NATIONAL BETTING AUTHORITY

**CONSULTATION DOCUMENT**

on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing in accordance with the Directive (EU) 2015/849 of the European Parliament and the Council of 20 May 2015.

## 1. Contents

# 1. INTRODUCTION

## 1.1. Money Laundering

1.1.1. Money laundering and the financing of terrorism is perhaps one of the most serious problems facing every country. For the immediate remediation of such issue targeted and proportional prevention of the use of the financial system for the purposes of money laundering and terrorist financing is indispensable.

1.1.2. This can be achieved by using the procedures and controls that can be implemented by each company and their employees, but also at the Member States level.

1.1.3. The risk for money laundering is increased in the field of gaming. In order to mitigate the risk, providers of gambling services should establish customer due diligence measures.

## 1.2. The role of the National Betting Authority

1.2.1. According to the Betting law of 2012, within the competence of the National Betting Authority (hereinafter the "authority"), is the adoption of directives to the gambling service providers (licensed Class A or B bookmakers and authorized representatives and licensees of premises), for the implementation of preventive measures for the prevention of money laundering, as well as their supervision, in order to verify that these instructions apply.

## 1.3. The Purpose of this Consultation Document

1.3.1. This document defines the requirements for the licensed Class A and B bookmakers, as well as licensed authorized representatives. These obligations will enter into force by virtue of the transposition into Cyprus law of 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 purposes of money laundering or terrorist financing (hereinafter the "4th directive ').

1.3.2. The proposals that will be submitted by stakeholders will be used for the formulation of the Directive to be issued by the Authority on the prevention of the use of the financial system for money laundering and the financing of terrorism.

1.3.3. The purpose of this document is to provide a general explanation of the basic obligations to combat money laundering and terrorist financing, as well as a general framework on how it is expected that licensees of existing Class A and B bookmakers, authorised representatives, as well as all the parties will comply with the specific obligations. This document will form the basis for the adoption of a more detailed sector-specific guidance document that will be issued at a later stage, after the adoption of the Directive of the Authority.

1.3.4. The document covers 11 main areas, each of which corresponds to what is considered by the NBA as being the main AML/CFT obligations of subject persons.

1.3.5. This document does not cover all AML/CFT obligations and the omission of any reference to other AML/CFT obligations is not to be considered as tantamount to the inapplicability of the same.

1.3.6. Licensees are strongly encouraged to read this document and consider all proposals with attention and respond within due course as predetermined below.

1.3.7. It is important for Licensees and other interested parties to note that the current document consists only of proposals and its role is clearly informative. Accordingly, the Authority is not bound by the contents of the present document which is subject to changes and revisions following any feedback received from Licensees and other interested parties.

1.3.8. This document, together with the feedback received, will form the basis for the adoption of the Directive and sector-specific guidance to be issued by the Authority.

1.3.9. Licensees and other interested parties are invited to submit any feedback they may have in relation to this document on the email address directives@nba.gov.cy until the 16 February 2018.

## 1.4 Definitions as per the 4th Directive and other useful definitions

**1.4.1.** **'Gambling services'**: means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;

**1.4.2.** **"Bet"** means any type of bet carried out on sporting or other events by a number of natural persons who participate in the same, under the condition that the winnings of every player are determined by the person organising the bet, prior to or at the time of processing the bet, with reference, not only to the amount each player has paid for his participation in the bet, but also with regard to the fixed yield of the particular bet and which is carried out following a licence for a Class A or B bet, as established in the present Law;

**1.4.3.** **'Transaction'** : 'Transaction' consists of the wagering of a stake, including:

- the purchase from, or exchange with, the casino of tokens for use in gambling at the casino
- payment for the use of gaming machines
- the deposit of funds/payment required to take part in lottery or betting,
- the deposit of funds required to take part in remote gambling, or
- the collection of winnings, including the withdrawal of funds deposited to take part in remote gambling or winnings arising from the staking of such funds

**1.4.4.** **'Obliged entities'** as per the 4AMLD are providers of gambling services. Obliged entities for the requirements of this Directive are the Licensees, Bookmakers of Class A & Class B and their Authorised Representatives.

**1.4.5.** **'Business Relationship'** means a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration;

**1.4.6.** **'Customer'** in this document means the customer that bets in licensed betting company.

## 1.5 Proposed areas for Consultation Purposes

1.5.1. The National Betting Authority has put forward the following areas for discussion in this consultation paper, to be directed to the licensees and other stakeholders of the Gaming Sector. These areas cover some of the primary obligations of Licensees and Subject persons and is not an exhaustive list of all obligations needed to be fulfilled:

i. Customer Due diligence (CDD)
ii. Customer Due Diligence Threshold (CDDT)
iii. Know Your Customer (KYC) Requirements
iv. Risk assessment and Risk Based approach
v. Politically Exposed Persons (PEPs)
vi. Compliance Officer
vii. Training
viii. Beneficial Ownership
ix. Transaction Monitoring
x. Reporting Suspicious Transactions
xi. Record and deletion of data

## 1.6 Consultation Question

Q1. Are there any issues that arise from this part and for which you would like some further explanations or would you like to make a comment?

## 2. CUSTOMER DUE DILIGENCE (CDD)

### 2.1. 4th Directive Requirements

2.1.1. Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:

a) when establishing a business relationship;
b) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

2.1.2. Customer due diligence measures shall comprise:

a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
c) assessing and, as 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 the transactions being conducted are consistent with the obliged entity'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.

2.1.3. However, obliged entities may determine the extent of such measures on a risk-sensitive basis.

2.1.4. Member States shall require that verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

2.1.5. By way of derogation from paragraph 2.1.4., Member States may allow verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist

financing. In such situations, those procedures shall be completed as soon as practicable after initial contact and before the next transaction takes place.

2.1.6. Member States shall require that, where an obliged entity is unable to comply with the customer due diligence it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the FIU in relation to the customer.

2.1.7. Member States shall require that obliged entities apply the customer due diligence measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

2.1.8. **Simplified customer due diligence**

2.1.8.1. Where a Member State or an obliged entity identifies areas of lower risk, that Member State may allow obliged entities to apply simplified customer due diligence measures.

2.1.8.2. Before applying simplified customer due diligence measures, obliged entities shall ascertain that the business relationship or the transaction presents a lower degree of risk.

