Guidelines on fighting money laundering and terrorist financing for the European online gambling sector

Final Version - 6 March 2023

EGBA | European Gaming & Betting Association

About EGBA

The European Gaming and Betting Association (EGBA) is the Brussels-based trade association representing the leading online gambling operators established, licensed, and regulated within the EU, including bet365, Betsson Group, Entain, Flutter, Kindred Group, and William Hill. EGBA works together with national and EU authorities and other stakeholders towards a well-regulated and well-channelled online gambling market which provides a high level of consumer protection and takes account of the realities of the internet and online consumer demand. EGBA member companies meet the highest regulatory standards and, in 2021, had 225 online gambling licenses to provide their services to 29,8 million customers across 21 different European countries. Currently, EGBA members account for 33% of Europe's online gambling gross gaming revenue (GGR).

The guidelines

EGBA has published these Guidelines:

1. Recognising the importance of Anti-Money Laundering (AML) laws for the European economy, the rule of law and the prevention of crime.
2. Stressing the need for more guidance from Member States' competent authorities.
3. Requesting more involvement from the European Commission on encouraging Member States to develop sector-specific guidance on AML for the online gambling sector.
4. Emphasizing the importance of businesses in fighting money laundering.
5. Underlining the commitment of Europe's online gambling sector to fight money laundering.
6. The European Gaming and Betting Association (EGBA) has reached agreement on the following Guidelines on fighting money laundering for the European online gambling sector. These Guidelines contain minimum anti-money laundering obligations to which gambling operators agreed to adhere and committed to implement in their organization, as well as sector specific clarifications.

Table of Contents

1. General provisions

1. EGBA aims to fill the existing gap regarding the absence of sufficient guidance on fighting money laundering for the online gambling industry by examining sector-specific issues, to assist in fighting money laundering more efficiently in the European Union and the EEA. EGBA underlines the importance of the proper implementation of Anti-Money Laundering obligations by setting minimum common standards in this document.
2. The key principle upon which the Guidelines are based is the risk-based approach, as is the approach in the European Union Anti-Money Laundering legislation.
3. Any national, European, or supranational laws on AML take precedence over these Guidelines. Should a conflict of interpretation arise, the former must be adhered to.
4. Any national, European, or supranational risk assessments take precedence over these Guidelines if a conflict of interpretation arises, the former must be adhered to.

2. Purpose & Scope

5. The online gambling industry is a designated non-financial business and profession ('DNFBPs') offering gambling services for entertainment purposes but also undertakes activities that are akin to financial institutions, such as accepting and withdrawing funds. Online gambling is subject to AML regulations due to the opportunity to launder money by funnelling criminal proceeds through a gambling platform, thereby obscuring their illicit origin.
6. These Guidelines aim to analyse sector-specific issues that should be considered when discussing money laundering (ML) and terrorist financing (TF) in the gambling industry, whilst providing operators with harmonized guidance to attain uniformity in the application, and minimum level of AML/CTF compliance obligations. Understanding the sector-specific ML/TF indicators is essential for the establishment of controls that help in the detection and prevention of such offences. These Guidelines shall focus on the requirements emanating from the EU AML Directives; however, the national transposition thereof is not in the scope. The upcoming EU AML Regulation[1] is taken into account as much as possible, given that the text is not finalised at the time of the publication of these Guidelines.
7. These Guidelines are covering only B2C operations of gambling operators and only with customers that are individuals.

3. The Risk-Based Approach

8. The application of a risk-based approach to combating ML/TF is an essential element of an effective AML/CTF compliance structure. This requires for measures to be commensurate to the risks identified. Operators shall assess the core risk factors at minimum, such as the categories of customers onboarded (particularly high-risk customers), the products and services offered, transactions, the jurisdictions they operate in, and the interface and delivery channels used. In addition to these basic categories, operators can add any other type of risk that they deem relevant for their organization.
9. In assessing the risks, operators should use already known risk assessment matrixes in the wider compliance area. The best practice approaches would suggest that operators should examine each

[1] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.*

risk on inherent and residual level, analysing threats and vulnerabilities for each risk and considering the probability and impact of each risk materializing.

