliance with the Law and this Direction and effectively address and prevent the AML/CTF risks.

5. Section "Financial Sanctions", of the present Direction is issued in accordance with the Article 3(2) of the Implementation of Provisions of the United Nations Security Council's Resolutions and Decisions (Sanctions) and Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law of 2016 (58 (I)/2016) with the aim of laying down the control systems, policies and procedures that the Operator should establish in order to achieve compliance with financial sanctions legislation.

6. The present Direction replaces the 'Prevention and Suppression of Money Laundering Activities' Direction, issued by the Commission in November 2019.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

# MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

## Risk based approach

Article 58 and 58A of the Law

7. Article 58(d) and Article 58A of the Law require the obliged entities (i.e. the Operator) to identify and assess money laundering and terrorist financing risks, and to establish and maintain proportionate policies, procedures and controls to mitigate and effectively manage the identified risks.

8. A risk-based approach to AML/CTF means that the Operator is expected to identify, assess and understand the money laundering and terrorist financing risks to which it is exposed and take AML/CTF measures commensurate to those risks in order to mitigate them effectively. The risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. The Operator needs to assess and evaluate the risk of how it might be potentially exposed or vulnerable through the use of its services by criminals for the purpose of money laundering and terrorist financing.

9. The risk-based approach involves a number of steps in assessing the most effective way to manage and mitigate the money laundering and terrorist financing risks faced. These steps require the Operator to:

(a) identify the money laundering and terrorist financing risks that are relevant to the Operator

(b) design and implement appropriate policies, procedures and controls to manage and mitigate these risks

(c) monitor the effectiveness of implemented controls and improve them if needed

(d) document what has been done, and why.

10. The Operator should always identify and assess the money laundering and terrorist financing risks associated with the following groups of risk factors as a minimum:

(a) products, services and transactions it offers

(b) countries or geographic areas

(c) the customers it attracts and

(d) delivery channels it uses to service its customers.

11. The Operator should risk assess (i) its business activity **(Business Wide Risk**

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

**Assessment)** and (ii) the risk to which it is exposed as a result of business relationships or occasional transactions **(Customer Risk Assessment)**. The Business Wide Risk Assessment is necessary for the Operator to understand the overall exposure of its business to money laundering and terrorist financing and to identify areas of business it needs to prioritise in the fight against money laundering and terrorist financing. The Customer Risk Assessment is necessary to understand its money laundering and terrorist financing risk exposure that is a result of a business relationship or occasional transaction.

12. The Operator when assessing its Business Wide Risk and Customer Risk, should consult data, information and reports that are published by the Financial Action Task Force (FATF) including:

(a) FATF's RBA Guidance for Casinos (click here to access the document)

(b) FATF's Guidance Vulnerabilities of Casinos and Gaming Sector (click here to access the document).

### Business Wide Risk Assessment

13. The steps taken for identification and assessment of money laundering and terrorist financing risk must be proportionate to the nature and size of the Operator. In this regard, the Operator must:

(a) keep an up-to-date record in writing of all the steps taken to identify and assess the money laundering and terrorist financing risks to which its business is exposed

(b) provide the written risk assessment it has prepared and the information on which it was based to the Commission on request.

14. The Business Wide Risk Assessment must be reviewed and updated at least annually and every time that there is a material change influencing the Operator's business – e.g. changes in regulation, introduction of new products/services, new technology, delivery channels etc.

15. The Business Wide Risk Assessment shall be signed-off at the Board level and needs to be kept up to date. Once the Business Wide Risk Assessment has been completed, the Operator should be in the position to set a "risk-appetite" which means that the Operator decides the level of risk it is prepared to accept.

### Customer Risk Assessment

16. Customer Risk Assessment shall be completed in the context of a business

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

relationship or occasional transaction that requires Customer Due Diligence under this Direction, and lead to categorization of customers and occasional transactions as low, medium or high risk.

17. The assessments of risk should be based on criteria that reflect the causes of risk and should be documented properly. Each category of risk should be accompanied by corresponding Customer Due Diligence measures, periodic monitoring and controls. A Customer Risk Assessment for every business relationship and occasional transactions shall be documented accordingly and the Operator should be able to provide the Commission with evidence that its Customer Due Diligence measures are commensurate with the risk level.

18. The assessment of risks is an ongoing process. Not all risks will be understood at the outset of establishing a business relationship with the customer or performing an occasional transaction. However, the Operator should be able to justify to the Commission that it has applied a holistic approach when identifying relevant risk factors related to particular customer, collected sufficient information about the customer based on risk level and performed adequate CDD measures in line with the level of risk.

*Customer risk factors*

19. When identifying the risk associated with its customers, including its customers' beneficial owners, the Operator shall consider, to the extent that circumstances require, the risks related to:

(a) the customer's and (where appropriate) the customer's beneficial owner's business or professional activity in whatever country they are associated with

(b) the customer's and (where appropriate) the customer's beneficial owner's reputation in whatever country they are associated with and

(c) the customer's and (where appropriate) the customer's beneficial owner's nature and behaviour in whatever country they are associated with.

*Country/geographic risk factors*

20. Some countries pose inherently higher money laundering and terrorist financing risk than others. The Operator should utilise a variety of credible sources to determine a level of money laundering and terrorist financing risk related to a specific country. In this regard, the Operator shall take into consideration as a minimum the risk factors provided in the Law and any Guidelines issued by the Commission.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

21. When identifying the geographic risk associated with countries and geographical areas related to a particular customer, the Operator shall consider, to the extent that circumstances require, the risk related to:

(a) the jurisdictions in which the customer and any beneficial owner are based

(b) the jurisdictions that are the customer's and any beneficial owner's main places of business

(c) the jurisdictions to which the customer and any beneficial owner have relevant personal links.

22. When assessing country/geographic risk the Operator should as a minimum consider any association with financial sanctions orders, quality of controls, terrorism risk and levels of corruption or other criminal activity related to the country/geographic area.

*Products, services and transactions risk factors*

23. When identifying the risk associated with its products provided, services or transactions, the Operator shall consider the risks related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords

(b) the complexity of the product, service or transaction and

(c) the value or size of the product, service or transaction.

*Delivery channel risk factors*

24. When identifying the risk associated with the way in which the customer obtains the Operator's products or services, the Operator shall consider the risks related to:

(a) the extent to which the business relationship is conducted on a non-face-to-face basis

(b) any introducers or intermediaries the Operator might use and the nature of their relationship with the Operator.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## RISK MANAGEMENT

### Design and implementation of internal controls to manage and mitigate the risks

Article 58, 58C and 58D of the Law

25. Regulation 18 of Casino Operations and Control (General) Regulations of 2016 introduces the obligation to the Operator to establish and maintain an AML/CTF program. Furthermore, the Article 58(d) and Article 58A of the Law require the obliged entities, including the casinos, to establish and maintain proportionate policies, procedures and controls to mitigate and effectively manage the identified risks. Therefore, the Operator is required to establish a risk-based AML/CTF program that contains policies, procedures and controls to effectively mitigate and manage its identified money laundering and terrorist financing risks.

26. This shall include as a minimum the following:

(a) customer identification and Customer Due Diligence measures

(b) record-keeping arrangements

(c) internal reporting and reporting arrangements to MOKAS

(d) internal control, risk assessment and risk management arrangements to prevent money laundering and terrorist financing

(e) detailed examination of each transaction which by its nature may be considered particularly vulnerable to association with money laundering or terrorist financing, in particular; complex or unusually large transactions and all other unusual patterns of transactions which have no apparent rationale, economic or visible lawful purpose

(f) risk management practices

(g) compliance management arrangements

(h) the recruitment and evaluation of the integrity of the employees

(i) informing its employees about:

i. the Operator's systems and procedures for the prevention of money laundering and terrorist financing

ii. the Law and AML/CTF Directions issued by the Commission

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

iii. the European Union's Directives with regard to the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and

iv. relevant Data Protection requirements.

(j) ongoing training of its employees in the recognition and handling of transactions and activities which may be related to money laundering and/or terrorist financing.

27. The Operator's policies, procedures and controls must be:

(a) proportionate regarding the size and nature of the Operator's business

(b) approved by Operator's Senior Management.

## Responsibility for addressing risk

28. The Operator's Board of Directors and Senior Management bear the final responsibility for ensuring that the Operator applies an effective system to prevent money laundering and terrorist financing as well as responsibility for creating the culture of compliance. They have the ultimate responsibility to ensure that appropriate and effective systems and procedures for internal control have been introduced and applied, which reduce the risk of the products and services of the Operator being used for money laundering and terrorist financing.

29. The commitment of Senior Management from all relevant areas of the Operator's business to the implementation of the AML/CTF measures is a key element for the design and implementation of a risk-based approach as well as active cooperation of all relevant employees. Senior Management must be fully engaged in the processes of the Operator's assessment of risks of money laundering and terrorist financing and be involved in decision making to develop and implement the Operator's policies and processes to comply with the Law. The Board of Directors has overall accountability for overseeing the AML/CTF risk management program and Senior Management's implementation of the AML/CTF program.

30. The Article 58D of the Law requires that the Operator appoint a competent member of the Board of Directors, to be responsible for the implementation of the provisions of the Law and relevant AML/CTF Directives and/or circulars and/or regulations, including any relevant acts, Directives and Regulations of the European Union.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

31. The specific duties and responsibilities of the director appointed under Article 58D of the Law as responsible for AML/CTF matters need to be recorded in the Board of Directors corporate governance or operating procedures and be approved by the Board of Directors.

32. It is required that the Operator's responsible director will be a Board member responsible for the Operator's compliance with the Law, this Direction, any applicable acts, Directives and Regulations of the European Union and the effectiveness of Operator's risk management arrangements. He/she will be responsible for the supervision of the AMLCO and the implementation of the Law and Directions as well as any other applicable regulations.

33. The person nominated for appointment as responsible AML Director must submit a Casino Key Employee License Application form and any additional information and documents that may be requested by the Commission from time to time. The Operator must, within 14 days of the appointment, inform the Commission of the identity of the individual appointed under the Article 58D of the Law, and any subsequent appointments or changes to that position.

34. Article 58C of the Law provides that the Senior Management of the Operator shall approve the policies, procedures and controls applied by the Operator in relation to money laundering and terrorist financing, shall monitor and, where appropriate, strengthen the measures taken.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## BOARD OF DIRECTORS & SENIOR MANAGEMENT DUTIES AND RESPONSIBILITIES

35. The Board of Directors and Senior Management shall have the following duties and responsibilities:

(a) The Board of Directors shall define, record and approve the general principles of the Operator's policy for the prevention of money laundering and terrorist financing, which it communicates to Senior Management and the AMLCO. An effective program for the prevention of money laundering and terrorist financing requires a recorded and clear message in relation to the risk appetite, which shall determine the expectations, parameters and limits of operation of the program and the Operator's commitment to combatting money laundering and terrorist financing.

(b) The Board of Directors shall give leadership by expressing the Operator's values and corporate compliance culture ensuring that its AML/CTF program behaviour reflects these values.

