

IGE

**Interactive Global Entertainment B.V.
Anti-Money Laundering and Counter-Financing of
Terrorism Policy and Procedure**

B2B Type

1. Contents

1. Contents	2
2. Abbreviations	3
3. Definitions	4
2. Background and Approach	6
2.1. Introduction	7
2.2. The Company	7
2.3. Objective	7
3. Policy	8
3.1. Procedures	8
3.2. Responsibilities	9
3.3. Importance of compliance culture	9
3.4. Review of effectiveness	10
4. Customer Due Diligence (CDD)	10
4.1.1. Verification of a legal entity (Company)	10
4.2. On-going monitoring	11
5. Risk Assessment (for clients and outsourcing entities)	12
5.1. Low-Risk Scenarios	13
5.2. Moderate-Risk Scenarios	13
5.3. High-Risk Scenarios	13
5.4. Enhanced Due Diligence (EDD)	13
5.6. Factors we look at on our risk assessment for clients/outourcing entities	14
6. Risk Assessment Procedure	15
6.1. Procedure: Client/Service Provider Onboarding and Contract Approval	15
7. Staff Education, Training and Development	17
7.1. Importance for AML/CTF risks	17
7.2. Integrity	17
7.3. Employees' recruitment	18
7.4. Compliance with Company policies and procedures	18
7.5. Technological Developments	18

Version Tracking, Release and Changes

Document Title	Anti-money Laundering and Counter Financing of Terrorism Policy and Procedure
Classification	Internal, Confidential

Version Control	Last Updated	Owner	Date of Approval	Changes
v1	06-08-2024	Director	06-08-2024	new policy
v1.1	14.11.2024	Director	14.11.2024	5.6 point 6 and 8 were updated with specific information about tools used for PEP and sanction screening.

2. Abbreviations

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering and Counter Financing of Terrorism
AML4D	Directive (EU) 2015/849
AML5D	Directive (EU) 2018/843
CDD	Customer Due Diligence
CFT	Counter Financing of Terrorism
CV	Curriculum Vitae
FT	Financing of Terrorism
KYC	Know Your Customer
ML	Money Laundering
ML/FT	Money Laundering and Financing of Terrorism
PEP	Politically Exposed Person

3. Definitions

The following terms used in the policy and procedure have the following meaning:

Beneficial Owner (BO) - any natural person(s) who ultimately own(s) or control(s) the customer and, or the natural person(s) on whose behalf a transaction or activity is being conducted, and:

(a) In the case of a body corporate or a body of persons, the beneficial owner shall consist of any natural person or persons who ultimately own or control that body corporate or body of persons through direct or indirect ownership of 25% plus 1 or more of the shares or more than 25% of the voting rights or an ownership interest of more 25% in that body corporate or body of persons, including through bearer share holdings, or through control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements consistent with European Union law or equivalent international standards which ensure adequate transparency of ownership information:

Provided that a shareholding of 25% plus 1 share or more, or the holding of an ownership interest or voting rights of more than 25% in the customer shall be an indication of direct ownership when held directly by a natural person, and of indirect ownership when held by one or more bodies corporate or body of persons or through a trust or a similar legal arrangement, or a combination thereof:

Provided further that if, after having exhausted all possible means and provided there are no grounds of suspicion, no beneficial owner in terms of this paragraph has been identified, subject persons shall consider the natural person or persons who hold the position of senior managing official or officials to be the beneficial owners, and shall keep a record of the actions taken to identify the beneficial owner in terms of this paragraph.

(b) In the case of trusts, the beneficial owner shall consist of:

- i. The settlor;
- ii. The trustee or trustees;
- iii. The protector, where applicable;
- iv. The beneficiaries or the class of beneficiaries in whose main interest the trust is set up or operates as may be applicable; and
- v. Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

(c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the beneficial owner shall consist of the natural person or persons holding equivalent or similar positions to those referred to in paragraph (b).