2.1.8.3. Member States shall ensure that obliged entities carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

2.1.9. **Enhanced customer due diligence**

2.1.9.1. In the cases referred to in Articles 19 to 24 of the Directive and explained here below and when dealing with natural persons or legal entities established in the third countries identified by the European Commission as high-risk third countries, as well as in other cases of higher risk that are identified by Member States or obliged entities, such as transactions with Politically Exposed Persons, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

2.1.9.2. Member States shall ensure that those cases are handled by obliged entities by using a risk-based approach.

2.1.9.3. Member States shall require obliged entities to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious. Specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down.

2.1.9.4. With respect to transactions or business relationships with politically exposed persons, Member States shall, in addition to the customer due diligence measures require obliged entities to:

a) 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 politically exposed person;
b) apply the following measures in cases of business relationships with politically exposed persons:
   - obtain senior management approval for establishing or continuing business relationships with such persons;
   - take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
   - conduct enhanced, ongoing monitoring of those business relationships.

## 2.2. Explanation of the Directive Requirements

2.2.1. **<u>Customer Due Diligence (CDD)</u>**

2.2.1.1. CDD should be exercised by:

a) Class A bookmaker towards its licenced authorised representative or/and the responsible person
b) Obliged entities (Class A and B bookmakers and authorised representatives) towards their customer

2.2.2. **<u>CDD to be exercised by Class A bookmaker towards its licenced representative</u>**

2.2.2.1. Class A bookmaker shall apply customer due diligence measures to the authorized representative and/or the responsible person with whom it intends to enter into a business relationship. Identification and verification of the potential authorized representative must be completed before the conclusion of the business relationship and details to be updated, as is discussed below:

### A. Identification

Identification, consists the collection of a series of personal details of the authorized representative and where applicable (i.e. when the authorized representative is a legal entity), the beneficial owner and/or the responsible person, which currently consist of:

- name,
- residential address,
- place and date of birth,

- nationality and identity card number of the authorized representative or/and of the responsible person
- bank statement
- criminal record

Where the authorized representative is a legal entity verification should be made available for all Board members.

**B. Verification**

Verification of the identity, residential address and all the information that the Authorised Representative has filed for the beneficial owner and Board Members and/or the responsible person, will be carried out by checking that the personal details provided by the person match with those reported by independent and reliable sources. For the purposes of this obligation, a reliable and independent source includes, inter alia, a government authority, department or agency, a regulated utility company or a subject person carrying out relevant financial business in Cyprus, in a Member State of the EU or in a reputable jurisdiction, since these entities would have already checked the existence and characteristics of the persons concerned.

**C. Nature of Business Relationship**

Obtaining information on the purpose and intended nature of the business relationship.

**D. Ongoing Monitoring Activities**

The bookmaker must be able to know the source of the wealth of the authorised representative, the money to be invested for the opening and operation of the premises and to ensure that the money did not originate from illegal or criminal activities.

When the Class A bookmaker enters into a business relationship with the authorised representative and/or the person responsible, must exercise ongoing supervision. The Class bookmaker must thoroughly consider all the transactions carried out in the premises and to reassure /verify/ensure that all due diligence measures applied by the authorized representative and/or responsible person, as to the players, are properly implemented.

Appropriate and thorough examination requires that a Class A bookmaker, collects information about the source of the wealth of the authorized representative. Source of wealth consists in determining how the authorised representative and/or the responsible person, acquired his net worth and whether these are justified by the nature of the operations carried out at the licenced premises and the transactions conducted. On the basis of this information, Class A bookmakers must be able to detect unusual behaviors or transactions and investigate as necessary. As to the extent of the information to be collected by Class A bookmakers, depends very much on the risk profile of the authorised representative and/or the responsible person.

In cases where the risk is moderate or lower, a declaration from the authorized dealer and/or the responsible person with some details (e.g. nature of employment/business, employer etc.) would suffice. However, where the risk of ML/FT is higher and where the customer's activities are controversial or not consistent with his profile or Class A Bookmaker has suspicions that the authorized representative provides illegal bets as defined in the Act of Betting of 2012, any such declaration would need to be supplemented by more specific information and documentation. In such cases the risk profile of the authorised representative should be put under review.

Further , Class A Bookmaker should ensure that the documents, data or information held are kept up-to-date. The level of on-going monitoring will inevitably depend on the risk profile of the customer but even in low risk situations there must be a degree of oversight taking place.

2.2.3. **CDD to be applied by Class B Bookmakers to its customers**

**A. Identification**

The Class B bookmaker must apply customer due diligence measures in respect of the customer. During the registration of the customer on the website of Class B bookmaker, the second must collect personal information of the customer, which currently consist of:

- name,
- residential address,
- place and date of birth,
- nationality
- identity card number

**B. Verification**

Verification of the customer identity, should be conducted within thirty days from the date of registration of the customer and before the payment of any amount from customer to customer account, as defined in the Betting Law of 2012 in the same way as mentioned above.

**C. Nature of Business Relationship**

Obtaining information on the purpose and intended nature of the business relationship.

**D. Ongoing Monitoring Activities**

The Class B bookmaker shall exercise on going monitoring and control over the client's transactions so as to reassure that the betting activity of the customer is consistent with the economic profile and that customer's account is controlled exclusively by himself.

Appropriate and thorough examination requires that a Class B bookmaker, collects information about the source of the wealth of the customer. Source of wealth consists in determining whether the customer's betting activity is justified by his economic profile. On the basis of this information, Class B bookmaker must be able to detect unusual behaviors or transactions and investigate as necessary. As to the extent of the information to be collected by Class B bookmakers, depends very much on the risk profile of the customer.

In cases where the risk is moderate or lower, the collection of information such as the identity, address and email is sufficient. However, in cases where the risk of ML/TF is higher and the customer's betting activity is not consistent with his profile (essentially the client is considered to be high risk) the Class B bookmaker should ask for more specific information and documents and to proceed to a thorough inspection.

Further , there must be an assurance that the documents, data or information held are kept up-to-date. The level of on-going monitoring will inevitably depend on the risk profile of the customer, which must be revised and classified in low, medium and high risk category according to their customer's behavior.

2.2.4. **CDD applicable from Class A bookmaker towards the customer**

2.2.4.1. The above-mentioned measures are to be applied only in the case of a business relationship where a responsible person must apply all four CDD measures (identification, verification, nature of the business relationship, ongoing monitoring activities).

2.2.4.2. An occasional transaction is a transaction other than a transaction carried out within a business relationship. In determinate sectors the application of CDD measures in the case of occasional transactions depends on the value thereof.