10. The inherent risk is the risk before application of any controls and therefore, it is a starting point which helps operators to understand how much they are exposed to, the specific risks in an environment without any controls. In calculating this risk, it is recommended that operators consider the probability for the risk to materialize, as well as its impact, if the risk does materialise.
11. The inherent risk probability is the chance of an identified ML/TF risk materializing as part of everyday operations and can also be interpreted as the vulnerability of each area identified, and how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others. Consideration should be given to factors such as the below when determining the probability of an identified risk:
    - The operator's exposure to a particular risk through business intelligence reports (data of a company).
    - If the market is more prone to a particular risk over others, considering ML/TF tendencies in that jurisdiction.
    - Reports issued by relevant authorities on severity and frequency of risks materializing.
12. The inherent risk impact describes the expected impact to the Company should the identified ML/TF risk materialize without any specific control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others. Consideration should be given to factors, such as the below, when determining the impact of an identified risk:
    - Risk ratings provided by the relevant authorities in national risk assessments, the Supranational Risk Assessment and sector specific guidance.
    - Facilitation of criminal conduct.
    - Risk of regulatory fines and legal prosecution.
    - Reputational damage to the Company.
13. By looking at these two factors (probability and impact) operators can get the final 'inherent risk' – the risk that resides in the essential nature of a product, feature, payment method characteristic etc., which must be addressed to avoid that risk materializing and/or to mitigate the effect of that materialization.
14. After defining the inherent risk level and analysing threats and vulnerabilities, the operators should define adequate control measures to be applied to each identified risk to bring the risk to within an acceptable level. That acceptable risk level is the **"residual risk"** i.e., risk level after the application of the controls. A residual risk level should also be calculated by combining the probability of the risk materializing and the resulting impact or damage, after control measures have been applied. What remains, the residual risk, is the accepted level of risk after application of AML/CTF controls. Residual risk scores should be monitored and re-assessed where there is a change in the original risk scoring.

4. Business Risk Assessment

15. One of the key documents that operators should develop is a Business Risk Assessment ('BRA'). The BRA is an essential document for building AML/CTF controls, since it should contain a list of the most important risks to which an organization is exposed, mitigating measures – controls, and a risk assessment. Based on the BRA, each operator should develop AML/CFT policies and procedure delineating the operators' approach towards combatting the ML/TF risks as identified in the BRA, and controls considering the requirements emanating from the applicable law of the market(s) of operation. The BRA allows for resources to be invested and applied where they are

most required. At a high level, the controls to manage and mitigate ML/TF risks should be aimed at the:

- Prevention (e.g., CDD measures).
- Internal control systems (e.g., employee training and screening).
- Detection (e.g., monitoring of suspicious activity).
- Reporting.
- Record-keeping to facilitate investigations.

16. Operators should take a holistic view on ML/TF risks on a business-wide level and not only at an individual-customer level. A Business Risk Assessment ('BRA') must analyse the business threats and vulnerabilities to identify, which areas present a higher ML/TF risk. The BRA is therefore the foundation of the risk-based approach. This must be distinguished from the Customer Risk Assessment ('CRA'), which as discussed further below is a risk assessment conducted upon each specific customer relationship as part of the operator's Customer Due Diligence ('CDD') obligations.
17. The application of a reasoned and well-articulated BRA will justify the judgements made regarding managing potential ML/TF risks through the assigned controls.
18. The BRA is not intended to be a static assessment but must be re-assessed on, at least, an annual basis, or earlier, depending on how the circumstances develop (e.g., how the business changes for example through new products or markets offered, new technology, changes in relevant regulations, etc.), and how the threats evolve. As such, operators must use their judgement, knowledge, and expertise to undertake an appropriate BRA for their specific organisation, structure and business activities.