(c) The Board of Directors and the Senior Management shall have knowledge of the level of risk of money laundering and terrorist financing that the Operator is exposed to, so as to decide whether all necessary measures are being taken for its management, according to its risk appetite.

(d) The Board of Directors designates an experienced person to the position of the AMLCO and ensures that the AMLCO and assistants have, and continually acquire the required knowledge and skills for their roles.

(e) The Board of Directors shall ensure that there is a clear access and reporting mechanisms between the responsible director and AMLCO for escalated incidents and monitoring the activity to manage money laundering and terrorist financing risk.

(f) The Board of Directors shall ensure that the AMLCO has sufficient resources to undertake his/her duties. This includes but is not limited to, competent staff, technology and equipment, and access to responsible executive(s) for the effective discharge of their duties. The AMLCO (and assistants) and any other person assigned with the duty of implementing or reviewing the program and procedures for the prevention of money laundering and terrorist financing shall have complete and timely access to all relevant data and information concerning customers' identity, transactions and other information maintained by the

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Operator so as to be effective in their duties.

(g) The Board of Directors and Senior Management shall ensure that policies, procedures and measures are applied across the Operator business activities so as the risk of money laundering and terrorist financing is identified, assessed and managed during the day-to-day operations of the Operator and in relation to:

(i) The development or introduction of new products, services, new business practices, including new delivery channels (including premises), new financial management arrangements, including contracts with affiliates or associates,

(ii) The use of new or developing technologies relating changes in existing products or their delivery, and

(iii) Possible changes in the business model /profile of the Operator.

Risk assessments should take place prior to the launch of the new/changed products, business practices or the use of new or developing technologies.

(h) The Board of Directors and Senior Management shall ensure that proper governance arrangements, reporting and information management arrangements for managing money laundering and terrorist financing risk are in place and are based on the three lines of defence model with clear definition of the responsibilities of each department involved in the prevention of money laundering and terrorist financing.

(i) The ability to make proper decisions will be weakened by unclear information management arrangements or poor data quality. The Operator must ensure that its program includes effective information management arrangements and arrangements to ensure data quality standards are maintained. Roles and responsibilities relating to data quality should be clearly defined and well organised. Data and information collected to meet the requirements of the Law and this Direction and the Operator's program should be accurate, easy to retrieve and retained in line with the requirements defined by the Law and this Direction.

(j) The Senior Management and the AMLCO are responsible for designing policies, procedures and controls and also the description and clear definition of responsibilities and limits of responsibility of each department that is dealing with matters related to the prevention of money laundering and terrorist

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

financing and to ensure that the internal practices, procedures and controls are appropriately documented.

(k) The Board of Directors shall ensure that the Operator has in place appropriate procedures for its employees, or persons in a comparable position, to report breaches of the Law and this Direction internally through a specific, independent and anonymous channel, proportionate to its nature and size.

(l) The responsible director and Senior Management shall approve the AML/CTF policies and procedures and ensure this is effectively communicated to all managers and employees that manage, monitor or control the customers' transactions with responsibility for the application of the practices, measures and procedures determined.

(m) The Board of Directors shall assess and approve the AMLCO's Annual Report and shall take all actions as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

(n) The Board of Directors and Senior Management shall ensure that all requirements of the Law and Commission's Directions are applied and that the Operator is able to assure the Commission with evidence that appropriate, effective and sufficient systems and controls are present for achieving the identification and management of money laundering and terrorist financing risk.

(o) The Board of Directors shall ensure that all employees are aware of the person appointed as the AMLCO (and alternates/assistants) to whom they shall report information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing.

(p) The Board of Directors and Senior Management shall receive sufficient, regular and objective information to have an accurate picture of the money laundering and terrorist financing risk to which the Operator is exposed.

(q) The Board of Directors and Senior Management shall receive sufficient and objective information from the AMLCO and Internal Audit regarding the effectiveness of the measures and controls against money laundering and terrorist financing.

(r) All relevant employees shall receive sufficient training related to AML/CTF matters necessary for performance of their roles at the Operator.

(s) The Operator shall apply explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

## Role of the Anti-Money Laundering Compliance Officer

### Appointment of Anti-Money Laundering Compliance Officer ("AMLCO")

#### Article 69 of the Law

36. Article 69 of the Law requires obliged entities to apply the following internal reporting procedures and reporting to MOKAS:

(a) Appoint as the AMLCO a Senior Management level employee who has the relevant skills, knowledge and expertise, to whom to report any information or other matter which comes to their attention and which, in their opinion proves or creates suspicion that another person is engaged in money laundering and/or terrorist financing.

(b) Require that any report be considered by the AMLCO in the context of all relevant information, to determine whether or not the information or other matter in the report proves this a fact or creates suspicion.

(c) Allow the AMLCO in line with the subparagraph (b) above, to have direct and timely access to any information, records and documents which may be of assistance to him/her and which is available to the Operator and

(d) In case where they know or have reasonable suspicion that funds, irrespective of their amount, are revenue from illicit activities or related to the financing of terrorism, ensure that MOKAS is immediately informed, at their own initiative, by the AMLCO referred to in subparagraph (a), by submitting a relevant report and providing further information at the request of MOKAS.

(e) Provide to MOKAS directly, at its request, all necessary information.

37. The Law explicitly provides for the obligation to report to MOKAS any attempt to execute suspicious transactions.

38. Further information pertaining to the reporting of suspicious activities and transactions can be found in Section titled "Suspicious Activities and Reporting" of this Direction.

39. The AMLCO should be appointed by the Board of Directors, after having been licensed to perform the role by the Commission. The Commission reserves the right to request his/her substitution if, in its opinion, he/she is no longer "fit and proper" to perform

his/her duties. Additionally, the casino Operator should also appoint an Alternate AMLCO who should assist the AMLCO in performance of his/her duties and deputize for the AMLCO in case of absence.

40. The AMLCO and any other person assigned with the duty of implementing or reviewing the program and procedures for the prevention of money laundering and terrorist financing must receive in-depth training concerning all aspects of the Law, this Direction and recent developments in the field, enabling them to update internal procedures in an effective manner and be able to demonstrate this to the Commission.

41. The AMLCO should act independently and autonomously to perform his/her duties and possess the appropriate seniority so as to command the necessary authority. In order to ensure his/her impartial judgement, the AMLCO should not, for example, have business responsibilities or undertake responsibilities for the data protection framework or the operation of internal audit.

42. Persons nominated for appointment as AMLCO or assistant AMLCO, must submit a Casino Key Employee License Application form, which includes information regarding the person's career, including the qualifications held and work experience, as well as details of any sanctions or criminal convictions against the person and any additional information and documents that may be requested by the Commission from time to time.

43. In case of change of the AMLCO and assistant, the Operator needs to inform the Commission in writing within a period of 14 days about such change, providing explanation as to reasons for a change and the details of the new proposed candidate for the AMLCO or assistant AMLCO position.

### Duties of the AMLCO

44. The role and responsibilities of the AMLCO and the Assistant AMLCO should be clearly specified by the casino Operator and documented in the relevant internal procedures and personal contract(s) of the individual(s).

45. Furthermore, the Operator's Compliance department should maintain a procedures manual for all AMLCO's tasks/responsibilities.

46. As a minimum, the duties of the AMLCO should include the following:

(a) The AMLCO has the responsibility, to record and assess on an annual basis all risks arising from existing and new customers, products and services as well as the measures or changes to the systems and procedures implemented by the Operator for the effective management of the aforesaid risks. This report

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(Business Wide Risk Assessment) should be submitted to the Board of Directors for consideration and approval, and the AMLCO is required to report to the Board of Directors and Senior Management of any change in these risks on an on-going basis. A copy of the Business Wide Risk Assessment and AMLCO's Annual report should be submitted to the Commission.

(b) The AMLCO shall prepare the AMLCO's Annual Report in line with the requirements of this Direction.

(c) The AMLCO and Senior Management are responsible for designing policies, procedures and controls relevant to the prevention of money laundering and terrorist financing as required by the Law, this Direction and any other relevant regulations. This should include the clear definition of responsibilities and limits of responsibility of each department that is identified within the AML/CTF program and ensure that the internal practices, procedures and controls are appropriately documented.

(d) The AMLCO shall develop and establish the Operator's Customer Due Diligence capabilities and procedures including Customer Risk Assessment methodology which are submitted to the Board of Directors for consideration and approval.

(e) The AMLCO shall monitor and assess whether the policies, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the AMLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments/premises of the Operator) which will provide him/her with the necessary information for assessing the level of compliance with the procedures and controls currently in force. The AMLCO shall regularly inform the Board of Directors and Senior Management regarding the findings of these audits and the level of compliance.

(f) The AMLCO shall ensure that the Operator prepares and maintains records of customers categorized following the risk-based approach into low, medium or high category and which should contain the information prescribed by the Law and this Direction.

(g) The AMLCO shall maintain a register of all cases of persons (prospective customers) for which the Operator declined the establishment of business relationship and/or terminated the business relationship for compliance reasons.

(h) The AMLCO shall verify that the third party with which the Operator intends to

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

cooperate on Customer Due Diligence issues meets the requirements stipulated in the Law and this Direction and gives his/her written consent for the cooperation which should be duly justified and kept in the file of the third party. The AMLCO shall also evaluate the quality of customers recommended by third party.

(i) The AMLCO shall receive information from the Operator's employees which is considered to be knowledge or suspicion of money laundering and/or terrorist financing activities or might be related with such activities. The information shall be received in a written report form (referred to as "Internal Suspicion Report"). All such reports should be registered and kept in a secure separate file.

(j) The AMLCO shall evaluate and examine the information received in the Internal Suspicion Report (ISR) by reference to other relevant available information and review the circumstances with the reporting employee and, where appropriate, their superiors. The evaluation of the ISR shall be completed as a separate written report (to be referred to as "Internal Evaluation Report") which will be documented and kept in a secure separate file.

(k) If as a result of completing the Internal Evaluation Report (IER), the AMLCO decides to notify MOKAS, then he/she shall complete a written report and submit it to MOKAS the soonest possible in the way and form prescribed by MOKAS. All such reports should be registered and kept in a secure separate file.

(l) Following submission of an AMLCO's report to MOKAS, the transactions of the customer(s) involved and related accounts shall be monitored by the AMLCO. Following any directions from MOKAS, the AMLCO shall investigate and examine all transactions. The conclusions of AMLCO monitoring and investigations should be accurately documented and kept in secure file.

(m) If following the evaluation and completion of the IER, the AMLCO decides not to notify MOKAS then he/she must fully document the reasons for the decision including all the steps and analysis that were performed during the course of the AML investigation. This will be recorded on the "Internal Evaluation Report" which should, be registered and securely retained.

(n) The AMLCO shall maintain a registry for ISRs, IERs and MOKAS reports with relevant management information (e.g. unit submitted the report, date of submission of the internal report, date of assessment, date of reporting to MOKAS).

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(o) The AMLCO shall act as a first point of contact with MOKAS, for all operational matters. The AMLCO shall respond to requests from MOKAS and provide all the supplementary information requested and fully co-operate with MOKAS. The AMLCO shall respond to all requests and queries from MOKAS and the Commission, provide all requested information and fully cooperate with MOKAS and the Commission.