2.2.4.3. When a customer that bets on Class A bookmaker (it is clear that a customer betting on a Class B bookmaker, creates a business relationship from the time of registration) makes an occasional transaction, the Class A bookmaker needs to apply the first two steps of CDD (identification and data verification), before the occasional transaction or shortly after, but before the next transaction takes place.

2.2.4.4. In high-risk scenarios, it is also recommended to identify the source of funds.

2.2.4.5. The initial three elements of CDD are carried out at the inception of the business relationship. However, the application of the risk-based approach allows the obliged entities to vary the extent and timing of CDD measures carried out depending on whether the particular business relationship is rated as presenting a high, medium or low level of ML/FT risk.

2.2.5. **Simplified Due Diligence('SDD')**

2.2.5.1. The carrying out of SDD in low risk situations, i.e. for identification and a sufficient level of on-going monitoring to be carried out but with verification and obtaining additional information on the business relationship postponed until a particular event takes place or a pre-established threshold is reached. However, it would still be necessary to determine whether the customer is a PEP or related to one. It is important to note that in situations where it may be possible to apply SDD but the subject person suspects ML/FT, the subject person is precluded from applying SDD.

2.2.6. **Enhanced Due Diligence ("EDD")**

2.2.6.1. The carrying out of Enhanced Due Diligence ("EDD") in high risk situations, i.e. taking more stringent steps in the application of CDD with special regard to the information to be collected on the purpose and intended nature of the business relationship and on-going monitoring. In particular, obliged entities would be expected to not only obtain information on the source of wealth and the source of funds but to substantiate the same with adequate documentation. In some cases the measures to be applied are set out by law as is the case of PEPs and persons associated therewith.

2.2.7. In all those other situations where the risk is neither low as to allow the application of SDD nor high to warrant the application of EDD, a subject person is expected to apply all four CDD measures, the initial three of which have to be complied with when establishing the business relationship.

2.2.8. Where the subject person is unable to fulfil its CDD requirements at customer on-boarding stage (i.e. identification, verification and determining the purpose and intended nature of the business relationship) because of the customer's own reluctance, the subject person is precluded from establishing the business relationship or carrying out of the occasional transaction. Moreover in such cases the subject person has to consider whether there are reasonable grounds to suspect ML/FT which would necessitate the submission of a suspicious transaction report with the Financial Intelligence Unit (FIU).

2.2.9. The 4$^{th}$ Directive states that CDD has to be carried out whenever a business relationship is established or an occasional transaction takes place. Specifically to the gaming sector, an occasional transaction is equated with the collection of winnings, the wagering of stakes or both of Euro two thousand (€2,000) or more. Thus, no CDD needs to be carried out by a licensee in the case of an occasional transaction unless the said threshold is met or exceeded.

2.2.10. On the other hand, in the case of a business relationship licensees will be required to carry out CDD upon the establishment of such a relationship.

2.2.11. Licensees should always remember that:

a) They cannot apply SDD if the risk assessment reveals that the business relationship is exposing them to a high risk of ML/FT in which case they are expected to apply EDD measures
b) In situations where the only high risk factor is the presence of a PEP or a person linked thereto, they would have to also apply EDD measures
c) They are precluded from applying SDD when they suspect ML/FT.

## 2.3 Consultation questions

Q1. Do you agree with the National Betting Authority's interpretation of the CDD requirements?

Q2. Do you agree with the requirements suggested for CDD measures and when these should be carried out?

Q3. Do you agree with the requirements suggested for SDD and how and when these are applied?

Q4. Do you agree with the requirements suggested for EDD and how and when these are applied?

Q5. Do you consider any requirements to be excessive or unable to be achieved? If yes what alternative measures do you suggest?

Q6. Do you agree with the principle that the client generates a business relationship with the Class B bookmaker from the moment of registration on the bookmaker's website?

Q7. When do you believe an occasional transaction takes place? Are the requirements for CDD for occasional transaction feasible to be implemented?

Q8. Do you have any other comments that you would like to bring to the Authority's attention?

## 3. CUSTOMER DUE DILIGENCE THRESHOLD

### 3.1 4th Directive Requirements

3.1.1. Obliged entities should apply customer due diligence measures in the following circumstances:

(a) when establishing a business relationship;
(b) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
(c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
(d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

### 3.2. Explanation of the Directive Requirements

3.2.1. In the 4th Directive, a key requirement is to make checks on customers, known as customer due diligence. Obliged entities must apply customer due diligence measures when they establish a business relationship, suspect money laundering or terrorist financing, or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

3.2.2. Obliged entities must also apply customer due diligence measures in relation to any single 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.

3.2.3. Transactions are considered as linked if they are carried out by the same customer –

- through the same game or
- in one gaming session.

3.2.4. A transaction consists of the wagering of a stake or the collection of winnings.

3.2.5. The *customer due diligence threshold* is determined by any transaction of €2,000 or more, whether it is a single transaction or occurs in several transactions which appear to be linked. The Authority may reduce the monetary threshold of €2,000 or more (for example to set it to €500), however the option of increasing the limit beyond €2,000 is not an option.

3.2.6. In this context, Class A bookmaker may utilize one of the two methods below to ensure the application of CDD measures –

- establishment of a business relationship with all of his customers, or
- overseeing the €2,000 threshold.

### 3.3. Establishment of a business relationship with all Customers

3.3.1. The business relationship between the bookmaker and the customer is a commercial relationship arising out of the licensed activities of the bookmaker, in which the customer is involved and requires duration.

3.3.2. The "duration term" is open to wide interpretation by the bookmakers, provided that the required procedures are applied.

3.3.3. The business relationship between the customer and the bookmaker is likely to be contracted when the customer is registered via an authorized representative, as a registered customer of the specific bookmaker (where the bookmaker provides such possibility).

3.3.4. At the inception of the business relationship, the bookmaker should take into account the following:

- the risk profile of the customer,
- the appropriate customer due diligence measures
- whether it is known or suspected that the customer might legalize revenue from illegal activities.

### 3.4 Overseeing the €2000 threshold

3.4.1. The Class A bookmaker must satisfy the Authority that has appropriate mechanisms to monitor the activity of each customer within the licenced premises and is in a position to immediately identify a transaction that has exceeded the upper limit. For example, in licensed premises in which the average profit/wagering is under €500 per customer, the bookmaker must be able to recognize linked transactions, i.e. identical and/or repetitive betting that either the deposit or winnings, or both exceed €2,000. It is at this point that bookmaker, through its authorised representative must apply CDD measures.