Business Relationship - means a business, professional or commercial relationship, which is expected to have an element of duration, between two or more persons, at least one of which is acting in the course of either relevant financial business or relevant activity.

Financing of Terrorism (FT): Financing/Funding of terrorism is the process of making monies or other assets available to support, directly or indirectly, terrorist activities. The funds to support the terrorist activity may be derived from both legitimate or illegitimate sources, or a combination of both. FT is committed when a person receives, provides or invites another person to provide money or other property with the intention to be used, or which s/he has reasonable cause to suspect that it may be used, for the purpose of terrorism. This offence can also be committed by any person who facilitates the retention or control of terrorist property by entering into or becoming concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property:

- By concealment;
- By removal from the jurisdiction;
- By transfer to nominees; or
- In any other way.

Money Laundering (ML) - Money Laundering can be explained as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to make these illegal proceeds look legitimate and 'clean'. The laundering process usually follows three stages:

- The placement stage: Introducing the money or assets derived from the criminal or illegal activity into the financial system. This is usually done after the funds have been broken down into smaller, less conspicuous amounts;
- The layering stage: The illegitimate funds are moved (ex by investing them or moving them to other jurisdictions) in order to distance them from the original source; and
- The integration stage: In this stage, the funds are 'collected' or entered back into the economy, appearing as clean funds.

Politically Exposed Person (PEP) - a natural person who performs or has performed significant duties of prominent public authority, other than middle ranking or more

junior officials. Family members and known close associates of such a person are also considered as PEPs.

Persons carrying out significant duties of public authority are:

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers and Parliamentary Secretaries;
- Members of the Parliament or similar legislative bodies;
- Members of the governing bodies of a political party;
- Members of superior, supreme and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors, or of the boards of central banks;
- Ambassadors, *chargé d'affaires* or other high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory boards of state-owned enterprises; and
- Anyone exercising a function equivalent to those set out above within an institution of the European Union or any other international body.

A 'family member' of a PEP means:

- His/her spouse;
- A partner equivalent to the spouse, in accordance with the law of the country of residence or a person who has had at least one year's common household with him/her as at the date of conclusion of the transaction;
- His/her children and their spouses or partners within the meaning of the preceding paragraph;
- His/her parents.

A 'known close associate' of a PEP means:

- a natural person who has close business relations with the person performing significant duties of public authority or who together with the person performing significant duties of public authority is the joint beneficial owner of a legal person or contractual legal entity;
- a person who, as the beneficial owner, fully owns a legal person or contractual legal entity that is known to have been established for the benefit of a person performing significant duties of public authority.

Where a PEP is no longer entrusted with a prominent public function, the continuing risk posed by that person shall be taken into account and s/he is still deemed to be a PEP for at least 12 months from the termination of such role.

2. Background and Approach

2.1. Introduction

This document has been compiled to create a core policy document to govern the various developed procedures and principles of the Company in one central location. This represents and ensures a prompt and up-to-date determined effort by the board of directors, senior management and the Company towards creating an appropriate framework and strategy to effectively prevent the misuse of the Company and its products and/or services for Money Laundering (ML) and Financing of Terrorism (FT).

2.2. The Company

Interactive Global Entertainment B.V. is a company registered under the Laws of Curacao. The Company has its registered office at Dr. M.J. Hugenholtzweg 25, Willemstad, Curacao. Chamber of commerce registration #153827.

2.3. Objective

The Company has set out this anti-money laundering (AML) and counter-terrorism financing (CTF) policy and procedure that is applicable to all staff to help prevent and detect potential ML/FT. The Company takes a zero-tolerance approach to ML/FT and other such financial crimes .

The objective of this document is:

- To provide a high-level assessment of the operations and services provided by the Company and the risk that they may pose to ML/FT; and
- To set out the policies, procedures, systems and controls necessary for the Company to meet the obligations.