(p) The AMLCO is responsible for the timely and accurate submission of reports to the Commission prescribed as necessary by this Direction or required to support investigations enquiries. The AMLCO shall respond promptly to any queries or clarifications requested by the Commission.

(q) The AMLCO shall maintain records for a period of 6 (six) years after the termination of business relationship with the third party with the data/information of the third person as prescribed in Section "Reliance on third parties" of this Direction.

(r) The AMLCO shall receive or suggest, depending on the case, corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing in accordance with the findings of any Commission investigation.

(s) The AMLCO shall take or suggest, where appropriate, corrective measures regarding the matters related to prevention of money laundering and terrorist financing in line with the findings of any audit conclusions of the Commission.

(t) The AMLCO shall evaluate the findings of the Internal Audit regarding the taking of corrective measures on issues related to the prevention and suppression of money laundering and terrorist financing.

(u) The AMLCO shall provide advice and guidance to the employees of the Operator on matters related to prevention of money laundering and terrorist financing.

(v) The AMLCO shall monitor and determine the Operator's departments and employees need for training and education and organize appropriate training sessions/seminars. In this regard, the AMLCO shall prepare and apply an annual staff training program which must include mandatory testing of employee's knowledge of AML/CTF matters.

(w) The AMLCO shall ensure that the records in relation to the seminars and other training of the Operator's employees are kept. The AMLCO assesses the

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

adequacy of the education/training provided. Such records shall include:

(i) Name of employee per department and position (i.e. management, officers, newcomers, etc.)

(ii) Date of the seminar, title, duration, names of lecturers, summary of the content of the training.

(iii) Whether the lecture/seminar was organized internally or offered by an external organization or consultants

(iv) Results of AML/CTF testing.

*AMLCO's Annual Report*

47. The AMLCO shall prepare an Annual Report which will assess the Operator's level of compliance with its obligations laid down in the Law, relevant regulatory framework and its program for the prevention of money laundering and terrorist financing.

48. The AMLCO's Annual Report should deal with money laundering and terrorist financing preventive issues pertaining to the preceding year under review and, as a minimum, shall cover the following:

(a) Description of the business operations/model of Operator during the last year, identifying the products/services offered, number and size of premises, changes to the operations and/or structure and the introduction of new products, services, technological developments that affected the procedures and controls for money laundering and terrorist financing.

(b) Information on measures taken and/or procedures introduced to comply with any amendments to the Law and AML regulatory requirements which took place during the year.

(c) Information as to the inspections and reviews performed by the AMLCO, the Internal Audit and independent third parties, identifying material deficiencies and vulnerabilities identified in the Operator's anti-money laundering and terrorist financing policies and procedures. The report shall state the significance of the deficiencies and vulnerabilities identified, the risk involved, recommendations and the action taken to rectify the situation.

(d) Information on inspections, audit and engagements with the Commission or any instructions or recommendations by the Commission, indicating any deficiencies and weaknesses identified, the risks involved as well as the corrective measures

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

and actions taken.

(e) Information on the procedures and information systems for the monitoring of the accounts and transactions of its customers by describing their main functions, including whether these are conducted in real time or after transactions, any weaknesses identified and the total number of alerts generated by the systems in place, the number of reports submitted to MOKAS as a consequence of these alerts, the number of false-positives alerts, increases/decreases in comparison with the previous year, and identified trends etc.

(f) The number of suspicious transaction cases investigated by the AMLCO but for which no report has been submitted to MOKAS.

(g) The number of internal money-laundering suspicious reports submitted by the Operator employees to the AMLCO, broken down by department. The number of reports submitted by AMLCO to MOKAS as a result of ISRs submitted by the Operator employees to AMLCO.

(h) The number of suspicious reports submitted by the AMLCO to MOKAS with information on the main reasons for suspicion and any particular trends identified.

(i) Information as to the number of high-risk customers with whom the Operator has a business relationship, country of origin and information on the policy, procedures and controls applied by the Operator in relation to high risk customers with whom it maintains a business relationship.

(j) Data for the type and size of the customer base during the last year, the number of customers per risk category, the number of persons with whom the establishment of business relationship was not allowed for compliance reasons, the number of customers with whom the business relationship was terminated, the number of frozen accounts following a court order/MOKAS and comparisons to previous years.

(k) Information on the policy, procedures and controls applied by the Operator for its compliance with sanctions and restrictive measures, as well as summary data on frozen accounts (e.g. number of frozen accounts, reasons for freezing and total amount).

(l) An overall assessment of the effectiveness of the AML/CTF systems and controls,

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

adequacy of resources and also areas likely to be equivalent to breaches of the legal and regulatory framework, describing in order of priority the actions for correction/prevention considered necessary and the expected deadline for completion.

(m) Information on the training courses/seminars attended by the AMLCO and assistant AMLCO(s) and on any other educational material received.

(n) Information on training/ seminars provided to staff during the year, reporting:

(i) The number of courses/ seminars organized/attended, their duration and summary of the content of the training

(ii) The number of employees attending, specifying their seniority i.e. management staff, officers, newcomers etc.

(iii) Employees failing the courses provided.

(iv) Names and qualifications of the instructor(s), and

(v) Specifying whether the courses/seminars were developed in-house or by an external organization /consultant

(vi) Information on the following year's training program.

(vii) Results of the assessment of the adequacy and effectiveness of staff training.

(o) Review of the structure and staffing of the AMLCO's department including recommendations for additional staff and technical resources which may be needed.

(p) Information (e.g. name, business address, business area, supervisory authority, date of commencement of business relationship, last review date, next review date, rating) on third parties or persons on whom the Operator has relied for performance of Customer Due Diligence measures and therefore has established a business relationship.

49. The AMLCO's Annual Report should be prepared within two months from the end of each calendar year (i.e. by the end of February, the latest) and should be submitted for evaluation and approval to the Board of Directors.

50. The Senior Management of the Operator shall then ensure the prompt and effective application of all appropriate measures to correct any shortcomings and/or omissions identified in the Report.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

51. The Annual Report, after its approval by the Board of Directors, is submitted to the Commission together with the minutes of the meeting, during which the Annual Report has been discussed and approved. It is provided that the said minutes include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures. These minutes and the Annual Report are submitted to the Commission within twenty days from the date of the relevant meeting, and not later than three months from the end of the calendar year.

## Internal Audit

Article 58B of the Law

52. The Operator is obliged to establish an internal audit capability to review and evaluate, on an annual basis, the effectiveness and adequacy of the policy, procedures and controls applied by the Operator for preventing money laundering and terrorist financing and to verify the level of compliance with the provisions of this Direction and the Law.

53. The internal auditor should have relevant expertise and experience of AML/CTF matters. Findings and observations of the internal auditor are submitted directly to the Board of Directors or Board Committee for evaluation and decision of the measures that should be taken and are subsequently notified to the AMLCO who takes the necessary measures to ensure the rectification of any weaknesses and omissions which have been detected by the internal auditor. The minutes of the abovementioned decision of the Board of Directors and the internal auditor's report are submitted to the Commission within twenty days from the relevant board meeting and not later than four months from the end of the calendar year.

54. The internal auditor monitors, on an ongoing basis, through progress reports, or other means the implementation of his recommendations and is directed by the Operator's Board of Directors or Board Committee. In any case, Board of Directors always remains accountable for proper implementation of recommendations of internal audit.

## Education and training of employees

55. Article 58 of the Law requires the Operator to establish adequate and appropriate systems and procedures to make their employees aware with regard to:

(a) the Operator's systems and procedures for the prevention of money laundering and terrorist financing

(b) the Law and Directives issued by the Commission

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(c) the European Union's Directives with regard to the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and

(d) relevant Data Protection requirements.

56. There is personal legal responsibility of each member of staff as regards omission to disclose information relating to money laundering and terrorist financing in accordance with the internal reporting procedures in force.

57. Staff of the Operator must be encouraged to report, without delay, matters that come to their attention in relation to transactions for which there is any suspicion that they are related to money laundering or terrorist financing. In this regard, the Operator must establish measures to ensure that staff is fully aware of their responsibilities and duties. Hence the responsibility of AMLCO in cooperation with other competent departments, to prepare and implement, on an annual basis, an education and training program for the staff.

58. The training program shall educate staff on the latest developments in AML/CTF and terrorist financing including the practical methods and trends used by criminals for this purpose. Training needs to be:

(a) Of high quality, relevant to Operator's money laundering and terrorist financing risks, business activities and up to date with latest legal and regulatory obligations

(b) Obligatory for all relevant staff

(c) Tailored to the particular roles of the staff; the training program shall have a different structure for new staff, front-line staff, compliance staff, staff moving from one department to another etc.

(d) Effective, to be checked by requiring staff to pass tests and by monitoring levels of compliance with the AML/CTF controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected

(e) Ongoing, and relevant; not be limited to when staff are hired

(f) Complemented by AML/CTF information and updates that are disseminated to relevant staff.

59. The Board of Directors and the Senior Management must be informed of their responsibilities under the Law and this Direction and changes and developments in the legal and regulatory framework. Without this, the Board of Directors and the Senior Management will not be able to provide effective management supervision, approve policies, procedures

or allocate sufficient resources for the effective prevention of money laundering and terrorist financing.

60. The AMLCO will evaluate the adequacy of the training provided and maintain detailed data regarding the seminars carried out, such as:

- Names of employees participating in the seminar/training by department and by position
- The date, title and duration of the seminar and the names of the trainers
- Whether the lecture/seminar was organised internally or offered by an external agency or consultants and
- Summary information regarding the content of the training.

61. The time and content of the training of the staff of different departments should be tailored to the needs of the staff and to the risk profile of the Operator. Moreover, the frequency of the training may vary depending on the amendments to the legal and/or regulatory requirements, introduction of new products, services or technologies, changes in the tasks of the staff as well as any other relevant changes.

62. It is important that all involved staff consistently implement the Operator's policy and procedures to prevent money laundering and terrorist financing and the promotion of a culture that understands the importance of the prevention of money laundering and terrorist financing, is the critical to the successful management of risks.

## Evaluation of integrity of employees

63. The obligation to apply appropriate policies, controls and processes that are proportionate to its nature and size, in order to mitigate and to effectively manage the risks of money laundering and financing of terrorism also relate to the recruitment and evaluation of the integrity of the employees.

64. The Operator should carry out screening of relevant employees appointed by the Operator, before and during the course of the appointment, involving an assessment of the skills, knowledge and expertise of the individual and their conduct and integrity.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

# CUSTOMER DUE DILIGENCE

## General requirements

Articles 60 – 64 of the Law

65. Customer Due Diligence is the process of obtaining and reviewing sufficient information about a customer to ascertain the level of money laundering and terrorist financing risk related to the customer's activities. This process facilitates the assignment of a risk rating to the customer and determines the appropriate level of ongoing scrutiny required.