3.4.2. Therefore, the bookmaker may defer the immediate application of the customer CDD and ask for identification and verification information when and if the limit of €2,000 break.

3.4.3. Alternatively, the bookmaker may consider that is more practical or more feasible, if the customer identification is carried out at the entrance of the customer at the premises and verification of data is performed when the limit of €2,000 is reached.

3.4.4. The advantages of identification when entering the premises (even if data verification is carried out at a later time) are many. Amongst others –

- this will not interrupt the activity of the customer when he exceeds the limit for identification purposes,
- there will be an automatic recording of betting activity per customer, strengthening thus the implementation of these measures
- the bookmaker will be able to integrate 'players rewards programs'
- the bookmaker will promote the application of new technologies to prevent the entry of underage persons on the premises.

3.4.5. On the contrary, the bookmaker will be responsible for the ability of each licenced premises to record and identify all transactions per customer and in accordance with the limit of €2,000 .

## 3.5. Consultation questions

Q1. Do you agree with the National Betting Authority's interpretation of the new threshold requirements?

Q2. In which of the following situations do you consider that it is necessary to apply CDD measures:

- To all new customers irrespective of threshold?
- To new customers that reach the threshold?
- To existing customers that reach the threshold?
- When the operator becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed?

Q3. Do you agree with the Authority's interpretation of linked transactions? Do you want to add any other situations as to when transactions should be considered linked?

Q4. Do you consider that transactions should be considered to be linked if the same customer has carried out a new transaction(s) in another bookmaker(s) in the same day for the same game?

Q5. Do you consider that it might be better to perform CDD on all new or existing customers irrespective of transaction threshold, from the day that the Law will be in force so that there will be no necessity to worry about transaction thresholds? In this case you will only be concerned with obtaining additional EDD in case of PEPs and/or other high risk situations.

Q6. Do you believe that the application of a "Player's Card" could largely eliminate the problems of identifying due diligence measures if the customer achieves the threshold?

Q7. Would you agree with the implementation of such a card? What are your concerns on the possible implementation of a player's card?

Q8. What is the duration (length of time) that is appropriate to exist between the customer and the bookmaker, in order to be conceived that the customer has entered into a business relationship?

## 4. KNOW YOUR CUSTOMER (KYC) REQUIREMENTS

### 4.1. 4th Directive Requirements

4.1.1. KYC requirements should be performed upon application of CDD measures.

4.1.2. Customer due diligence measures shall comprise:

(a) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
(b) Identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;
(c) Assessing and, as 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 the transactions being conducted are consistent with the obliged entity'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.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

4.1.3. The verification of the identity of the customer and the beneficial owner take place before the establishment of a business relationship or the carrying out of the transaction.

4.1.4. The verification of the identity of the customer and the beneficial owner might be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. In such situations, those procedures shall be completed as soon as practicable after initial contact and before the next transaction takes place or winnings withdraw.

### 4.2. Explanation of the Directive Requirements

#### 4.2.1. Identification

4.2.1.1. The identification of customers consists of the collection of various information, such as the customer's name, the current residential address, date of birth, place of birth, physical

appearance, professional occupation, financial history, even the family circumstances of the client.

4.2.1.2. A Class A bookmaker verifies the identity of players through its authorized representatives and the persons responsible within the licenced premises, who will record the personal information of players in a database, including the identity, home address and date of birth.

The verification of the information is performed by –

- requesting the customers national identity card or passport that has a customer's picture
- requesting a driving license or any other document issued by a governmental department, or public utility bill or bank account document or other trusted institution bearing the address of the customer
- verifying the information of the document, by the authorised representative of the specific licensed premises, in which the client is a client for some period of time.

4.2.2. **Verification**

4.2.2.1. The information about the customer's address can be verified through documents, data and information obtained from a reliable and independent source. The verification may be made through the submission of original documents or certified copies thereof by certifying officers.

4.2.2.2. The submission of a government document such as an identification card or passport, indicating identification details including a photo of the customer, is sufficient for identity verification purposes.

4.2.2.3. Authorised representatives and responsible persons must receive adequate training so that they can, within a logical framework, identify and reject forged documents. In the event that suspicions arise in respect of any submitted document, the bookmaker should take practical measures and in proportion to the issue arising, to determine whether the document in question is the product of a loss, theft or forgery.

4.2.2.4. Specialized software and computerized systems that check the validity of such documents are widely available and possible to facilitate the implementation of the obligations of the bookmaker.

## 4.3. Consultation questions

Q1. Do you agree that the KYC documents should be collected by the bookmaker when the threshold has been reached by the player?

Q2. Do you agree that bookmakers should be able to identify transactions that are linked? Do you think that authorised representatives and responsible persons, with the proper training, will be able to detect such transactions? If not, what are your suggestions?

Q3. Do you agree with the National Betting Authority's suggestion for the collection of the said aforementioned documents for KYC requirement purposes?

Q4. Do you have any other suggestions?

## 5. RISK ASSESSMENT AND RISK-BASED APPROACH

### 5.1. 4th Directive Requirements

#### 5.1.1. Risk assessment

5.1.1.1. Obliged entities must take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities.

#### 5.1.2. Risk Based-Approach

5.1.2.1. The risk assessments shall be documented, kept up-to-date and made available to the authority as requested. Obliged entities shall have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

5.1.2.2. The policies, controls and procedures referred to above shall include:
(a) the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;
(b) where appropriate with regard to the size and nature of the business, an independent audit function to test the internal policies, controls and procedures referred to in point (a).
(c) Obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

### 5.2. Explanation of the Directive Requirements

#### 5.2.1 Risk Assessment

5.2.1.1. The cornerstone of the risk-based approach is the risk assessment which has to be carried out at different stages of obliged entities activities. This assessment allows the obliged entities to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the obliged entities will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

5.2.1.2. However, each customer exposes the obliged entities to different risks. A customer-specific risk assessment must therefore be carried out so that the obliged entities are able to identify potential risks upon entering into a business relationship with or carrying out an occasional transaction for a customer. This assessment enables the obliged entities to develop a risk profile for the customer and to categorise the ML/FT risk posed by such customer as low, medium or high.