4.1. Customer Risk Assessment

19. The core of a risk-based approach includes the assessment of the operator's customers, via the Customer Risk Assessment (CRA), since it provides operators with an understanding of the risks coming from a customer relationship, and therefore allows to adequately address such risks via the application of different measures. The level of risk can most commonly be deemed to be low, medium, or high.
20. Various indicators influence the risk of ML/TF taking place via online gambling operators. The key risk factors, which operators need to consider in carrying out the CRA can be grouped into:
    a) **Customer risk:** determining the potential ML/TF risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. This is dependent on the type of customer. Categories of customers whose activities may indicate a higher risk include PEPs, high risk occupations, high spenders, disproportionate spenders, etc.
    b) **Interface and delivery channels:** this risk relates to the different channels through which the operator establishes a business relationship with a customer. Business relationships that do not take place face to face, such as online gaming, pose a higher ML/TF risk (e.g., risks of identity theft and other fraudulent acts relating to impersonation). However, due to the technological mitigating measures and controls put in place, this risk can be mitigated to an acceptable level. Operators need to ensure that their internal procedures properly account for that.
    c) **Product risk:** certain gaming products may be deemed as more attractive for criminals to launder funds due to their specific nature. This may be due to the actual or perceived ease to disguise illicit funds. Games with hedging can be used to secure a return on wagers placed, whilst disguising the activity as normal gameplay for entertainment purposes. Where the outcome can be influenced by the customer such as in the case of poker,

operators need to monitor for signs of individual misuse or collusion. Transfer of funds between the accounts of different players within the same operator presents a risk factor, which must be considered due to the peer-to-peer nature. Operators should classify the products offered in accordance with the 'gaming type' (e.g., fixed odds games with or without hedging, sports betting, and peer-to-peer games) to assess the vulnerabilities associated with the particular product. In general, it is considered that P2P games are of a higher risk, while fixed odd games without hedging are of a lower risk.

d) Payment method/transaction risk: this relates to the degree of anonymity and traceability that different payment methods offer. Some payment methods are more vulnerable to criminal exploitation because they provide customers with the possibility to mask their identity and their source of funding, such as pre-paid vouchers for depositing on the player account. These pose a high ML/TF risk as the purchaser of the vouchers might not be legitimate and it is difficult to carry out the same level of checks as may be performed on accounts held with financial institutions. On the other hand, where a customer transfers funds from a bank account or a card linked to a bank account held in their name with an institution established in a reputable jurisdiction, the ML/TF risk is low. This is the case since credit or financial institutions are themselves subject persons and as part of their CDD obligations they monitor customer account and card activity on an ongoing basis.

d) 1. Specific provisions on cryptocurrency: Acceptance by the EU regulated online gambling industry of cryptocurrency is in its infancy and very few operators do so. As a new payment method, it necessitates vigilance and robust risk assessment and compliance methods. The approach proposed, should thus be future proof. The use of cryptocurrency as a payment method is usually subject to specific requirements of local laws due to their high-risk nature. Particular attention needs to be paid to customers who might be funding their play through money derived from crypto assets. Cryptocurrency will, however, be subject to EU laws in the near future, which should mitigate some of the associated risks.[2] It should be specified that depositing money on the account through crypto assets does not always leave, or otherwise complicate, the funds' audit trail, and allow the customer to operate with a degree of or complete anonymity such as virtual financial assets. However, special attention needs to be paid to cryptocurrency in respect to its use as a payment method, as to ensure traceability and source of funds.

Online gambling operators must not act as cryptocurrency exchange platforms. The case of accepting FIAT payment methods that may process cryptocurrency, necessitates additional vigilance. The associated risk is mitigated by the fact that payment providers are obliged entities under AML laws, but operators should ensure that payment service providers they work with have a robust AML understanding and procedures.