66. The casino Operator shall apply Customer Due Diligence in any of the following cases, when:

(a) establishing a business relationship

(b) there is suspicion of money laundering and/or terrorist financing, regardless of the amount or any derogation, exemption or threshold

(c) there are doubts regarding the veracity or adequacy of documents or information previously obtained for the purposes of customer identification

(d) In situations where the Operator carries out an occasional transaction that is a transfer of funds as defined in Article 3(9) of Regulation (EU) 2015/847 with the amount of €1,000 or more, provided that the Operator is authorized to perform such transactions.

(e) The Operator must also apply Customer Due Diligence measures in relation to any transaction that amounts to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

## Application of Customer Due Diligence measures

Article 61 of the Law

67. Customer Due Diligence measures consist of:

(a) identifying the customer and verifying the customer's identity

(b) where there is a beneficial owner who is not the customer, identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the Operator is satisfied that it knows who the

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

beneficial owner is and that it understands the ownership and control structure of the customer.

(c) assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that:

(i) the transactions being conducted are consistent with the Operator's knowledge of the customer and the business and risk profile

(ii) including where necessary their source of funds and

(iii) documents, data or information held are kept up to date.

68. Where a person claims to act on behalf of a customer, the Operator shall:

(a) verify that the person is authorised to act on the customer's behalf

(b) identify the person

(c) verify the person's identity on the basis of documents or information which, in either case, is obtained from a reliable source which is independent of both the person and the customer.

69. The Operator does not need to repeat Customer Due Diligence measures if a customer visits another casino premises operated by the Operator in Cyprus, but Customer Due Diligence records held by the Operator will need to be available across the Operator's different casino premises, and the Operator's policies and procedures must include details of how the Operator will manage this.

70. The ways in which the casino Operator meets the requirements for Customer Due Diligence and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.

71. In assessing the level of risk arising in a particular case, the Operator shall consider at least the following factors:

(a) the purpose of a customer account, transaction or business relationship

(b) the amount deposited by a customer or the size of the transactions undertaken by the customer

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(c) the regularity and duration of the business relationship

72. The Operator when applying customer due diligence measures shall take into account the factors of Annex II and III of the AML Law.

73. Where the Operator identifies an increased risk of money laundering and/or terrorist financing it shall take enhanced due diligence measures. Where situations of lower risk are identified, the Operator may apply simplified due diligence measures.

74. The Operator shall be able to demonstrate to the Commission that the due diligence measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

75. Notwithstanding the provisions of Article 61(1) of the Law, the Operator may not apply due diligence measures where their implementation may constitute an offence under the provisions of Article 48 of the AML Law. In such case, the Operator shall inform MOKAS immediately.

## Timing of Customer Due Diligence measures

Article 62 of the Law

76. The Operator must comply with the requirement of the Law to perform Customer Due Diligence measures before the establishment of a business relationship or the carrying out of the transaction.

77. Despite the above, Article 62(2) of the Law allows, by way of derogation, Customer Due Diligence to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is low risk of money laundering and/or terrorist financing. In such situations these procedures shall be completed as soon as practicable after the initial contact.

78. However, Article 62(4) explicitly requires that in situations where the Operator is unable to comply with the Customer Due Diligence measures stipulated in Article 61(1)(a) to (c), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, shall terminate the business relationship, and shall consider whether under the circumstances a report should be filed with MOKAS.

## Customer relationships

79. Customer means a person that establishes a business relationship or performs an occasional transaction with the Operator, while a person is defined as both natural person and legal entity. Customers/person may be both individuals and legal entities.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

80. Consequently, within the context of a casino, a customer may be the person using the casino premises for gaming or the person that brings people and/or money or facilities to the casino for the purpose of gaming.

81. Customer relationships for AML purposes consist of three aspects:

(a) the establishment of the business relationship with the customer, requiring verification of the customer's identity (to a reasonable degree) and completion of customer due diligence

(b) the monitoring of customer activity

(c) the termination of the relationship with the customer.

82. At all stages of the relationship it is necessary to consider whether the customer is engaging in money laundering and/or terrorism financing; whether there is a need to report suspicious activity; and level of risk posed to the Operator.

## Establishment of a business relationship

83. A business relationship is a business, professional or commercial relationship between the casino Operator and a customer which is linked to the professional activities of the Operator and is expected by the Operator, at the time when the contact is established, to have an element of duration.

84. In the context of the Operator, a business relationship occurs when:

(a) a customer opens an account with the Operator

(b) a customer is introduced by a Junket operator and plays at the casino

(c) a customer applies for a credit facility at the Operator

(d) a customer sends front money to the Operator

(e) a customer uses a safety deposit box at the Operator

(f) a customer signs up for documented agreement that includes a rebate program (i.e. Premium Agreement).

85. The list above is not exhaustive, and the Operator shall consider any other situations when circumstances otherwise arise with a customer from which it expects or it could be reasonably inferred that it expects, that the relationship with the customer will have an element of duration. The Commission acknowledges that this may not necessarily be the case when the Operator permits a customer to join a casino loyalty scheme. However, the

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Operator shall determine in such cases based on materiality if the business relationship has occurred or not.

86. In case that a customer performs individual transactions with the amount of €2,000 or more, linked transactions with total amount of €2,000 or plays at the casino on a regular basis, the Operator needs to determine when the criteria for the establishment of a business relationship with the customer have been met (i.e. having an element of duration) and when it needs to perform Customer Due Diligence measures in line with Section "Customer Due Diligence" of this Direction.

## Occasional transactions

87. An occasional transaction is defined as any transaction other than a transaction which takes place in a business relationship. Therefore, any transaction that is not performed during the course of a business relationship should be considered as an occasional transaction.

88. The Operator has the obligation to establish systems and adequate controls to be able to identify the following occasional transactions:

(a) Individual transactions with the amount of €2,000 or more, for which the Operator has the obligation to perform Customer Due Diligence measures as described in Section "

(b) Customer Due Diligence" of this Direction.

(c) Linked transactions with the cumulative amount of €2,000 or more during a period of twenty-four hours from 6am until 6am of the next day1. The Operator is obliged to monitor linked transactions that are individually below the €2,000 threshold but that cumulatively meet or exceed this threshold, and in such case has the obligation to perform

(d) Customer Due Diligence measures as described in Section "Customer Due Diligence" of the present Direction.

[1] Please also check the relevant record keeping requirements – Section " Record Keeping".

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

89. The Operator should establish systems and procedures for detection of linked transactions performed by the same customer within a single casino premises.

## Business to Business relationships (including Junkets)

90. In case of business to business relationships, the Operator shall undertake appropriate Customer Due Diligence measures in line with the Section "

91. Customer Due Diligence" of this Direction before a contract is signed and before an application is submitted to the Commission (in case of Junket operators). The business relationship should be subject to ongoing Customer Due Diligence by the Operator as described in Section "

92. Customer Due Diligence" of this Direction and be monitored through the course of the relationship to ensure that money laundering and terrorist financing risks are identified and records of the monitoring kept and made available for examination by the Commission.

## Identification and verification

93. Applying Customer Due Diligence measures involves several steps. The Operator is required to identify and verify customers identities. The verification of identity requires confirming claimed identity against documents, data or information obtained from a reliable and independent source including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council2 or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities.

94. For the purposes of customer due diligence, proof of identity is satisfactory if:

(a) It is reasonably possible to establish that the customer is the person he/she claims to be and

(b) The person who examines the evidence is satisfied, that the customer is actually the person he claims to be.

---

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## Natural persons

### *Identification*

95. The identification of customers may be conducted through collecting various data, including the name, address, date of birth, place of birth, nationality, external appearance features, professional and financial background (e.g. occupation, business, name of employer, annual salary etc.), identity card information. The amount of information collected shall be in line with the materiality of risk and Operator's risk assessment of the customer.

96. The Operator shall identify the customers who are natural persons by obtaining the following information as a minimum:

(a) True name and/or names used as these are sated on the official identification documents

(b) Full permanent address, including postal code

(c) Government issued document number, issuing date and country

(d) Date and country of birth

(e) Nationality

### *Verification*

97. Information about customer identity shall then be verified through documents, data and information which come from a reliable and independent source. The acceptable method for the verification of a customer's identity is the reference to original documents which are issued by an independent and reliable source. At least one document used for verification purposes should include the customer's photo.

98. It is generally considered good practice and especially in high-risk situations, to obtain from the customer at least one document from an authoritative source that verifies the customer's full name and address or full name and date of birth with photograph and supporting documentation that verifies their name and either date of birth or address.

99. As a primary source of verification official state issued documents with photograph shall always be used or any other form of identification approved by the Commission.

100. Original documents should be examined so that, as far as reasonably practicable, forgeries are not accepted.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

101. The Operator should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, the Operator should take practical and proportionate steps available to establish whether the document offered is a forgery or otherwise false.

102. The Operator shall ensure that any documentation obtained for verification purposes is in a language that is understood by the Operator and the officers or employees carrying out the verification process. Where this is not the case, appropriate steps should be taken to ensure that the document does provide the necessary evidence to verify the customer's identity details. A translation in writing of any such document should be retained on file.

103. If satisfied that the original and genuine identification documents have been presented, the Operator should keep copies of the pages containing all relevant information which must be certified as true copies of the original documents by the Operator's employee who verified the identity of the customer.

104. The certifier should:

(a) sign and date the copy document (showing his name clearly in capitals underneath) and

(b) such certification should be evidenced by a written statement stating that: the document recorded is a true copy of the original document; the original document has been seen and verified by the certifier; and (where the document contains a photo) the photo is a true likeness of the customer.

105. The Operator may meet the obligations referenced in paragraph 102 of this Direction in electronic form as long as the following conditions are met:

(a) Full name of the Operator's employee who verified the identity of the customer and certified the document should be kept and easily retrievable.

(b) The date of the verification of the identity should be kept and easily retrievable.

(c) The certification disclaimer of the Operator's employee who verified the identity needs to be kept and needs to meet the requirement of paragraph 102(b) of this Direction.

(d) The system should not allow the possibility of amending and deleting the information collected in line with the requirements of paragraphs 93 and 94 of this Direction before the expiration of Record keeping obligations of the AML Law and AML Direction.

(e) All the above information needs to be kept in line with the Record keeping requirements of the AML Law and AML Direction.

## Legal entities

### *Identification*

106. The identification of a legal person comprises obtaining information relating to the following:

(a) The legal form of the legal entity

(b) The registered corporate name and trading name used

(c) The registered number, country and date of registration

(d) Full address of registered office

(e) Full addresses of the Head office/principal trading offices

(f) The telephone numbers and e-mail address

(g) The individuals that are duly authorised to act on behalf of the legal person (i.e. their legal representatives)

(h) The members of the board of directors

(i) The beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements

(j) The registered shareholders that act as nominees of the beneficial owners

### *Verification*

107. The verification of the identity of a legal person, comprises obtaining the following documents or documents similar to the below, depending on the jurisdiction:

(a) Memorandum and Articles of Association

(b) Certificate of Incorporation

(c) Certificate of Good Standing

(d) Certificate of Registered Address

(e) Certificate of Directors and Secretary

(f) Certificate of Registered Shareholders in the case of private companies and public companies that are not listed in a regulated market of a European

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Economic Area country or a third country with equivalent disclosure and transparency requirements

(g) In the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed

(h) Documents and data for the verification of the identity of the persons that are authorised to act on behalf the legal person, as well as the registered shareholders and beneficial owners of the legal person.