5.2.1.3. The obliged entities must subsequently ensure that the AML/CFT measures, policies, controls and procedures adopted are sufficiently flexible to allow addressing the specific ML/FT risks arising from the particular business relationship or occasional transaction. The application of these measures, policies, controls and procedures to be implemented to particular risk scenarios, has to result from the subject person's Customer Acceptance Policy (CAP).

### 5.2.2. What is the Risk-Based Approach?

5.2.2.1. Licensees may already be aware that the AML/CFT regulatory framework that will be applicable to them as obliged entities adopts a risk-based approach, i.e. it requires obliged entities to adopt measures, policies, controls and procedures that are commensurate to the ML/FT risks to which they are exposed, in order to prevent and mitigate the said risks from materialising themselves.

5.2.2.2. The risk areas that arise from a business risk assessment as well as the customer-specific risk assessment can be divided into four, i.e.

a) customer risk,
b) product/service/transaction risk,
c) interface risk and
d) geographical risk.

5.2.2.3. The risk-based approach recognises that the ML/FT risks faced by each sector and each subject person are different, and allows for resources to be invested and applied where they are most required. It is diametrically opposed to a prescriptive tick-box approach and entrusts subject persons with significant discretion in its application.

5.2.2.4. An effective risk assessment has to be a dynamic one. Obliged entities have to ensure that they revise the same procedures when there are significant developments within the environment within which they are operating and within their business structures/activities. Any such changes can lead the subject person to be exposed to new ML/FT risks. Identifying the same through a revision of the risk assessment allows the obliged entities to take action to ensure that its measures, policies, controls and procedures are robust enough to cater for these.

### 5.2.3. Specific High Risk Situations

5.2.3.1. It is important to note that independently of the risk assessment carried out by the obliged entities, there will always be instances that are deemed to be high risk. One such instance is dealing with Politically Exposed Persons ("PEPs"), their family members or close business associates ("persons linked thereto"). In such cases, the regulatory framework itself sets out the measures to be applied, to adequately address the risks arising from dealing with the said individuals. This aspect is considered further in Section 6 below.

### 5.2.4. Business Risk factors specific to the Gaming Sector

5.2.4.1. Licensees will be required to carry out a business risk assessment to identify the ML/FT risks they are exposed to and ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate the same.

5.2.4.2. The business risk assessment has to be documented and approved by the Board of Directors (or equivalent) of the licensee, and made available to the Authority upon request.

5.2.4.3. Licensees will be expected to revise their business risk assessment whenever there are changes to the environment within which they are operating and within their business structures/activities. Thus, situations such as a widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered should lead to a revision of the business risk assessment. The same applies when the licensee changes its structure or undertakes major operational changes. In the absence of any of the above, licensees should assess their business risk assessment at least once a year, to evaluate whether any changes thereto are necessary.

5.2.4.4. Licensees may engage external consultants to assist them in the drawing up and /or the revision of their business risk assessments. However, it will be necessary for any report, findings and conclusions to be adopted by the licensees who retain responsibility, to ensure it complies with its obligation to carry out a business risk assessment. It is understood that in such a case, the Authority will be informed.

### 5.2.5. Risk Factors Specific to the Gaming Sector including the Remote Gaming Sector

#### *5.2.5.1. Customer Risk*

5.2.5.1.1. The risk of ML/FT may vary in accordance with the type of customer.

5.2.5.1.2. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. A customer having a single source of regular income will pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.

### 5.2.5.2. *Product/Service/Transaction Risk*

5.2.5.2.1. Some products/services/transactions are inherently more risky than others and are therefore more attractive to criminals.

5.2.5.2.2. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it on his own or in collusion with others. The use by customers and the acceptance by licensees of specific funding methods should also be treated as high risk factors.

5.2.5.2.3. This includes cash and other payment method that may not leave or disrupt the audit trail and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies.

### *5.2.5.3. Interface Risk*

5.2.5.3.1. The channels through which a licensee establishes a business relationship and/or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favour anonymity increase the risk of ML/FT if no measures are taken to address the same.

5.2.5.3.2. However, licensees may want to note that situations where interaction with the customer takes place on a non-face to face basis will no longer be considered as automatically high risk as long as technological measures are in place to address the heightened risk of identity fraud or impersonation present in these situations. It is the Authority's opinion that the use of technological measures are sufficiently effective to counter the above mentioned risks emanating from the fact that the potential customer is not sighted physically prior to the provision of gaming services. These measures allow a licensee to establish whether or not the customer providing the relative identification details is actually the person he alleged to be.

5.2.5.3.3. On the other hand, the use of electronic databases only allows for determining whether the identification details provided correspond to those of an actual person but does not provide sufficient comfort in establishing whether the customer is that individual. Hence, the risk inherent in non-face to face transactions will not have been sufficiently addressed and additional risk mitigation measures in the form of enhanced due diligence would become necessary.

### *5.2.5.4. Geographical Risk*

5.2.5.4.1. The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship.

The nationality, residence and place of birth of a customer should also be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT.

## 5.3 Consultation questions

Q1. Do you understand the requirements of the Risk Assessment and the Risk-based approach?

Q2. Do you understand how the risk-based method should be used?

Q3. Do you foresee any areas in which complications may exist in the risk based methodology?

Q4. Which areas do you consider as high risk from the gaming sector products offered by the licencees?

## 6. POLITICALLY EXPOSED PERSONS (PEPs)

### 6.1. 4th Directive Requirements

6.1.1. With respect to transactions or business relationships with politically exposed persons, obliged entities are required to:

(a) 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 politically exposed person;
(b) apply the following measures in cases of business relationships with politically exposed persons:

(i) obtain senior management approval for establishing or continuing business relationships with such persons;
(ii) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
(iii) conduct enhanced, ongoing monitoring of those business relationships.

6.1.2. Where a PEP is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organisation, obliged entities shall, for at least 12 months be required to take into account 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.

6.1.3. The measures described above, shall also apply to family members or persons known to be close associates of PEPs.

### 6.2. Explanation of the Directive Requirements

6.2.1. The meaning 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions domestic or in a foreign country and includes the following:

(a) heads of State, heads of government, ministers and deputy or assistant ministers;
(b) members of parliament or of similar legislative bodies;
(c) members of the governing bodies of political parties;
(d) 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;
(e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;
(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

6.2.2. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

6.2.3. The establishment of a business relationship or the execution of an occasional transaction with a PEP, may expose obliged entities to enhanced risks.

6.2.4. Obliged entities should pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards. In order to effectively manage such risks, obliged entities should assess the countries of origin of their customers in order to identify the ones that are more vulnerable to corruption.