Gambling operators should risk assess the PSPs AML approach. Additionally, it should be noted that certain payment providers are riskier than others, especially in the case where they accept and process cryptocurrency, and care should be taken that only reputable PSP providers, registered in the EU/EEA are used to serve European customers.

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets and Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.

Strong internal controls are required when accepting cryptocurrency as a form of payment. Robust compliance with the rules put forward by the regulator is necessary.

e) **Geographical risk:** Some countries pose an inherently higher ML/TF risk than others, as should be established via the jurisdictional risk assessment. Operators should risk-rate all relevant countries against reliable and internationally credible sources (e.g., the Basel Index, Transparency International Index, FATF monitored jurisdictions and Global Sanctions listings). Countries with a high-level of corruption, lax or inexistant AML/CFT frameworks, low level of transparency/accountability or which are subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction, are risk rated as high, whilst countries with better risk metrics are rated as medium or low. Operators need to assess any connections, which customers might have with higher risk countries (for example, linked to their citizenship, country of business, country of residence, etc.).

21. Once the level of risk is determined, risk- specific procedures must be employed when dealing with the customer and adequate CDD measures per risks exhibited. Policies, controls, and procedures must be put in place accordingly and must have in-built flexibility to address the specific risk posed by the customer. Thus, a risk management process should exist that covers identifying the risk, conducting the risk assessment, and ensuring appropriate systems are in place (to identify, address and mitigate the risk).
22. The CRA must be reviewed from time to time depending on the risk level and where there are circumstances, which materially affect the initial assessment, and which may, therefore, warrant changes in the customer risk rating.

5. Customer Due Diligence (CDD)

23. The best protection against abuse by money launderers is to know your customer – this is done through Customer Due Diligence (CDD). CDD refers to all processes and controls applied to ensure that at all stages of the business relationship the operator has a clear understanding of who the customer is and their behavioural pattern.
24. Operators should apply CDD:
    - Upon certain pre-defined thresholds as determined in applicable laws.
    - When the operator has knowledge or suspicion that the funds being used are proceeds of criminal activity, irrespective of any threshold.
    - At appropriate times and on a risk-sensitive basis, including at times when the operator becomes aware that the relevant circumstances have changed.
    - When doubts arise about the veracity or adequacy of previously obtained customer identification information.
25. The main aim of CDD is to make sure that the operator has effective mechanisms in place to:
    - Identify a customer.
    - Verify customer identity.
    - Keep customer information up to date.
    - Establish the purpose and intended nature of the business relationship along with the customer's business and risk profile.
    - Monitor customer activity on an on-going basis to reduce fraudulent and ML/TF activity during the life cycle of a customer.
26. Identification should always be conducted on establishment of a business relationship. However, in relation to all other CDD checks (especially verification), their extent, timing and quantity of

information required, will be determined based on the customer risk assessment and local requirements.

27. For the online gambling sector, CDD (including the CRA) should be carried out at the 2000[3] EUR threshold.[4] This means that operators can postpone verification until this threshold is met.
28. Therefore, operators should define in their AML/CFT policies and procedures:
    - In which instances they will conduct CDD (based on monetary and non-monetary thresholds, etc.).
    - The extent of CDD to be applied depending on the customer risk assessment.
    - Timelines in which customers should provide documents requested for the purpose of CDD (grace period) and status of the customer during this period (e.g., any restrictions, etc.).
    - Actions to be taken if customers do not cooperate during the CDD process (e.g., consideration of lodging a suspicious activity report, termination of business relationship).
29. An important specific in the context of the gaming industry, is that the purpose and intended nature of the business relationship is self-evident since most customers use the services for entertainment purposes, so operators do not need conduct any further checks to understand why the customer is opening an account. However, during the relationship operators need to follow the customer activity, and on a risk-basis establish the customer's business profile (gathering information about source of wealth and source of funds) so they can properly assess a customer's activity.