108. Where deemed necessary forming a better understanding of the activities, sources and uses of funds/assets of a legal person, the Operator obtains copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

### Unincorporated businesses, partnerships and other persons with no legal substance

*Identification*

109. The identification of unincorporated businesses, partnerships and other persons with no legal substance comprises obtaining of the following:

(a) full name

(b) business address

(c) names of all partners/principals who exercise control over the management of the partnership

(d) names of individuals who own or control over 25% of its capital or profit, or of its voting rights.

*Verification*

110. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, beneficial owners and other individuals who exercise control over the management of the partnership is verified according to the procedures set for identification and verification of natural persons. In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate is obtained and where it exists, the formal partnership agreement shall be obtained.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

111. The Operator shall obtain documentary evidence of the head office address/trading address of the business, ascertain the nature and size of its activities.

## Identification of beneficial owners

112. The Operator is required to identify the beneficial owner(s) of a customer, where applicable, and to take reasonable measures to verify the identity to ensure that the Operator is satisfied of knowing who the beneficial owner is. In the case of a customer being a body corporate, foundation, trust or similar legal arrangement, the Operator is also required to take reasonable measures to understand its customer's ownership and control structure.

113. Where the beneficial owner identified is the senior managing official, the Operator shall take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process.

114. The Operator shall collect appropriate documents for verification of ownership structure including certificates of the registered shareholders for the companies participating in the ownership structure of the customer, ownership charts etc. as well as appropriate information and documents for verification of identity of individual that are ultimate beneficial owners.

115. In the case where the Operator enters into a new business relationship with a corporate or other legal entity, or a trust or a similar legal arrangement, which are subject to the registration of beneficial ownership information pursuant to the provisions of section 61A or 61B or 61C of the Law, the Operator shall collect proof of registration or an excerpt of the beneficial ownership information held in the relevant register.

116. It is noted that the Operator is not allowed to rely solely on the information stored in the central registers of beneficial owners defined in the Law for the fulfilment of the requirements of the due diligence measures and identification of the customer's identity.

## Assessing and obtaining information on the purpose and intended nature of the business relationship

117. The Operator must assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship in order to evaluate whether the proposed business relationship is in line with the Operator's expectation and to provide the Operator with a meaningful basis for ongoing monitoring.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

118. Information that is relevant may include the following:

(a) The anticipated turnover/size of transactions and kind of wagering activities in which the customer is likely to engage

(b) The origin of funds

(c) The source and size of the customer's wealth and annual income

(d) Regularity or duration of the relationship.

## Ongoing monitoring

Article 61.1(d) of the Law

119. The Operator must conduct ongoing monitoring of its business relationships including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Operator's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

120. Moreover, Article 60(d) of the Law requires obliged entities to apply Customer Due Diligence measures when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information. Furthermore, Article 62(6) of the Law requires the application of Customer Due Diligence measures not only to new customers but also at appropriate times to existing customers, depending on the level of risk of being involved in money laundering and/or terrorist financing activities or when the relevant circumstances of a customer change, or when the Operator has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s), or if the Operator has had this duty under the Administrative Cooperation in the Field of Taxation Law.

121. The ongoing monitoring must include the following:

(a) Scrutiny of transactions undertaken throughout the course of the relationship (including where necessary the source of funds) to ensure that the transactions are consistent with the casino's knowledge of the customer, the customer's business and risk profile. All such reviews and investigations should be properly documented, and relevant records kept for in line with Record keeping requirements of the Law and this Direction.

(b) Undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying Customer Due Diligence

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

measures up-to-date.

122. The Operator needs to ensure that the arrangements it has in place are effective in monitoring customers and the accounts they hold are sufficient to manage the risks the Operator is exposed to.

123. The Operator's policies and procedures should determine the timeframes for the regular review, examination and update of the customer identification data, depending on the risk categorisation of each customer. The outcome of the review should be recorded in a separate form and be kept in the respective customer files.

124. If at any time during the business relationship with an existing customer, the Operator becomes aware that reliable or adequate Customer Due Diligence data and information are missing regarding the customer, then the Operator should take all necessary action, by applying the Customer Due Diligence measures to collect the missing data and information, the soonest possible, so as to complete the customer's profile.

125. In addition to the requirement for the regular update of the Customer Due Diligence data and information, when it is observed that unreliable or inadequate data and information or whenever there is a material event that could influence the overall customer's risk categorization or profile is being held this should be rectified. This could be inter alia:

(a) An individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions of the customer.

(b) Identification of material negative information about the customer which points to the need for an update of the data and information about the customer or to a possible risk reclassification.

(c) Any indication that the identity of the customer, or of the customer's beneficial owner, has changed.

(d) Any transactions which are not reasonably consistent with the Operator's knowledge of the customer.

(e) Any change in the purpose or intended nature of the Operator's relationship with the customer.

(f) Any other matter which could affect the Operator's assessment of the money laundering and/or terrorist financing risk in relation to the customer.

126. The details of any periodic and off-cycle reviews of customer's profile should be documented accordingly together with the rationale for making all relevant decisions and for classification of a customer into a certain risk category. The records should include the Customer Due Diligence measures taken and the reasons for continuing/terminating the business relationship and the decision maker. This information should be kept within the customer file in line with the record keeping requirements defined by the Law and this Direction.

127. The Operator's system of monitoring as a minimum shall have the following characteristics:

(a) Flags up transactions and/or activities for further examination.

(b) The transaction reports are reviewed promptly by the AMLCO and

(c) Appropriate actions are taken on the findings for any further examination.

128. Monitoring can be either:

(a) In real time, in those transactions and/or activities can be reviewed as they take place or are about to take place

(b) After the event and based on the level of AML/CTF risk, through the AMLCO's review of the transactions and/or activities that a customer has undertaken.

129. In either case, unusual transactions or activities should be flagged for further examination and details of relevant examinations and investigations properly documented and kept by the Operator.

130. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer risk.

131. The scope and complexity of the monitoring process will be influenced by the nature and structure of the Operator's business activities, and size. The key elements of any system are the ability to have current and accurate customer information from all of its casinos, on the basis of which it will be possible to identify the unusual and ask questions as to the reasons for unusual transactions or activities, in order to judge whether they are suspicious.

## Simplified (customer) Due Diligence

Article 63 of the Law

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

132. The Article 63 of the Law provides that the Operator may apply Simplified Due Diligence measures in situations where the money laundering and terrorist financing risk associated with a business relationship or occasional transaction has been assessed as low and provided that there is no suspicion that a transaction is related to money laundering and/or terrorist financing.

133. Before applying Simplified Due Diligence measures the Operator is required to ascertain that the business relationship or occasional transactions presents a low degree of risk. Simplified Due Diligence is not an exemption from any of the Customer Due Diligence measures; however, the amount, timing or type of each or all of the Customer Due Diligence measures may be varied commensurate to the low risk that has been identified.

134. Simplified Due Diligence measures may include but are not limited to:

(a) adjusting the timing of Customer Due Diligence

(b) adjusting the quantity of information obtained for identification, verification or monitoring purposes

(c) adjusting the quality or source of information obtained for identification, verification or monitoring purposes

(d) adjusting the frequency of Customer Due Diligence updates and reviews of the business relationship.

135. The Operator must make sure that this does not result in a de facto exemption from keeping Customer Due Diligence information up to date.

136. The information the Operator obtains when applying Simplified Due Diligence measures must enable the Operator to be reasonably satisfied that its assessment that the risk associated with the relationship is low is justified.

137. It must also be sufficient to give the Operator enough information about the nature of the business relationship to be able to comply with the obligation to carry out sufficient monitoring of the transactions and business relationships to enable it to detect any unusual or suspicious transactions.

138. Simplified Due Diligence does not exempt the Operator from obligation of ongoing monitoring and reporting suspicious transactions to MOKAS.

139. Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering and/or terrorist financing is being attempted or where the Operator has doubts about the veracity of the information obtained, Simplified

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Due Diligence must not be applied (i.e. where specific high-risk scenarios apply and there is an obligation to conduct Enhanced Due Diligence, Simplified Due Diligence must not be applied).

140. When assessing factors and types of evidence of potentially lower risk which relate to types of customers, geographical areas and particular products, services, transactions or delivery channels, the Operator shall take into consideration at least the relevant risk factors stipulated in Annex II of the Law as well as information provided in this Direction and any Guidelines issued by the Commission.

## Enhanced (customer) Due Diligence

Article 64 of the Law

141. The Operator must apply Enhanced Due Diligence measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. When assessing the said risks the Operator takes into account at least the factors of potentially higher risk, as set out in Annex III of the Law. Enhanced Due Diligence measures cannot be substituted for regular Customer Due Diligence measures but must be applied in addition to such Customer Due Diligence measures. Enhanced Due Diligence measures, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

142. The Enhanced Due Diligence measures must be applied:

(a) if the Operator has determined that a customer or beneficial owner is a PEP, or a family member or a close associate of a PEP

(b) in any business relationship or transaction with a customer from a high-risk third country

(c) in any business relationship with a Junket operator

(d) in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose

(e) in any other case which, by its nature or circumstances, can present a higher risk of money laundering and/or terrorist financing

143. The AMLCO should be aware of high-risk customers and act as an advisor to Senior Management before the establishment of a business relationship or performing the

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

transaction. The approval of the AMLCO is required for the reclassification of high-risk customers to a lower risk level.

### Politically Exposed Persons (PEPs)

144. Article 64 of the Law requires the Operator to apply Enhanced Due Diligence measures with respect to transactions or business relationships with PEPs. The definition of a PEP includes family members of such person and persons known to be close associates of such person.

145. With respect to transactions or business relationships with PEPs, the Operator is required to have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a PEP.

146. In cases of business relationships or transactions with PEPs, in addition to the Customer Due Diligence measures laid down above, the following Enhanced Due Diligence measures must be applied:

(a) obtain Senior Management approval for establishing/continuing business relationships with such persons or performing a transaction.

(b) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons.

(c) conduct enhanced, ongoing monitoring of those business relationships.

147. Where a PEP is no longer entrusted with a prominent public function, the Operator shall, for at least 12 months, be required to consider the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.

148. Although under the definition of a PEP an individual cease to be so regarded after he/she has left office for 12 months, the Operator should apply a risk-based approach in determining whether or when it should cease carrying out appropriately enhanced monitoring of transactions. In cases where the PEP presents a high risk of money laundering and/or terrorist financing, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately decreased.

149. The Operator's policies and procedures should include when and how customers will be checked for PEP status and how and when Senior Management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided by Senior Management.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

150. There is a hierarchy of risk for individual PEPs, where some PEPs have higher relative risk and others have lower relative risk. The measures taken for particular PEPs should therefore be informed by the relative risk attributed to the PEP, including consideration of the jurisdiction from which they originate and the position they hold.