6.2.5. Where a person has ceased to be entrusted with a prominent public function for a period of at least one year, the Bookmakers shall not be obliged to consider such a person as politically exposed.

6.2.6. 'Immediate family members' of a PEP includes the following:

- the spouse or a person considered to be equivalent to a spouse, of a politically exposed person
- the children and their spouses or persons considered to be equivalent to a spouse, of a politically exposed person
- the parents of a politically exposed person

6.2.7. 'Persons known to be close associates' of a PEP includes the following:

- any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP.
- any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the PEP.

6.2.8. Obliged entities adopt the following additional due diligence measures when they establish a business relationship or carry out an occasional transaction with a PEP.

6.2.9. Put in place appropriate risk management procedures to enable them to determine whether a prospective customer is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the customer himself or from publicly available information. In the case of legal entities and arrangements, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute

PEPs. In case of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in the Law and the present Directive.

6.2.10. The decision for establishing a business relationship or the execution of an occasional transaction with a PEP may be taken by the senior management of the obliged entities and /or the compliance officer. When establishing a business relationship with a customer (natural or legal person) and subsequently it is ascertained that the persons involved is or has become a PEP, then an approval is given for continuing the operation of the business relationship by senior management of the obliged entities and/or the compliance officer.

6.2.11. Before establishing a business relationship or executing an occasional transaction with a PEP, the obliged entity obtains adequate documentation to ascertain not only the identity of he said person but also to assess his business reputation (e.g. reference letters from third parties).

6.2.12. The obliged entity creates the economic profile of the customer. The details of the expected business and nature of activities of the customer forms the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. The obliged entity should be particularly cautious and most vigilant where its customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

6.2.13. The account is subject to annual review in order to determine whether to allow its continuance of operation. A short report is prepared summarising the results of the review by the person who is in charge of monitoring the account. The report is submitted for consideration and approval to by the compliance officer to the senior management and filed in the customer's personal file.

## 6.3. Consultation questions

Q1. Is the meaning of a PEP well understood? Is there any aspect which requires further explanation?

Q2. What measures do you think need to be implemented by an authorized representative or responsible person to know if the client is PEP?

Q3.What measures do you think Class A Bookmaker should apply to know if the client is PEP?

Q4. Is it clear when enhanced Due Diligence measures should apply?

Q5. Is it clear what type of additional measures are necessary to be performed?

Q6. Do you have any concerns with regard to the requirements to be applied for PEPs?

Q7. Do you agree that the decision to accept or carry on a business relationship with a PEP should require approval by the senior management?

Q8. What responsibilities should the authorized representative or the person responsible have, if they don't realize that a customer is PEP?

## 7. COMPLIANCE OFFICER

### 7.1. 4th Directive Requirements

7.1.1. Member States shall ensure that obliged entities have in place policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified at the level of the Union, the Member State and the obliged entity. Those policies, controls and procedures shall be proportionate to the nature and size of the obliged entities.

7.1.2. The policies, controls and procedures referred to in paragraph 7.1.1. above shall include: the development of internal policies, controls and procedures, including model risk management practices, customer due diligence, reporting, record-keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening;

### 7.2. Explanation of the Directive Requirements

7.2.1. The 4th Directive requires that an individual must be appointed as a compliance officer at the bookmaker's company.

7.2.2. The role of the compliance officer, is to monitor and manage the risk of money laundering with determination. Amongst the responsibilities of the compliance officer is the submission of an internal report to the Board of Directors as well as the reporting to the FIU of any suspicious transactions or other information regarding money laundering activities, related predicate offences and the financing of terrorism.

7.2.3. An appointed compliance officer, should have a managerial position, so as to command the necessary authority.

7.2.4. The compliance officer is responsible for overseeing all aspects of AML/CFT within the company. Furthermore, the compliance officer of a Class A Bookmaker, is also responsible for monitoring all of the licensed premises and authorised representatives providing licensed services on his behalf.

7.2.5. The compliance officer should:

- be empowered to act independently in the performance of his duties, and
- should have direct communication with the National Betting Authprity and the FIU.

7.2.6. The duties and the responsibilities of the compliance officer should be clearly stated in an employment contract in a clear and complete manner.

7.2.7. The bookmaker must ensure that the compliance officer is independent to carry out the monitoring activities within the company and to provide him with seamless access to all relevant information that would allow him to fulfil his duties. Responsibilities include the objective review of all related administrative decisions and, in some cases, the provision of recommendations, even when these contradict with the short-term operational objectives of bookmaker.

7.2.8. The bookmaker should make available to the compliance officer all sufficient means necessary to carry out his tasks, including technology, qualified personnel and training. In case of temporary absence of the compliance officer, another person with sufficient expertise should replace him.

7.2.9. The bookmaker may appoint a compliance officer, someone who already has, at the same time, other roles and responsibilities within the company. In this case the bookmaker should ensure that the compliance officer is able to carry out his duties properly, including the direct reporting of events to the Board, and the FIU, as well as having the decision-making ability to fight fraud regardless of business concerns.

7.2.10. The compliance officer should be able to monitor the daily operation of the policies around AML/CTF and to respond promptly to any requests by the Authority under the relevant Directive. The compliance officer has the ultimate administrative responsibility for AML issues, without providing relief to the Board of Directors of the company from any liability.

7.2.11. Where it is deemed necessary due to the volume and/or the geographic spread of the services/activities, an assistant of the compliance officer may be required to be appointed, for the purpose of assisting the compliance officer in his duties and passing internal suspicion reports to him.

7.2.12. Outsourcing of the compliance position or compliance assistant position will not be allowed.

7.2.13. The Bookmaker communicates immediately to the Authority, the names and positions of the persons it appoints as compliance officer and assistant of the compliance officer. In case of replacement, it shall immediately inform the Authority and shall within 14 days report the person's details. If the recipient chooses to appoint an assistant compliance officer, the notification to the Authority also applies to him.

**7.3. Consultation questions:**

Q1. As bookmakers are required to have an in-house compliance officer and assistant, please indicate whether you consider this requirement reasonable and what additional costs and impacts, if any, would be incurred by your business?

Q2. Do you believe the compliance officer needs to be certified having passed specialised exams?

Q3. If your answer to question 3 is positive, do you believe that these exams should be specialized just for the gaming industry or should they be for other obliged entities and industries?

Q4. Are there any implications that the National Betting Authority should be aware of?