5.1. Steps in the CDD process: Identification

30. A sound CDD program should have reliable customer identification and account-registering procedures that allow the operator to establish the identity of the player. All prospective customers must be subjected to the process of identification upon registration, which involves the gathering of minimum necessary personal data of the player (which may be tailored to the risk posed by the customers). Customers shall be prohibited from opening anonymous accounts or accounts under fictitious names and where such an account is identified action should be taken.
31. Moreover, although they are not necessarily part of the registration process (usually, they are mandated by local laws very early after the registration) it is important to mention some specific checks that are very relevant for gambling operators. One of the very important checks concerns Politically Exposed Persons (PEP). PEP checks are necessary to determine whether a customer is a politically exposed person. PEPs pose a high risk of ML/TF; therefore, EDD measures are necessary to mitigate the potential risks. Each PEP does not have the same level of risk; thus, gaming operators are required to assess and determine the level of ML/TF risk posed by that particular PEP. Based on the resulting CRA, gambling operators should consider the level of EDD measures required for each case depending on the risk. Agreement to accept a PEP as a client should be left to senior management. All procedures regarding PEPs should apply to their family members and close associates as well. Screening for PEP status should be done with some regularity to ensure customers status has not changed and an assessment of the continued risk should be done.
32. Also, the operator should always check a customer for any economic sanctions imposed on a particular country/individual or on all persons residing within any country or on persons who are associated with certain political, religious, or criminal organizations. Operators are prohibited from

[3] *Directive EU 2015/849, Article 11 (d).*
[4] *This threshold is differently calculated in different jurisdictions. For example, in some countries comprehensive CDD is required at registration and therefore there is no regulatory threshold for further CDD, but it is rather up to Operators to define their internal thresholds for CDD. Conversely, in other markets a basic CDD (identification) is conducted at registration and the full CDD (verification) is conducted at the 2000 EUR threshold (or lower threshold if defined by the regulator). However, irrespective of any thresholds, operators should be able to detect suspicious ML/TF activity even before reaching the 2000 EUR (or any other) threshold.*

carrying out business (and are required to immediately block any accounts) with any person who is subject to a financial sanction. On the other hand, persons with a strong connection with a sanctioned country should be classified as high risk and subject to EDD. The same applies to all third countries identified by the European Commission as high-risk third countries. Therefore, operators should develop their jurisdictional risk assessment that will include classification of countries per risk level based on different criteria (see below).

33. In addition, operators can also check media with due regard to the quality and independence of sources checked and the nature of the offence reported on, since previous criminal records on customers can imply important concerns to be considered and adequately addressed in line with local laws.
34. Finally, in the gambling industry, each customer may register only one account per brand under a license. This requirement is beneficial not only for AML/CFT purposes but also from a fraud perspective, since it enables operators to have visibility of the entire customer activity, preventing any fraudulent attempts to bypass the controls. For customers who have more than one account per operator, operators should have a link between those accounts to identify any holistic risks. This is also needed to ensure that for when the 2000 EUR CDD limit is reached, it would be applied across the entire operator's activities and not only per brand. Additionally, e, checks for customers holding duplicate accounts are important to minimize risks of bonus abuse, ID fraud, and participation in illegal rented ID schemes, designed to defraud operators.

5.2. Steps in the CDD process: Verification

35. The identity of customers should be verified using reliable, unexpired, independent source documents, data, or information, for example by requesting a copy of a government issued identity document such as an ID card, passport, residence permit, driver's license or through electronic means such as e-ID, bank ID, etc.
36. The timing and extent of verification can vary depending on the risk level of the customer. This should be done according to local requirements for standards of verification.
37. Verifying personal data provided should be done in a robust way to ensure reliability. Electronic verification methods are preferred to be used should the jurisdiction permit for their use. Electronic verification methods include e-ID, Bank ID schemes, and reliable public or commercial electronic databases. Extra care should be taken, particularly when using commercial databases, to ensure that the specific person not only exists but is in fact the operator's customer.