The Company's approach is based upon:

- Directive (EU) 2015/849 (AML4D);
- Directive (EU) 2018/843 (AML5D);

- Curacao Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction
- Any other regulations, codes of practice, guidance notes, rules and directives applicable to the Company.

The Company is responsible for assessing its ML/FT risks and ensuring the appropriate implementation of a risk-sensitive policy and procedure within the business.

3. Policy

It is the Company's policy that the European and Curacao statutory and regulatory obligations to prevent ML/FT are to be met in full and the Company is committed to meeting and where possible exceeding such obligations.

Positive management action will be exercised in order to minimise the risk of the Company's services and gaming activities being abused for the purposes of laundering funds associated with criminal activity.

The Group will not continue established relationships with participants or business partners whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant or business partner relationship where the participant's/partner's conduct gives reasonable cause to believe or suspect involvement with illegal activities.

The Company's vigilance, policy and procedures are based upon the legislations and regulations referred to above and associated guidance issued by the European and Curacao laws.

3.1. Procedures

The purpose of these procedures is to assist the officers and staff of the Company in fulfilling their obligations under the European and Curacao statutory and regulatory obligations, thus ensuring effective implementation of the AML/CFT measures and mitigating risks. These will be maintained to ensure the following:

The risk of the Company's products or services used as a vehicle for ML/FT is minimised;

- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations;
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation;
- The Company's ongoing monitoring systems are implemented and regularly reviewed; and
- Appropriate knowledge and awareness are maintained regarding EU's and Curacao's statutory and regulatory obligations and in the gaming industry.

3.2. Responsibilities

The Company's director and senior management are responsible for various matters such as:

- Setting the principles for the prevention of ML/FT, policies and supporting procedures;
- Ensuring that the Company's policies and procedures are designed and operate effectively to manage the risk of the business from being used for financial crime and to fully meet the requirements of the AML/CFT regime; and
- Approve the departments' documented operational procedures which procedures must be in line with the AML/CFT (among others) and as per requirements of the regulatory and supervisory authorities.

3.3. Importance of compliance culture

Detailed and comprehensive policy and procedures are not sufficient to forestall the facilitation of ML/FT. If the compliance culture of the Company is weak, then they will be ineffective.

The board of directors and senior management are to encourage a compliance culture by:

- Demonstrating support for compliance with these policies, procedures and with sound corporate ethics;
- Providing support for staff in their AML/CTF efforts;
- Demonstrating no tolerance of clients and other external parties who are not transparent or are not cooperative in AML/CTF efforts;
- Encouraging risk awareness in staff;

- Encouraging a spirit of compliance;
- Fostering awareness through training;
- Taking the appropriate action in respect of breaches;
- Encouraging the raising of concerns by employees at all levels; and
- Providing the necessary resources for proper application of procedures and to address concerns.

3.4. Review of effectiveness

The board of directors and senior management are to review and assess the culture within the Company and the effect of human factors on the effectiveness of procedures as part of its risk review.

4. Customer Due Diligence (CDD)

4.1.1. Verification of a legal entity (Company)

In cases where the Company enters into a business relationship or an occasional transaction with a legal entity, the Company must first identify the client by obtaining the below information:

- Official full name of the Company;
- Company registration number;
- Company's date of incorporation or registration;
- Company's registered address of the principal place of business.

After the client has been identified, the Company should verify all the information obtained by referring to appropriate independent and reliable sources. These identification details can be verified by obtaining either of the below:

- Certificate of Incorporation;
- Company registry search;
- The most recent version of the Memorandum and Articles of Association or another constitutive document including all shareholders and directors;
- Group structure chart.

These documents may be retained either in original (where applicable), as downloaded copies from official registers or as certified true copies. In the case of certified true copies, additional checks and safeguards will be applied to ascertain the robustness of the verification measures. Furthermore, the Company will also verify the legal status of the client by confirming that the client has not been, or is in the process of being dissolved, struck off, wound up or terminated. Supporting documentation confirming the legal status of the client will also be retained.