## 8. TRAINING

### 8.1. 4th Directive Requirements

8.1.1. Member States shall require that obliged entities take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to this Directive, including relevant data protection requirements.

8.1.2. Those measures shall include participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

8.1.3. Member States shall require that, where applicable, obliged entities identify the member of the management board who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive.

### 8.2. Explanation of the Directive Requirements

8.2.1. In order for the Bookmaker to apply effective controls, all the responsible officials, must be educated and have knowledge of the money laundering and financing of terrorism matters at regular times. Bookmakers must ensure that all responsible officials understand the National Law, the 4th Directive, the processing of personal data Law, as well as the Directive to be adopted by the Authority relating to money laundering and continuously and correctly apply all processes. Further, the bookmaker must ensure that all responsible officials can handle the software programs and the technology available to the recipient, as well as to identify unusual or high risk transactions. They also need to know the procedures they need to follow once they realize that a transaction is suspicious.

8.2.2. The bookmaker must keep a register of all trained officials, which will notify to the Authority, citing the training they have received.

8.2.3. For the purposes of this document, "officials" means the employees of the bookmaker dealing with monitoring of transactions, engaged in the management of the company, authorised representatives and/or responsible persons.

### 8.3. Consultation questions

Q1. Do you agree that responsible officials must be trained?

Q2. Do you agree that the responsibility for training of responsible officials must lie with the bookmaker?

Q3. Do you agree that the recipient must keep a register, which will notify the Authority, with all the responsible officials that have been trained, citing the training they have received?

Q4. Do you think that the authority should organizes specialized seminars and issue training certificates?

## 9. BENEFICIAL OWNERSHIP

### 9.1. 4th Directive Requirements

9.1.1. Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. Member States shall ensure that those entities are required to provide, in addition to information about their legal owner, information on the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures.

9.1.2. Member States shall ensure that the information referred to in paragraph 9.1.1 above is held in a central register in each Member State, for example a commercial register, companies register. The information on beneficial ownership contained in that database may be collected in accordance with national systems.

9.1.3. Member States shall require that the information held in the central register referred to in paragraph 9.1.2 above is adequate, accurate and current.

9.1.4. Member States shall ensure that the information on the beneficial ownership is accessible in all cases to:

(a) competent authorities and FIUs, without any restriction;

(b) obliged entities,

(c) any person or organisation that can demonstrate a legitimate interest.

9.1.5. The persons or organisations referred to in point 9.1.4. (c) shall access at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held. For the purposes of this paragraph, access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee. The fees charged for obtaining the information shall not exceed the administrative costs thereof.

### 9.2. Explanation of the Directive Requirements

9.2.1. Obliged entities (legal entities) will be required to provide to the Authority information as to their own beneficial ownership.

9.2.2. Obliged entities are also required to provide details of their beneficial ownership to the Authority that will hold the central register of beneficial ownerships (applies only to bookmakers and their authorized representatives who are legal entities).

9.2.3. The information provided to the registers should be adequate, accurate and current and the central register should be accessed by competent authorities and governmental authorities, other obliged entities such as other bookmakers and persons that can demonstrate a legitimate interest. The term legitimate interest, adequate, accurate and current information is to be determined in due course.

9.2.4. The information to be accessed from the central register by legitimate persons should be at least the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held. Access to the information on beneficial ownership shall be in accordance with data protection rules and may be subject to online registration and to the payment of a fee.

9.2.5. Access to the information in accordance with data protection rules will be determined by the Authority in due course.

## 9.3. Consultation Questions

Q1. Are the requirements regarding the beneficial ownership understood clearly?

Q2. Are there any aspects that require further explanation?

## 10. TRANSACTION MONITORING

### 10.1. 4th Directive Requirements

10.1.1. Customer due diligence measures shall comprise amongst other requirements conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity'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.

10.1.2. With respect to transactions or business relationships with politically exposed persons, in addition to the customer due diligence measures obliged entities are required to conduct enhanced, ongoing monitoring of those business relationships.

### 10.2. Explanation of the Directive Requirements

10.2.1. Obliged entities are required to conduct on going monitoring activities on all transactions undertaken by customers in order to ensure that transactions are in accordance with the customers risk profile and knowledge of the customer activities and profile. As a result the customer's profile should be compiled and kept up to date and accessible at all times for comparison and review purposes.

10.2.2. Transactions should also be monitored to ensure that the threshold has not been exceeded at any point in time without appropriate due diligence procedures performed.

10.2.3. In addition all transactions with PEPs should be continuously monitored.

### 10.3. Consultation Questions

Q1. Are the requirements regarding transaction monitoring clearly understood?

Q2. Do you have any questions regarding the method to be used for transaction monitoring?

## 11. REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

### 11.1. 4th Directive Requirements

11.1.1. All suspicious activities / transactions, including attempted transactions, shall be reported.

11.1.2. Suspicious activities / transactions and other information relevant to money laundering, associated predicate offences and terrorist financing should be reported to the FIU, which should serve as a central national unit for receiving, analysing and disseminating to the competent authorities the results of its analyses. All suspicious activities / transactions, including attempted transactions, should be reported, regardless of the amount of the transaction. Reported information could also include threshold-based information.

### 11.2. Explanation of the Directive Requirements

11.2.1. In cases where there is an attempt of executing transactions which the bookmaker knows or suspects that are related to money laundering or terrorist financing, immediately he should report through the compliance officer its suspicion to the national FIU.

11.2.2. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the bookmaker has created for the customer. The bookmaker ensures that maintains adequate information and knows enough about its customers' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

11.2.3. Obliged entities are required to have internal and external procedures providing for the reporting of suspected or known instances of ML/FT. The internal reporting procedures must allow for obliged entities employees' to even report a suspected instance of ML/FT to the Money Laundering Reporting Officer ("MLRO") when their immediate superior is in disagreement with them. It will be then up to the MLRO to determine if the information available can be considered as sufficient for a Suspicious Transaction Report ("STR") to be made to the FIU.

11.2.4. When the ML/FT suspicion is linked to a transaction still to be processed, it is important that the Subject person refrains from carrying out the same, files an STR and delays the execution of the transaction for one (1) working day following the day on which the licensee files the STR. During this time the FIU has to determine and communicate to the bookmaker whether it objects to the execution of the said transaction. Where refraining from carrying out the transaction is not possible or doing so would prejudice

an analysis or investigation of the suspected instance of ML/FT, the bookmaker may decide to proceed with the transaction's execution. The impossibility to refrain from processing a transaction must arise from the nature of the transaction itself and the bookmaker must then submit a STR to the FIU immediately afterwards.