5.3. Steps in the CDD process: Enhanced Due Diligence

38. Where the risk associated with a business relationship is likely to be low, to the extent permitted by applicable law, operators may be able to apply simplified customer due diligence measures (SDD). Where the risk associated with a business relationship are increased, operators must apply enhanced customer due diligence measures (EDD) to manage and mitigate those high risks appropriately (e.g., where transactions are complex, unusually large, and conducted in an unusual pattern).
39. In line with the risk-based approach, EDD are extra CDD measures undertaken by the operator to address any heightened customer risk factors, for example: customer, geography, product/service/interface risks. EDD is conducted by asking customers to provide identity documentation or general information that may be necessary to achieve certain objectives during the course of the customer relationship, such as:

- To additionally verify and validate the customer identity.
- To update more regularly the information held on customer.
- To obtain additional information evidencing customer's location, occupation, source of wealth / funds.
- To obtain additional information on the intended nature of the business relationship.
- To obtain approval from senior management to commence or continue the business relationship.
- To increase the number and timing of controls applied.

40. In their AML/CTF policies/procedures, operators must provide guidance on how to recognize high-risk scenarios and examples of additional information to be sought, and of any monitoring carried out.

5.4. Steps in the CDD process: Ongoing customer due diligence

48. Operators have the duty to conduct ongoing monitoring of all customer relationships. The initial satisfactory identification of a new customer is not, by itself, a sufficient reason to mitigate ML/TF risk. Moreover, certain aspects of the customer profile cannot be established at the time of the onboarding of the customer, such as the customer's future activity. The purpose for ongoing monitoring is two-fold:
    a) To use reasonable endeavours to ensure documents, data or information held are kept up to date, relevant, and questioning the veracity of the data held whenever any inconsistencies are identified.
    b) To scrutinize the transactions undertaken during the relationship to ensure that they are consistent with the operator's understanding of the customer risk profile. Through monitoring of customer transactions and activity, operators should be in a better position to:
        - Identify behaviours/transactions, which diverge from the usual pattern, or do not fit with the customer's profile, or are otherwise not in line with what is normally expected from the customer.
        - Identify suspicious activity in relation to which a suspicious transaction report ('STR') needs to be filed with the relevant authority.
        - Determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the operator's risk appetite.
49. Any unusual activity that departs from habitual patterns of players should be investigated further. Examples of this may be unusually large volumes of transactions (if inconsistent with player activity or information operators have on the player) or unusually large amounts being deposited (this can also indicate possible concerns relating to problem gambling). Measures, such as obtaining sufficient information and documentation on the matter can be taken when unusual activity is observed. This may also include establishing the customer's source of funds.

6. Relationship with safer gambling and sports integrity

50. The gambling industry is a highly regulated industry that is subject to many strict legal obligations coming from applicable local laws and licencing obligations, that are trying to achieve goals that are close to AML/CTF ones. The most important of these are responsible gambling and fighting match-fixing. Therefore, the relationship between these should be explained.

51. Operators should note that given the wide scope of AML checks, reviews undertaken by the operator's AML team can also discover potential problem gambling signs. Therefore, whenever such signs are identified, this must be escalated to the safer gambling ('SG') team for further review. On the other hand, some of new regulatory tendencies in SG (such as affordability check) can also be of use to AML team. For that reason, it is important that operators recognize these issues of common interest and share information between relevant teams for these purposes, if that is compatible with local data protection laws.
52. When it comes to match-fixing, this topic is commonly misunderstood as an indication of AML issues. Match-fixing in many countries is criminalized or sanctioned under other local legal instruments and presents a dishonest and fraudulent practice, which also defrauds gambling operators from funds and must be prevented. Therefore, indications of match-fixing should not be automatically taken as an indication of ML/TF. However, in the same way as noted for SG, this information can be of relevance for AML teams and therefore operators should ensure they have adequate processes in place to allow for the internal sharing of such information that might be of importance for other teams.