### Unusual transactions

151. The Operator shall put in place adequate policies, procedures and systems to detect unusual transactions or patterns of transactions. The Operator shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfil at least one of the following conditions:

(a) they are complex transactions

(b) they are unusual large transactions

(c) they are conducted in an unusual pattern

(d) they do not have an apparent economic or lawful purpose

152. In particular, the Operator shall increase the degree and nature of monitoring of the business relationship in order to determine whether those transactions or activities appear suspicious. In such circumstances the Operator must apply Enhanced Due Diligence measures.

153. These Enhanced Due Diligence measures shall be sufficient to help the Operator determine whether these transactions give rise to suspicion and must at least include:

(a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business/occupation to ascertain the likelihood of the customer making such transactions and

(b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. The Operator shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

### High-risk third countries

154. With respect to business relationships or transactions involving high-risk third countries identified pursuant to Article 9(2) of the AML Law, the Operator should apply the following enhanced customer due diligence measures:

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(a) obtain additional information on the customer and the beneficial owner(s).

(b) obtain additional information on the intended nature of the business relationship.

(c) obtain additional information on the source of funds, and source of wealth of the customer and of the beneficial owner(s).

(d) obtain information on the reasons for the intended or performed transactions and their consistency with the business relationship.

(e) obtain the approval of senior management for establishing or continuing the business relationship with such person.

(f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

### Other high-risk situations

155. In all other high-risk situations, the Operator should take an informed decision about which Enhanced Due Diligence measures are appropriate for each high-risk situation. The extent of additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

156. In all cases the Enhanced Due Diligence measures must include as a minimum the following:

(a) obtaining approval by Senior Management for the commencement/continuation of a business relationship.

(b) examining the background and purpose of the transaction and taking adequate measures to ascertain the source of wealth and source of funds.

(c) systematic and thorough monitoring of the transactional behaviour of the customer.

157. In some cases, depending on the risk it may be appropriate to apply and one or more of additional Enhanced Due Diligence measures. The Operator is not required to apply all the Enhanced Due Diligence measures listed below in all cases. For example, in some high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship.

158. Additional Enhanced Due Diligence measures the Operator should apply may include:

(a) Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile.

(b) Carrying out additional searches to better inform the customer risk profile.

(c) Obtaining information about the intermediary's underlying customer base and its AML/CTF controls.

(d) Undertaking further verification procedures on the customer or beneficial owner to better understand if the customer or beneficial owner may be involved in criminal activity.

(e) Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship.

(f) Obtaining further documentary evidence for source of wealth.

(g) Obtaining further documentary evidence for source of funds.

## Cash Deposits

159. Even though the use of cash has been gradually reduced by consumers, it is still one of the common methods to launder the proceeds of crime. Almost all crime types make use of cash to facilitate money laundering and/or terrorism financing at some stage, not only traditional crimes which generate cash profits, but also threats now arising from new technologies such as crypto currencies, where cash is used as an instrument to disguise the criminal origin of proceeds.

160. It is essential that the Operator develops and applies appropriate procedures commensurate to the level of ML/TF risk, when accepting large amounts of cash and depending on the assessed risk, to carry out adequate measures in order to ascertain the source and origin of the cash where necessary.

### Article 2B of the Law

161. According to article 2B (2) (c) of the Law, in cases where a transaction or payment is carried out by a customer in cash for the amount of equal or exceeding of €10,000 or the equivalent in another foreign currency, and the customer has submitted a declaration of cash in accordance with Article 5 of the Control of Cash Entering or Leaving the European

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

Union and the Exercise of Intra-Union Controls on Cash law of 2022 (Law 63(I)/2022), a copy of the said declaration, must be submitted to the Operator pursuant to the provisions of the AML law. The Operator shall establish and implement appropriate policies, procedures, and internal controls to ensure compliance with the obligation set out in paragraph 159 of this Direction. These shall include at a minimum:

(a) Mechanisms for identifying and verifying whether incoming cash from abroad (in national or foreign currency), exceeding €10,000 was declared in accordance with Article 5 of Law 63(I)/2022.

(b) Procedures for requesting such declarations from the customers and ensuring their authenticity as well as assessing their consistency with the customer's profile and declared source of funds.

(c) Clear record-keeping requirements, including maintaining a copy of each declaration in the customer's file as per record keeping requirements of this Direction.

(d) Clearly defined escalation procedures to handle non-compliance or suspicious behaviour.

(e) Internal policies, controls, and procedures to detect and prevent instances of structuring, whereby customers may attempt to divide large cash amounts into smaller transactions to avoid the obligation to submit a cash declaration. If the Operator detects or suspects any attempt to structure transactions to evade the cash limit of €10,000 or equivalent amount in foreign currency, it must immediately file a Suspicious Transaction Report (STR) with MOKAS.

(f) Proactively informed its customers to declare cash, by placing certain mechanisms.

(g) Ensure that relevant staff receive appropriate training.

### Information Collection During Registration and Subsequent Transactions

162. The Operator shall ensure that, during the registration process, the customer is clearly requested to disclose whether any funds they intend to use are coming from abroad and, if so, whether these funds have been declared to Customs upon entry into Cyprus. In cases where the funds are confirmed to have been declared to Customs, the relevant copy of the declaration shall be obtained and retained by the Operator.

163. In instances where the €10,000 threshold is reached during a subsequent visit to the Operator's premises following initial registration, the Operator shall repeat the request

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

for the above information and, where applicable, collect the Customs declaration at that point.

164. This obligation shall apply to any transaction by any natural person of amount equal or above €10,000 or the equivalent in another foreign currency - whether the transaction is executed in a single operation or in several operations which appear to be linked.

### Integration and Internal Control Procedures

165. The Operator shall integrate the obligation to obtain and assess cash declarations into its Customer Risk Assessment and Customer Due Diligence Standard Operating Procedures (SOP) to ensure (i) that the risk associated with the scenarios listed in paragraph 165 are appropriately captured in the CRA tool and assessed accordingly (ii) detection of undeclared or suspicious cash transactions.

166. All relevant operational SOPs, including the Cage SOP, must be updated to reflect these requirements, especially where high volumes of cash are processed.

167. The procedures must clearly define actions to be taken when a customer, amongst others:

(a) Refuses or fails to provide a required customs declaration in circumstances where such a declaration is expected under applicable legislation and after being informed by the Operator.
(b) Provides false, inconsistent, or altered information or Customs Cash Declaration.
(c) Claims domestic origin of funds but does not provide adequate supporting evidence.

168. In such cases, the Operator shall follow its risk-based escalation process, which may include referral to the AMLCO, application of Enhanced Due Diligence (EDD), and submission of a Suspicious Transaction Report (STR) to MOKAS, as appropriate.

169. The Operator's Customer Risk Assessment (CRA) tool must be enhanced in order to be capable of triggering elevated scores on response to repeated non-compliance, refusal to cooperate, provision of questionable explanations or other behaviour indicating higher ML/TF risk. The Operator is expected to amend its CRA/ CDD SOP to ensure that these specific risk factors are recognised, and that appropriate weighting is given to them.

### Record-Keeping Requirements

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

170. The Operator shall maintain a centralised record of all customers interactions and subsequent cash declarations received and ensure that details such as origin and intended use of the cash transportation details (such as means of transport, departure country, arrival date), customer identifiers, and dates of submission i.e. date of submission to the Operator and date of declaration to Customs Department are properly maintained. These records shall be retained in accordance with the AML Law and this Direction's record keeping requirements and be made available to the Commission upon request.

171. Additionally, the Operator shall maintain documented evidence confirming that the customer was previously informed of the obligation to submit a customs cash declaration. This communication must be clearly documented in the customer's file, including the date, content of the notification, and any customer response.

172. Documented proof of such communication shall be retained and used, where necessary, to demonstrate regulatory compliance.

### Risk-Based Escalation Procedures

173. The Operator shall establish and implement a formal escalation policy, as part of its internal AML framework, that sets out at least the steps to be taken for the scenarios outlined in paragraph 165.

174. The Operator shall ensure that its internal procedures include a tiered and proportionate escalation framework which allows for the appropriate handling of such cases based on the specific risk factors identified. While the exact escalation steps may vary depending on the circumstances, the framework should be designed to reflect the seriousness of repeated non-compliance or intentional evasion, and to escalate promptly where behaviour suggests increased risk.

175. Where an incident occurs for the first time and no additional risk indicators are present, an immediate escalation to AMLCO might not be required, however if further incidents occur, or if other risk indicators are identified, the case must be escalated to the AMLCO.

176. Where a customer repeatedly or deliberately fails to comply, with the obligation to submit a customs cash declaration, or where the customer's behaviour suggests an attempt to circumvent reporting obligations, the Operator must treat the case as a matter of significant concern from a ML/TF risk perspective and the case must be escalated immediately to the AMLCO for further assessment and appropriate action. It is noted that a repetitive failure is defined as an incident occurring subsequent to the initial failure.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

177. The AMLCO shall assess each escalated case in light of the overall customer profile and determine the appropriate course of action based on the nature and severity of the risks involved. Depending on the circumstances, this may include the application of one or more Enhanced Due Diligence (EDD) measures, such as:

(a) Verification of the customer's source of funds (SoF) and source of wealth (SoW).

(b) Enhanced monitoring of the customer's transaction activity.

(c) Temporary restriction or suspension of the customer's ability to carry out further cash transactions or gaming activity until the matter is resolved.

It is noted that the list of the abovementioned EDD measures is not exhaustive.

### Handling / Escalation process for claimed domestically originated funds

178. Where a customer claims that the funds were not declared because they domestically originated, the Operator must verify this claim by requesting appropriate supporting documentation. Verification of the claimed domestic origin of funds must be conducted on a risk-based basis, taking into account a range of factors including the customer's overall risk profile, the amount and frequency of cash activity, transactional history, and the plausibility of the explanation provided.

179. The Operator must ensure that its internal procedures and controls do not establish or rely on high materiality thresholds that could result in potentially high-risk cases being excluded from review. In particular, the Commission considers that thresholds used for triggering verification of claimed domestic origin must be proportionate and aligned with the €10,000 threshold established under Article 5 of Law 63(I)/2022 for cash declarations.

In the absence of such documentation, or where the explanation lacks credibility, the matter shall be escalated to the AMLCO for further review. The AMLCO shall assess the case and determine the appropriate course of action based on the level of risk identified. Depending on the circumstances, this may include the application of Enhanced Due Diligence (EDD) measures as mentioned in paragraph 174.

### Reporting obligations to MOKAS

180. Where the facts and circumstances give rise to reasonable grounds for suspicion of money laundering or other criminal activity, the AMLCO shall also assess whether the cases outlined in this section, warrants the submission of a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) to MOKAS, in accordance with the AML Law and this Direction.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

### Customer Awareness and Staff Training

181. The Operator shall ensure that relevant staff receive appropriate training on the obligations arising from both the national and European Union legal frameworks on cash controls. This training shall include, inter alia, an understanding of:

(a) The Operator's obligation to obtain and retain cash declarations under Article 2B of the AML Law.