11.2.5. The need not to prejudice an analysis or investigation into ML/FT is also at the basis of the non-disclosure obligations arising from filing a STR or receiving a request for information with the FIU. Safeguarding the integrity of an analysis or investigation is also why caution is advised when a bookmaker takes action to terminate a relationship or otherwise block a transaction following the filing of an SAR or STR. Drastic action should only be taken once the FIU has been advised of the subject person's intentions as any unjustified action may alert the customer that he is being suspected of foul play. In such circumstances it would be more advisable to increase on-going monitoring and submit additional STRs to the FIU on any other suspected instances of ML/FT instead of breaking of the relationship with the customer.

11.2.6. Licensees have the obligation to report transactions they suspect to be linked to ML. The filing of a STR should also be made in the following circumstances:

i. For any suspicious transactions that the licensee becomes aware of in the exercise of his business that a person is linked to ML/FT or that ML/FT is being committed or may be committed independently of whether any transactions have taken place or otherwise.
ii. In situations where there is a suspicion of FT or that funds are the proceeds of crime.
iii. Reporting has to take place also when licensees have reasonable grounds to suspect that ML/FT may be taking place, this being a more objective ground for reporting. This implies that a further obligation to report arises where, on the basis of objective facts, the subject person ought to have suspected that ML/FT existed.

11.2.7. What kind of behaviour or transactions should alert licensees to a possible case of ML/FT and result in an internal report to the MLRO? There are red flags that may alert licensees but they are merely indicative and need not necessarily taken on their own point to ML/FT taking place. These red flags include:

i. Customer does not cooperate in the carrying of CDD.
ii. Customer attempts to register more than one account with the same licensee.
iii. Customer deposits considerable amounts during a single session by means of multiple prepaid cards.
iv. Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
v. Customer makes small wagers even though he has significant amounts deposits, followed by a request to withdraw well in excess of any winnings.
vi. Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
vii. Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.

viii. Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.

ix. Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.

x. Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.

xi. Customer displays suspicious behaviour in playing games that are considered as high risk.

## 11.3. Consultation Questions

Q1. Is there any aspect which requires further explanation?

Q2. Is it clearly understood when, how and where STRs should be filed?

Q3. Is the role of the compliance officer understood for filing SAR/STR?

Q4. Is there any point of reference from the above that causes you concern or worry of its execution?

Q5. Do you consider that the reference to one working day in point 11.2.4. as well as the way the Authority suggests handling such a case to be reasonable and feasible in its execution;

Q6. Are the red flags listed in point 11.2.7 understandable; Is there any red flag that you disagree on the way that it should be handled?

Q7. Do you think that in the case where it is determined that a suspicious transaction has taken place, should in addition to the FIU, the Authority also be informed?

## 12. RECORD AND DELETION OF DATA IN ACCORDANCE WITH DATA PROTECTION LAW

### 12.1. 4th Directive Requirements

12.1.1. Certain aspects of the implementation of this Directive involve the collection, analysis, storage and sharing of data. Such processing of personal data should be permitted, while fully respecting fundamental rights, only for the purposes laid down in this Directive, and for the activities required under this Directive such as carrying out customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

12.1.2. The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to avoid different approaches and in order to fulfil the requirements relating to the protection of personal data and legal certainty, that retention period should be fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary for the purposes of prevention, detection or investigation of money laundering and terrorist financing, and after carrying out an assessment of the necessity and proportionality, Member States should be able to allow or require the further retention of records for a period not exceeding an additional five years, without prejudice to the national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings. Member States should require that specific safeguards be put in place to ensure the security of data and should determine which persons, categories of persons or authorities should have exclusive access to the data retained.

### 12.2. Explanation of the Directive Requirements

12.2.1. Obliged entities upon performing CDD should collect, analyze, process and store customer personal data.

12.2.2. The collections and processing of personal data should be limited to what is necessary for the purpose of complying only with the current requirements of this Directive and should not be used or shared with anyone for any other purpose. The disclosure of any information to third parties should be made only with the authorization of the person to whom it belongs.

12.2.3. The disclosure of information is permissible only in respect of the exchange of information by the competent authorities and / or the exchange of information by credit institutions and financial institutions and other obliged entities.

12.2.4. The processing of personal data for commercial and advertising purposes is strictly forbidden.

12.2.5. Bookmakers should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. The retention period should be fixed at five years after the end of a business relationship or of an occasional transaction.

12.2.6. However, if necessary for the purposes of prevention, detection or investigation of money laundering and terrorist financing, and after carrying out an assessment of the necessity and proportionality, retention of records may be kept for an additional period not exceeding five years.

12.2.7. However, if required by national criminal law or a criminal investigation or judicial procedure, record keeping should be retained for as long as the formal investigation or judicial procedure is required. Member States should require specific safeguards to ensure the security of data and should determine which persons or categories of persons or authorities should have exclusive access to the data retained.

## 12.3. Consultation Questions

Q1. Are there any queries with regard to the retention of personal data?

Q2. Are there any queries with regard to the deletion period for personal data?

Q3 Would you like any further explanations or clarifications with regard to any of the above requirements?

## 13. HOW TO RESPOND TO THIS CONSULTATION

**13.1.** The Authority is committed to a full and open consultation and would welcome comments on any aspect of this document.

**13.2.** A response template will be available on our website. We would prefer respondents to complete the response template provided and send it by email to: directives@nba.gov.cy

**13.3.** The deadline for responses to this consultation is the **16th of February 2018.** Respondents are of course welcome to comment on any or all of the areas addressed by this consultation.

**13.4.** When responding, please state whether you are responding as an individual or representing the views of an organisation. If responding as an individual, please mention your own interest in the consultation.

## 14. ABBREVIATIONS

| | |
|---|---|
| NBA | National Betting Authority |
| CDD | Customer Due Diligence |
| CDDT | Customer Due Diligence Threshold |
| KYC | Know Your Customer |
| SDD | Simplified Due Diligence |
| EDD | Enhanced Due Diligence |
| AML | Anti-money Laundering |
| CFT | Combating the Financing of Terrorism |
| AML/CFT | Anti-Money Laundering / Combating the Financing of Terrorism |
| CAP | Customer Acceptance Policy |
| PEP | Politically Exposed Person |
| MLRO | Money Laundering Reporting Officer |