7. Lack of cooperation during CDD

53. CDD is a crucial process for mitigating ML/TF risks and customers should be aware of the importance of this process. Therefore, cooperation of customers, as well as their behaviour, are also an important factor that should be considered in the risk assessment process. When CDD cannot be completed, the attempts to obtain CDD should be duly documented as well as the reasons for the inability to complete the processes, such as for example, lack of answer by the customer to information requests. The player should be given opportunity to provide the necessary evidence. Where the operator is unable to complete or apply the required CDD measures in relation to a particular customer, operators should desist from carrying out any transaction until CDD is completed or act in accordance with relevant local laws. Normal business can resume only if CDD is complete within the grace period (if such exists). If not, the business relationship should be discontinued.[5] Operators should be mindful that non-cooperation during CDD could potentially be an indication of ML and therefore, in each such case the operator's staff and particularly the front-line operational teams should assess if red flags are present. If indication is found to exist for filing an STR submission, the case should be escalated to the MLRO for their decision.

8. Suspicious Transaction Reporting (STR)

54. Well-founded suspicions of money laundering should lead to a suspicious transaction report (STR) in accordance with instructions from the responsible Financial Intelligence Unit (FIU). STR reporting is an important obligation in the AML framework and therefore each operator should develop policies/procedures and an internal channel for reporting the STR. Sound guidance for the MLRO on how to decide upon and handle STRs (in line with local applicable law) should also be developed. One of the important aspects of these internal documents should be the protection of the confidentiality of the reporting person and confidentiality of the STR, as well guidance to employees on how to act to avoid tipping-off the player. When submitting STRs is it crucial that operators follow procedures issued by the relevant FIAUs and that they cooperate with them in this process, especially when it comes to the questions of handling the customer account.

[5] *This can take the form of suspension, freezing or closing of the account.*

55. The customer's activities should then be considered wholistically when conducting any assessments, especially when operators have multiple brands in one jurisdiction ensuring any reporting is done so under the applicable operator licence for each brand and in accordance with data sharing and privacy laws.
56. Although operators should encourage employees to report any suspicious of ML/TF, even when they are not sure, this reporting should be distinguished from reporting any other irregularities that might be in contradiction with local AML/CTF laws. Further, operators must have in place appropriate whistleblowing procedures for their employees, or persons in a comparable position, to report any contravention of applicable AML law internally through a specific, independent, and anonymous channel, proportionate to the nature and size of the operator. This is intended to protect individuals from any retaliation, particularly from adverse or discriminatory employment actions, and to provide such whistle-blowers with appropriate protection, particularly regarding their right to protection of personal data and their rights to effective judicial protection and representation.

9. Record-keeping requirements

57. Operators should maintain, for the duration prescribed in applicable local law, all transaction records necessary to reconstruct individual transactions so that these can be produced as evidence in response to investigations carried out by relevant authorities. These records shall, at least, include:
    - Details of how compliance has been monitored by the operator.
    - Information or other material concerning possible ML/TF not acted upon by the operator, with reasoning why no further action was taken.
    - Customer identification and verification information, supporting records in respect of business relationships and all other relevant data of customer profile.
    - Employee training records.
    - Internal reports and external STRs.
    - Contact between the operator and the relevant authorities.

10. Outsourcing and third-party reliance

58. Outsourcing performance of the money laundering obligations to a third party can be a risk factor, thus control and accountability needs to be ensured. Risks should be assessed in the BRA. Depending on the role of the third party, such cooperation may be classified as either a reliance or an outsourcing business relationship.
59. Outsourcing is defined as the use of a third party to perform a process, service, or activity on behalf of the operator, which would otherwise be undertaken by the operator itself. The outsourced entity applies the CDD measures in accordance with the operator's policies/procedures and subject to the operator's control of the effective implementation thereof. Therefore, whilst the outsourcing of AML/CFT obligations is permitted for specific activities as defined in the local law, the operator must ensure reliability of the entity entrusted. Moreover, the operator must carefully consider which functions can, and conversely, which functions cannot be outsourced in line with local applicable law, to ensure appropriate execution of their licensing obligations as well as adherence to anti-money laundering laws. Monitoring of the execution of the tasks outsourced must be undertaken with some regularity, in proportion to the complexity and importance of the latter. All these details should be covered in agreement with the entity to which specific activities are outsourced.
60. In a 'third-party reliance' scenario, the third party, which must be an entity in an EU Member State or a reputable jurisdiction which is subject to AML/CFT requirements and supervision equivalent to