(b) The customer's obligation to declare cash pursuant to Article 5 of Law 63(I)/2022 and Regulation (EU) 2018/1672.

(c) Indicators /scenarios that a declaration may be required or may have been made.

(d) The steps to be taken when a declaration is submitted by a customer; and

(e) The potential consequences of non-compliance by the customer.

182. The Operator should proactively inform its customers of their legal obligation to declare cash when entering or leaving the country and their duty to provide this declaration, by placing certain mechanisms to ensure that:

(a) Pre-arrival communication is conducted in advance, when deemed applicable, with customers such HVPs or Junket / Agent customers.

(b) Proper training of Junkets and Agents is conducted.

(c) Reference to Cash Declarations obligations in Certificates of Winnings.

(d) Customer Awareness obligation during the on-boarding process.

It is noted that the obligation for obtaining the cash declaration relates to all customers, regardless of the risk categorisation, who fall within the obligation under Article 5 of the of Law 63(I)/2022.

### Certificate of Winnings

183. The Operator should establish mechanisms to ensure that the customer's obligation to declare cash leaving the country is clearly stated in the Certificate of Winnings, if this is requested to be issued by the customer i.e. via a standardised note or clause. In addition, the Operator shall comply with the relevant requirements set forth in the Commission's Direction for the Issuance of Certificate of Winnings.

## Cashing out

184. The Operator should implement adequate controls, taking into account its assessment of risk, to ensure that the customers are cashing out chips or Ticket in, ticket out' ("TITO") tickets derived from their buy-in and gaming activity at the casino, and keep relevant records as evidence. It is noted that the relevant controls should be carried out in real-time i.e., at the time when the transaction in question occurs.

## Reliance on third parties

Article 67 of the Law

*General requirements*

185. Article 67 of the Law allows the obliged entities to rely on third parties for the implementation of Customer Due Diligence measures, as these are prescribed in Article 61(1)(a),(b),(c) of the Law.

186. The Law explicitly states that the ultimate responsibility for performing the above-mentioned measures remains with the Operator if relying on a third party. The responsibility to apply Customer Due Diligence measures cannot be delegated to the third party.

187. Based on the Law the third parties are defined as:

(c) Obliged entities referred to in paragraphs (a), (b), (c) and (d) of subparagraph (1) of Article 2A of the Law (credit institutions, financial institutions, auditors, external accountants and tax advisers, independent legal professionals, trust or company service providers)

(d) Other institutions or entities located in the Member States or in a third country, which:

(i) Apply Customer Due Diligence measures and keep records at the same level with those established by the EU Directive and

(ii) Are subject to supervision which is at the same level as relevant requirements of EU Directive.

188. A Junket operator is not an obliged entity under the Law, nor can it be considered a third party as above. The Operator may not rely on Customer Due Diligence performed by a Junket operator.

189. Further, the Operator may not rely on due diligence measures of a third party established in a high-risk third country.

190. The Operator shall request from the third party to:

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(a) Make immediately available data, information and documents obtained as a result of the application of the Customer Due Diligence measures in accordance with the requirements of the Law and

(b) Forward immediately, upon request, to the Operator, relevant copies of identification and verification data, including, where available, data obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities of Cyprus.

191. The Operator's relationship with a third party needs to be based on a written agreement in which the obligations of every party for the offering of relevant services are specified, including the financial terms. Customer Due Diligence measures need to be applied by the Operator on the third party before the business relationship commences.

*Procedures for verification of suitability of a third party*

192. The AMLCO has the responsibility to verify and properly document that any agreed third party fulfils the criteria specified in this Direction.

193. The AMLCO should maintain a separate file with the information on the identity of any third party, including the economic and risk profile of the third party, minutes of the meetings with third party and information that verifies that the third party fulfils the criteria of a third party as defined in this Direction.

194. The AMLCO should maintain a register with the following information relating to the third party with which the Operator has or used to have a business relationship:

(a) Name

(b) Business address

(c) Professional activity sector

(d) Supervisory authority

(e) Date of commencement of business relationship

(f) Date of latest evaluation

(g) Date of next evaluation

(h) Number of the customers introduced to the Operator per year

(i) Number of customers reported to MOKAS

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

(j) Date and reason for termination of business relationship, if applicable.

195. The commencement of the business relationship with the third party must bear the written and duly justified approval of the AMLCO and must be kept in the individual record file of the third party maintained by the Operator.

196. The AMLCO should maintain a register with the following information on the third party with which a business relationship proposal was rejected:

(a) Name

(b) Business address

(c) Professional activity sector

(d) Supervisory Authority

(e) Date of rejection

(f) Reasons for rejection

197. The Operator may rely on third parties as defined in Article 67 of the Law only at the outset of establishing a business relationship with the customer for the purpose of performing initial Customer Due Diligence measures. Any additional data and information for the purpose of updating the customer's information during the course of business relationship and/or examining unusual transactions needs to be obtained directly from the customer.

## Transactions and products that favour anonymity

Article 66(3) of the Law

198. The Law requires the Operator to pay special attention to every threat or danger for money laundering and/or terrorist financing which may result from products or transactions which may favour anonymity. The Operator is required to take measures, to prevent the use of products and services that may favour anonymity for money laundering and terrorist financing activities.

199. The Operator is also required to establish and apply reasonable measures and procedures to identify the risks arising from technological developments and new financial products.

## Prohibition of opening or maintaining anonymous or numbered accounts

Article 66(2) of the Law

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

200. It is prohibited for the Operator to open or maintain anonymous or numbered accounts or accounts in names other than those stated in customers' official identity documents. Maintaining anonymous safety deposit boxes is also prohibited.

201. The Operator shall take appropriate measures to identify and assess the risks of money laundering and terrorist financing before promoting any new technology, service or product thereof.

202. The Operator when carrying financial or other business activities shall pay special attention to every threat or danger for money laundering and/or terrorist financing which may result from products or transactions which may favour anonymity, shall take measures, if needed, to prevent their use for such activities and to apply to the extent possible reasonable measures and procedures to face the dangers arising from technological developments and new financial products.

203. The Operator is not allowed to engage in crypto assets activities. In case the Operator wishes to engage in crypto assets activities, it should first obtain approval from the Commission.

## Requirements to cease transactions or terminate relationship

Article 62(4) of the Law

204. Where the Operator is unable to apply the required Customer Due Diligence measures in relation to a particular customer, the Operator shall:

(a) not carry out a transaction with or for the customer through a bank account

(b) not establish a business relationship or carry out a transaction with the customer

(c) depending on the case, terminate any existing business relationship with the customer

(d) consider whether it is required to make a report to MOKAS.

205. The Operator must have clear policies in place on how it will manage situations where it is unable to apply the Customer Due Diligence measures.

## Safety deposit boxes

206. In the case that the Operator offers safety deposit boxes to its customers, it should ensure that in such cases Customer Due Diligence measures are always applied.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

# RECORD KEEPING & DATA PROTECTION

## General requirements

Article 68 of the Law

207. Data and information collected to meet the requirements of the Law and this Direction and the Operator's compliance program should be accurate, easy to retrieve and retained in line with the requirements defined by the Law and this Direction.

208. The Operator is required to keep the following documents and information, for a period of 6 (six) years after the end of business relationship with the customer or after the date of the occasional transaction:

(a) A copy of the documents and information required in order to comply with the due diligence requirements, as defined in the Law and this Direction including, where available, data obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014, and in the Law on the implementation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authority.

(b) Supporting evidence and records of transactions that are necessary for identification of transactions.

(c) Relevant correspondence with the customers and other persons with which it keeps a business relationship.

(d) Any other records that are necessary to demonstrate compliance with the obligations under the Law and this Direction.

209. As per the AML Law, the Operator is also required to obtain and retain adequate, accurate and up-to date records about its beneficial ownership, including the details of the rights held by its beneficial owners as per the provisions stipulated in Article 61A of the Law.

210. The Operator needs to ensure that it is able to link Customer Due Diligence information for a particular customer to the transactions that the customer conducts at the casino and that this information is retained for a period of six (6) years. The Operator needs to ensure that transactional information always includes at least the calendar date and time of the transaction.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

211. In relation to the evidence of a customer's identity, the Operator must keep a copy of any documents or information obtained to satisfy the Customer Due Diligence measures required under the Law and this Direction.

212. The Operator has the obligation to apply systems which make possible the timely response to enquiries of MOKAS or the Commission as to whether it keeps or has kept during the last six (6) years a business relationship or has performed occasional transactions with specific persons and the type of this business relationship. The Operator needs to ensure that all the documents are made available in a timely manner and without delay to MOKAS and the Commission for the purpose of performing their duties by the Law. The data and documents relevant to ongoing investigations are kept until MOKAS confirms that the investigation has been completed and the case has been closed.

213. Article 47 of the Law provides that where relevant information is contained in a computer, the information must be presented in a visible and legible form which can be used in a straightforward manner by MOKAS.

214. MOKAS needs to be able to compile a satisfactory audit trail of illicit money and be able to establish the business profile of any account and customer under investigation. The Commission may also in certain circumstances need to obtain detailed information regarding customer's activity at the Operator.

215. To satisfy this requirement, the Operator must ensure, it will be able to provide the following information:

(a) the identity of the person undertaking the transaction

(b) the identity of the actual owners/beneficiaries if any

(c) information on connected persons/transactions if any

(d) information on the source of money

(e) the form in which the funds were placed and withdrawn i.e. cash, cheques, funds transfers etc., exact value of the funds placed and withdrawn (buy in and buy out) and exact value of winnings

(f) the type and amount of the currency involved

(g) the type, identifying number, calendar date and time of any transaction performed by the customer.

216. Where documents verifying the identity of a customer are held in one licensed casino premises within the Operator in Cyprus, they do not also need to be held in duplicate

form in another licensed casino premises of the Operator in Cyprus. It is sufficient for the Operator to undertake identification and verification providing that the information is available to each premises or site. The records need to be accessible to all premises that have contact with the customer, the AMLCO and law enforcement.

217. The copies of the customer identification evidence must be certified by the Operator's employee who verifies the identity of the customer. The aforementioned certification for customers who are natural persons should be done in line with the requirements of this Direction provided in Section "Identification and verification" of this Direction. In the case of customers who are natural persons introduced by the third person, it should bear the stamp of the third person to whom the Operator relies for the purpose of verifying the identity of the customer.

218. In case of business relationships with legal entities, the original documents should be obtained. However, after having seen the original documents, the Operator may maintain true copies of the said documents in the customer file. The said copies must be certified by an employee of the Operator, bear the name of the employee, the signature of the employee who certifies the documents as well as the date of the certification.

## Supporting records (gaming machines)

219. TITO and 'smart card' technology means that machines produce supporting records that can be attributed to a customer who falls within the record keeping requirements, in which case such records must be retained in accordance with the Law and this Direction.

## Data Protection

220. Article 70B of the Law provides that the processing of personal data carried out under the provisions of the Law is subject to the provisions of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data and Regulation (EU) 2016/679 (General Data Protection Regulation) ("the GDPR"). Personal data must be processed by the Operator only for the purposes of the provisions of the Law and not for any other incompatible processing purpose. The processing of personal data for purposes other than those provided for by Law, such as commercial purposes, is prohibited.