In addition to the above, the Company is also obliged to identify the Directors of the client, understand the ownership and control structure and identify and verify the beneficial owners. These identification details can be verified by obtaining either of the below:

- Valid Passport / Identity Document
- Official document confirming the current full residential address (not older than 12 months)

It is imperative to note that the ownership and control structure should lead up to any natural persons.

4.2. On-going monitoring

On-going monitoring is conducted by the Company in order to ensure that the information collected about the client at the onboarding stage, is still current and valid and to determine whether there is any suspicious activity that requires further investigation. The on-going monitoring of a business relationship includes, but is not limited to:

- Ensuring that the documents, data or information held by the Company are kept up to date. Documents should be retained and updated as they expire for the whole duration of the business relationship. Upon termination of the relationship, the documents should be retained for a period of five (5) years after the end of a business relationship or an occasional transaction, as per current regulatory requirements.
- On a risk-based approach, the Legal Department will review the documents for all customers to ensure to check the validity of the documents. Accordingly, the Legal Department will take care of scheduling the documents needed to be updated throughout the business relationship with

the customer. The Legal Department will contact the clients accordingly to ask for an update of the documents.

- If the client does not respond reply to the documents request within 6 months from the initial request, the company will consider limiting the services or closing the service (temporary) until the pending document is provided.

5. Risk Assessment (for clients and outsourcing entities)

At Interactive Global Entertainment B.V., our commitment to AML compliance extends to a meticulous risk assessment process during client onboarding and when engaging outsourcing entities. We employ a risk-based approach that takes into account various factors to gauge the potential AML risks involved. For instance, when onboarding a new client, we consider factors such as the jurisdiction of operation, the nature of the gambling services they offer (e.g., online casinos, sports betting), and the expected transaction volumes. For example, if we onboard a client operating in a high-risk jurisdiction known for lax AML regulations, we conduct enhanced due diligence procedures, such as more extensive background checks and monitoring of their financial activities. Additionally, we evaluate the client's source of wealth, identifying any unusual or inconsistent financial behaviors.

Similarly, when onboarding outsourcing entities, we assess their AML controls and procedures rigorously. For instance, if we engage a third-party payment processor to handle transactions, we evaluate their AML policies and practices. We ensure that these entities maintain AML programs that align with our own standards and the regulatory requirements for AML. If an outsourcing entity operates in a jurisdiction known for weak AML enforcement, we exercise prudence by implementing additional monitoring and reporting mechanisms to mitigate potential risks. Furthermore, we continuously monitor these entities to ensure their AML controls remain effective and in compliance with our policies and EU regulations. Our approach to risk assessment allows us to tailor our AML measures to specific scenarios and prioritize resources effectively to prevent money laundering and uphold the highest standards of AML compliance in the gambling industry.

At Interactive Global Entertainment B.V, our AML policy employs a multi-tiered approach to assess and define the levels of risk associated with client onboarding and the engagement of outsourcing entities.

5.1. Low-Risk Scenarios

Definition: These are situations where the potential AML risk is minimal. They typically involve clients or outsourcing entities from jurisdictions with strong AML regulations, straightforward business models, and well-documented licences.

Examples: Onboarding a client operating an online casino in a jurisdiction with stringent AML laws, or engaging a payment processing outsourcing entity from a reputable financial center.

5.2 Moderate-Risk Scenarios

Definition: These scenarios involve a moderate level of AML risk. This might include clients or outsourcing entities operating in jurisdictions with less robust AML controls, complex ownership structures, or moderately high transaction volumes.

Examples: Onboarding a client offering sports betting services in a jurisdiction with moderately effective AML regulations, or engaging a software development outsourcing entity with complex ownership structures.