those required in terms of applicable EU legislation, will usually have an existing business relationship with the customer, which is independent from the relationship of the customer with the relying operator, and would apply its own procedures to perform the CDD measures. However, even if the operator is relying on third party CDD measure, the relying operator remains ultimately responsible for compliance with its CDD obligations. Therefore, in these scenarios it is recommended for operators to ensure that:

- They do not rely on third parties established in high-risk jurisdictions (unless the third party is a branch or majority-owned subsidiary of the EU-based operator and is subject to group-wide policies and procedures).
- The cooperation is subject to a contractual agreement confirming that the third party accepts being relied upon.
- The third party will provide copies of any CDD documents or other information obtained, as soon as practicable, upon request.
- The third party is regulated, supervised, or monitored for, and has measures in place for compliance with CDD and record-keeping requirements.

61. Finally, it is worth mentioning one common business practice in the gambling industry that is usually misinterpreted in the context of outsourcing/reliance - cooperation with affiliates. Affiliates are third party entities that are cooperating with operators in marketing activities. Therefore, affiliates most commonly act as providers of marketing services or acquisition services (by bringing/redirecting customers to the operator's website). In such cases, and especially where an affiliate directs a customer to the operator, it is important to note this situation should not be considered as an "intermediary scenario" and influence elevating risk score, since CDD is always done by the gambling operator themselves.

11.Training

62. It is necessary that all relevant employees (the ones working on relevant positions such as transactions execution, AML/Fraud, etc.) of gambling operators, undergo AML training in accordance with their position and responsibilities. Generally, relevant employees should be aware that money laundering risks exist and what internal procedures need to be adhered to in the context of fulfilling AML obligations for their specific role and level.
63. Specifically, all relevant employees should receive training on:
    - The vulnerabilities of the gaming sector to ML/TF.
    - The identification of unusual transactions.
    - Red flags to consider when detecting and reporting suspicious activities.
64. Training needs to be targeted, well planned, and proportionate to the size and type of gaming operator.

12. Monitoring and implementation of the Guidelines

65. EGBA members have six months to implement the Guidelines into their AML Compliance systems from the date of their publication. Any signatory, who is not an EGBA member will have six months from the date of signing up to the Guidelines to implement.
66. Once a year signatories will present a report on their implementation of the Guidelines at the latest on the date of publication in that given year.
67. Every year signatories will present their reports and discuss any changes to the Guidelines on an annual EGBA AML workshop to be held after reports are submitted.

13. Glossary

1. AML - Anti-Money Laundering
2. BRA - Business Risk Assessment
3. CDD - Customer due diligence
4. CFT - Combatting the financing of terrorism
5. EU - European Union
6. FIAU - Financial Intelligence Analysis Unit
7. FATF - Financial Action Task Force
8. FIs - Financial Institutions
9. FIUs - Financial Intelligence Units
10. KYC - Know-your-customer
11. ML - Money Laundering
12. SG- safer gambling
13. STRs - Suspicious Transaction Reports
14. TF - Terrorist Financing
15. Operator/gambling operator/online gambling operator are used interchangeably.
16. Player and customer are used interchangeably.

Contact:

Dr Ekaterina Hartmann
Director of Legal and Regulatory Affairs

T: +32 2 554 0890
E: ekaterina.hartmann@egba.eu

EGBA | European Gaming & Betting Association