221. The Operator must provide its new customers with the information required under Article 13 of Regulation (EU) 2016/679, prior to the commencement of a business relationship or the execution of an occasional transaction.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

222. The Operator should provide information to their new customers before commencing the business relationship or executing an occasional transaction about the processing of personal data under the provisions of the Law for the purpose of preventing money laundering and terrorist financing.

223. Pursuant to Article 23 of Regulation (EU) 2016/679 on the protection of personal data, the Law removes the data subject's right of access to personal data relating to him or her and the processing to which they are subjected in the following cases:

224. For the purpose of the proper fulfilment of the duties of the Operator and supervisory authorities, including the Commission, as they derive from the Law

225. In order not to obstruct the conduct of official or legal investigations, analysis or procedures for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and financing of terrorism are not jeopardised.

226. The processing of personal data under the provisions of the Law in order to prevent money laundering and terrorist financing is considered a matter of public interest in accordance with the provisions of Regulation (EU) 2016/679 (General Data Protection Regulation).

227. All information held by the Operator in order to comply with its obligations must be secure and accessibility should be limited to those approved by the AMLCO and responsible AML Director. AML/CTF records accessed must identify the person accessing them and include the time, date and reason.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

# SUSPICIOUS ACTIVITIES AND REPORTING

## Internal reporting

Articles 26, 27, 59 and 69 of the Law

228. In accordance with the Law, all obliged entities, including the Operator, should implement internal reporting procedures enabling all employees to report and disclose any information or other matter that creates reasonable suspicions of money laundering and terrorist financing.

229. For the purposes of complying with the requirements set out in the Law and this Direction, the Commission released a Guidance for Suspicious Activity Reporting (click here to access the document), hereinafter referred to as the "Guidance", providing additional insight on the subject.

230. Under Article 27 of the Law, it is an offence for any person who knows or reasonably suspects that another person is engaged in money laundering and/or financing of terrorism, and not to report to MOKAS this information, as soon as is reasonably practical, after it comes to their attention.

231. It is important that the Operator's AMLCO maintains staff's awareness of the money laundering and terrorist financing typologies as well as of red flags. A list containing examples (red-flags) of what might constitute suspicious transactions/activities related to money laundering and terrorist financing can be found in the Guidance. The said list is not exhaustive nor includes all types of transactions that may be used, nevertheless it can assist the Operator and its employees in recognizing the main methods used for money laundering and terrorist financing. This knowledge will assist in interpreting what is being seen or reported and should be included within the training provided to staff.

232. In the case of Operator's employees, Article 26 of the Law recognises that internal reporting to the AMLCO will satisfy the reporting requirement imposed by virtue of Article 27 of the Law. This means that once the Operator's employee has reported their suspicion to the AMLCO, they are considered to have fully satisfied their statutory requirements, under Article 27 of the Law.

233. The Operator shall ensure that its employees are aware of their legal obligations and know the person (i.e. the AMLCO) to whom they should report money laundering and/or terrorist financing knowledge or suspicion. Internal reports to AMLCO and reports made by AMLCO to MOKAS, must be made as soon as is practicable.

234. In accordance with Article 69B of the Law, the Operator must provide protection against any threat or hostile action or any exposure to threats or hostile acts and in particular from adverse or discriminatory actions at the workplace towards a person who submits an internal report or a report to MOKAS for suspicious transactions under the provisions of Article 69 of the Law.

235. All suspicions reported to the AMLCO should be documented or electronically recorded. Internal reports are to be submitted in writing (manually or in electronic format), preferably using a standard template, together with all relevant information and documentation available to the employee to assist the AMLCO in making a determination as to how best to proceed. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion of money laundering and/or terrorist financing. All internal enquiries made in relation to the report should also be documented or electronically recorded.

236. All of the "Internal Money Laundering Suspicion Reports" must be registered and maintained in a secure and separate file by the AMLCO.

## Evaluation and determination by the AMLCO

237. The Law provides that the Operator's AMLCO must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The Operator must permit the AMLCO to have access to any information, including Customer Due Diligence information, in the Operator's possession that could be relevant. The AMLCO may also require further information to be obtained from the customer if necessary.

238. If the AMLCO decides not to make a report to MOKAS, the reasons for not doing so should be clearly documented or electronically recorded and retained. The Operator must have regard to the secure storage and access protocols of these records that should be kept securely and separately by the AMLCO.

## External reporting to MOKAS

Article 69 and 70

239. The AMLCO must report to MOKAS for any transaction or activity that, after their evaluation, they know or suspect that may be linked to money laundering and/or terrorist financing. The obligation to report to MOKAS includes also any attempt to carry out suspicious transactions. Report must be made as soon as is practicable after information

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

comes to the AMLCO and the AMLCO performs their evaluation. The AMLCO has the responsibility to keep records of all reports made to MOKAS.

240. Having submitted a report to MOKAS, the Operator needs to consider if the relationship with the customer needs to be terminated or not. Decision needs to be properly documented and retained. In such an event, the Operator should exercise particular caution, as per Article 48 of the Law, not to alert the customer concerned that a disclosure report has been filed with MOKAS.

241. If once a report is filed the Operator decides to maintain the business relationship with the customer who is the subject of the report, the Operator should:

(a) classify the customer as a high-risk customer; and

(b) monitor the activities of that customer to a larger extent. In such circumstances, the Operator should not automatically report to MOKAS every transaction carried out by that customer after the report has been filed. The Operator should analyse the circumstances of the case and where necessary consider passing on additional information to MOKAS.

242. After submitting the report to MOKAS, the Operator should adhere to any instructions given by MOKAS.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## WHISTLEBLOWING

243. In addition to the procedures outlined in the section pertaining to the reporting of suspicious transactions, under Article 59 of the Law, the Operator shall also have in place appropriate procedures for its employees, or persons in a comparable position, to report breaches of the Law or this Direction internally through a specific, independent and anonymous channel, proportionate to its nature and size.

244. In the case of Operator's employees, prior to making an internal report, they shall consider whether the information they are seeking to disclose should be reported internally to the AMLCO by making use of the internal reporting procedures maintained by the Operator to report knowledge or suspicion of money laundering and terrorist financing.

245. Individuals, including an employee and representative of the Operator, who report suspicions of money laundering and/or terrorist financing internally or to MOKAS, are legally protected from being exposed to threats, retaliation, or hostile actions, in particular from adverse or discriminatory employment actions.

246. Individuals who are exposed to threats, retaliatory or hostile actions, or adverse or discriminatory employment actions for reporting suspicions of money laundering and/or terrorist financing internally or to MOKAS are entitled to present a complaint in a safe manner to the Commission. Without prejudice to the confidentiality of information gathered by MOKAS, such individuals have the right to an effective remedy to safeguard their rights under this paragraph.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## FINANCIAL SANCTIONS

247. As Member State of the United Nations (UN) and the European Union (EU), the Republic of Cyprus has an obligation to enforce/implement:

(a) International Sanctions adopted by the Security Council under chapter VII of the UN Charter and

(b) Restrictive Measures adopted by the Council of the EU via relevant Decisions and Regulations, within the framework of Common Foreign and Security Policy (CFSP).

248. Under the Article 3(1) of the Implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and of the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law 58(I) of 2016, the Commission has been established as competent authority for ensuring the implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and of the Decisions and Regulations of the Council of the European Union (Restrictive Measures) within the casino gaming sector in the Republic of Cyprus.

249. Article 23 of the Anti-Terrorism Law of 2019 75(I)/2019 requires that the Operator as an obliged entity as defined in Article 2A of the Law, freeze all funds, financial assets and financial resources belonging to or controlled by a designated person or entity, owned or controlled in whole or in part, directly or indirectly, by a designated person or entity, derive or stem from funds or other assets owned or controlled, directly or indirectly, by a designated person or entity, owned or controlled by a person or entity, acting on behalf of, or following instructions by a designated person or entity.

250. In case that the Operator discovers that it is in possession or control of or is otherwise dealing with the funds or economic resources of a designated person, the Operator needs:

(a) To freeze the assets immediately

(b) Not deal with them or make them available to or for the benefit of the designated person

(c) Report to the Commission.

251. According to Article 24 of the Law 75(I)/2019, the Operator as an obliged entity must report to the Commission as their Supervisory Authority, who will, in turn, report to

the Ministry of Foreign Affairs, any assets that have been frozen or any action taken in relation to compliance with the restrictive measures of the European Union and the sanctions of the Security Council of the United Nations, as referred to in Article 25 of Law 75(I)/2019. If the Operator fails to comply with the provisions of Article 24 or Article 23 of the Law 75(I)/2019 then the Commission may take the measures as provided for in section 59(6) of the Law.

252. The Operator should identify and assess the sanctions risks to which it is exposed and implement a sanctions screening program in line with its nature, size and complexity. Sanction screening is a control used to detect, prevent and manage sanctions risk. Systems should be in place to detect newly designated sanctioned individuals and to prevent dissipation of assets.

253. The Operator should consider the likelihood of sanctioned persons using its facilities, considering local demographics and its customer base including matters such as jurisdiction where it is operating and its proximity to sanctioned countries, locations where the customers are resident/based, jurisdictions where they perform business activities etc. The Operator should also take appropriate measures to mitigate these risks.

254. The Operators AML/CTF program should include a sanctions screening program that comprises screening policies, procedures and controls to monitor financial transactions preventing breaches of the financial restrictions legislation. The Operator should refer to the current versions of the legislation imposing the specific financial sanctions to understand exactly what is prohibited.

255. The sanctions screening program created in line with the AML/CTF program should include:

(a) Policies and Procedures: Outlining the requirements as to when screening needs to be done and at which frequency, how alerts should be handled and especially how to deal with the alerts if not enough information is available.

(b) Responsible person: Potential sanctions matches should be reviewed by person with appropriate skills and experience. The staff should be properly trained to know how to deal with potential sanctions matches.

(c) Risk Assessment: Risk-based approach should be applied to decision making regarding the set-up of sanctions screening program and this needs to be clearly documented.

(d) Internal controls: It is necessary to document how the screening system is

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

configured in order to demonstrate that it is reasonably expected to manage specific sanctions risk.

CYPRUS GAMING & CASINO SUPERVISION COMMISSION

## SUBMISSION OF DATA AND INFORMATION

Article 59(9) of the Law

256. According to Article 59(9) of the Law the Commission may request and collect from persons subject to its supervision information necessary or useful for the performance of its functions and request within a specified deadline the provision of information, data and documents. In case of refusal of any person under its supervision to comply with its request for the provision of information within the specified deadline or if the person refuses to give any information or demonstrates or provides incomplete or false or manipulated information, the Commission has the power to impose an administrative fine in accordance with the provisions of subsection 6 of the above Article.

257. The AMLCO is responsible for submission of regular and ad hoc reports to the Commission as requested by the latter from time to time.

Harris Tsangarides

Harris Tsangarides
Chief Executive Officer