5.3 High-Risk Scenarios

Definition: These scenarios present a substantial AML risk. This typically includes clients or outsourcing entities operating in jurisdictions known for weak AML enforcement, unusually high transaction volumes, non-transparent ownership, or unclear sources of wealth.

Examples: Onboarding a client operating in a jurisdiction with a history of money laundering issues, or engaging an outsourcing entity providing payment processing services with inadequate AML controls.

5.4 Enhanced Due Diligence (EDD)

Definition: In situations where we identify high-risk factors, we conduct Enhanced Due Diligence. This involves more extensive background checks, thorough documentation reviews, and ongoing monitoring.

Examples: For a high-risk client, we might request additional documentation to verify the source of funds or conduct ongoing transaction monitoring for unusual patterns.

Our risk assessment approach allows us to categorize clients and outsourcing entities into these levels based on specific criteria. This classification helps us tailor our AML measures accordingly, allocating resources where they are needed

most to maintain compliance with EU AML regulations and uphold the integrity of our operations in the gambling industry.

5.6 Factors we look at on our risk assessment for clients/outsourcing entities

1. Jurisdiction and Geographic Location:

The jurisdiction in which the client or service provider operates or is based can significantly impact the level of AML risk. Some jurisdictions have strong AML regulations and enforcement, while others may have weaker controls.

2. Business Activities:

The nature of the client's or entity's business activities is crucial. Certain activities, such as online gambling, can inherently carry higher AML risks due to the potential for large financial transactions.

3. Transaction Volumes:

The volume of financial transactions conducted by the client or entity can be an indicator of AML risk. Unusually high transaction volumes may warrant additional scrutiny.

4. Ownership Structure:

The ownership structure of the client or entity is essential. Complex ownership structures or offshore accounts can raise concerns and increase the risk level.

5. Source of Wealth:

Understanding the source of a client's wealth or the source of funds for an entity is critical. Unexplained or questionable sources of wealth can indicate AML risk.

6. Reputation and Industry Standing:

The reputation of the client or entity within the industry is a factor. Clients or entities with a history of regulatory violations or negative publicity may pose higher AML risks. All clients' UBOs are screened against OFAC lists to ensure they have not been sanctioned in any jurisdiction globally.

7. Regulatory Compliance History:

The client's or entity's history of compliance with AML and other regulatory requirements is assessed. Previous violations or fines may increase the risk level.

8. Political Exposure:

Any political exposure or affiliations of the client or entity can be a risk factor. Politically exposed persons (PEPs) may require more scrutiny due to the potential for corruption. As part of our due diligence process, the company uses an online tool called PepChecker to screen all UBOs, ensuring that business is not conducted with politically exposed persons.

9. Relationships with High-Risk Jurisdictions:

If the client or entity has relationships with parties or jurisdictions known for weak AML controls, this can elevate the risk level.

10. Unusual or Suspicious Behavior:

Any unusual or suspicious behavior detected during the due diligence process, such as inconsistent financial transactions, may increase the risk assessment.

These factors collectively contribute to the risk assessment process. By carefully analyzing these elements, Interactive Global Entertainment B.V. can categorize clients and service providers into low, moderate, or high-risk levels, which then guides the appropriate level of due diligence and ongoing monitoring required for compliance with AML policies and regulatory requirements. The procedure will be executed on Monday system.

6. Risk Assessment Procedure

6.1 Procedure: Client/Service Provider Onboarding and Contract Approval

Step 1: Legal Department Due Diligence Request

When the Legal Department initiates a new client or service provider onboarding process, they begin by conducting due diligence. This involves gathering necessary information about the potential client or service provider, such as their identity, business activities, jurisdiction, and ownership structure. This due diligence is crucial for assessing the AML risk associated with the client or service provider.

Step 2: Contract Preparation

Simultaneously, while conducting due diligence, the Legal Department also prepares the contract that will govern the relationship between Interactive Global Entertainment B.V. and the client or service provider. This contract will include terms, conditions, and obligations that align with both legal and AML requirements.

Step 3: Evaluation Request to Compliance Department

Once the Legal Department has gathered the necessary due diligence information and prepared the contract, they send an evaluation request to the Compliance Department. This request includes all relevant details about the client or service provider that are necessary for the evaluation.

Step 4: Compliance Department Review

The Compliance Department plays a critical role in assessing the AML risk associated with the potential client or service provider. They carefully review the due diligence information, contract terms, and other relevant factors. Their evaluation aims to determine if the proposed client or service provider complies with AML policies and regulations.

Step 5: Compliance Approval or Rejection

If the Compliance Department approves the onboarding based on their evaluation and finds that the client or service provider aligns with AML policies, they provide their approval. Legal can then proceed to have the client or service provider sign the contract.

Step 6: Escalation to Business (If Compliance Rejects)

In the event that the Compliance Department rejects the onboarding due to significant AML concerns or non-compliance issues, the case is escalated to the Business Department. Business will receive the Compliance Department's recommendations and reasoning for rejection.

Step 7: Final Decision by Business (Based on Compliance's Recommendations)

Business reviews the Compliance Department's recommendations and conducts additional assessments if necessary. They make the final decision on whether to proceed with the onboarding or not. Their decision will take into account both legal and AML considerations.

This structured procedure ensures that all client or service provider onboarding processes are thoroughly evaluated for AML compliance. It establishes a clear path for assessing and mitigating AML risks while also adhering to legal requirements, ultimately helping Interactive Global Entertainment B.V. maintain the highest standards of AML compliance within the gambling industry.

7. Staff Education, Training and Development

7.1. Importance for AML/CTF risks

The Company is required to ensure that all of its staff are kept aware of the Company's AML/CFT policies and procedures and the relevant legislation and to provide training in relation thereto, as well as in relation to the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in ML/FT.

The awareness and training should be an ongoing exercise to ensure that all employees are constantly kept up to date with any developments or changes in the operations of the Company and any changes in the applicable laws. Training will take place at least once a year, although new members of staff must receive training as part of their on-boarding/enrolling program as managed by the HR function within 60 days of joining the Company.

7.2. Integrity

The integrity of the board of directors, senior management, staff and employees of the Company are the foundation of its AML/CTF measures. If staff lack integrity, there is a danger that they may become involved in or become willing accomplices to ML/FT activities.

Direct involvement in ML/FT operations is the possible extreme. It is more likely that staff without the right attitude will not:

- Maintain awareness and detect ML/FT;
- Report ML/FT if they become aware of it;
- Take training seriously; and/or

- Encourage reporting and foster a culture that supports ML/FT prevention.

Furthermore, independent and objective compliance testing is an essential step in evaluating whether appropriate internal controls are in place and being properly implemented across the Company.

An independent review shall be undertaken by the Company's internal auditor of the company.

7.3. Employees' recruitment

It is essential that the Company takes appropriate steps to ensure the integrity of the new Employees. Such steps should be risk-based, with the extent of the effort proportional to the role of the employee and the ML/FT threat inherent in the role they are being recruited for.

The following employee' screening procedures are implemented by the Company:

- Copies of relevant qualifications will be confirmed by requesting sight of certificates, copies of which will be retained on the employees' file;
- Curriculum Vitae (CV) will be obtained from all prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer;
- Obtaining a copy of the identification document and proof of residence document; and
- Conduct screening on prospective employees against sanctions lists, PEP lists and to verify whether they are subjects of any adverse news.

7.4. Compliance with Company policies and procedures

Failure to comply with the Company's policies and procedures may result in disciplinary action being taken against the employee/staff which may include summary dismissal.

7.5. Technological Developments

The Company recognises the risks associated with the misuse of technological developments for the purpose of ML/FT. As a consequence:

- The board of directors and senior management should retain a close eye on technological developments that are taking place, particularly in relation to phishing activity, identity fraud, ML/FT etc.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solution.