Corporate Policy on Prevention of money laundering and funding terrorism

Version	Approved by:	Date:
v.1	Board of Directors CODERE S.A	14/07/2011
v.2	Board of Directors CODERE GROUP TOPCO	17/03/2025

1. Introduction

According to the Shareholder's Agreement related to Codere Group Topco (Schedule 1, Part A, Conduct of Business), the Company and the Group Companies shall comply with all Laws applicable to it in respect of the conduct of its business and in particular:

- Comply with all Anti-Corruption Laws and Money Laundering Laws and maintain and enforce policies and procedures designed to prevent violations of Anti-Corruption Laws and Money Laundering Laws.
- Maintain complete and accurate books and records, including records of payments to any Government Official or Government Entity in accordance with Anti-Corruption Laws, Money Laundering Laws and generaCIly accepted accounting principles.
- Not permit any Government Official to serve in any capacity within any Group Company, including as a director, employee, officer or consultant.
- Adopt and implement proper and appropriate policies, procedures and measures designed to ensure that no Group Company nor any of its Agents from time to time is included on a Sanctions List, engaged in any dealings or transactions with any person on a Sanctions List or acts in a manner that is otherwise in violation of any Sanctions.

The Board of Directors of Codere Group Topco S.A. (the **"Company"**) has the power to design, assess and continuously revise the Governance System, and specifically the guidelines governing the conduct of the Company and of the companies belonging to the Codere Group (the "**Group**").

2. Overview

Codere Group Topco S.A, as the parent company of an international group ("**the Group**"), is fully aware of the key role that institutions like Codere play in the prevention of Money laundering and terrorist financing.

As a global group that operates in multiple social environments whose well-being it is committed to, anti-money laundering and counter-terrorist financing ("**AML**") is one of the essential pillars of Codere's corporate culture. Its practical expression is included in the Group's Code of Conduct and the Compliance Function System.

As a practical response to this commitment, Codere Group has put in place a management model for the anti-money laundering and counter-terrorist financing risk ("**AML model**"). A model already applied in the Group, aimed at preventing the use of the products and services for illicit purposes, and which is already applied within the Group.

The design, implementation and monitoring of the AML model falls under Compliance function, one of the foundations on which the Group strengthens its institutional commitment to engaging in all its operations and businesses in strict compliance with the legislation in force, in accordance with strict canons of ethical behavior and through a proactive risk management.

The General Anti-Money Laundering and Counter-Terrorist Financing Policy (the "**Policy**") formalizes the AML model. It has been drafted taking account of applicable regulations and the best practices of the gambling industry in this matter.

3. Purpose

The purpose of the AML General Policy is to establish the common criteria for action to be followed by the Codere Group to prevent, identify, measure and manage the money laundering and terrorist financing risk ("**AML**").

The intention is to establish a framework of compliance at Group level that every company must observe over the course of its activities, business and relationships, both nationally and abroad, to prevent money laundering and terrorism financing, as well as to comply with the various international financial sanctions and countermeasures programmes that may apply.

4. General principles of the Policy

Codere Group operates on the principles of:

- Integrity
- Prudent risk management
- Transparency
- Achievement of a profitable and sustainable long-term business.
- Compliance with applicable law at any given time

In addition, Codere Gropu General AML Policy establishes the following AML principles:

- Codere Group's pledge to incorporate measures to prevent the products and services from being used for illicit purposes.
- Promotion of a preventive and risk-based approach to ML risk management, including the development of the necessary culture within the Group.
- Codere Group's pledge to incorporate measures to prevent the products and services from being used for illicit purposes.
- Promotion of a preventive and risk-based approach to ML risk management, including the development of the necessary culture within the Group.

5. Scope of Application

This Policy is corporate in nature. As a result, the guidelines defined are applicable to all the companies of the Codere Group that engage in any of the activities included within its scope.

The governance bodies of Codere Group companies will make the decisions necessary to integrate the provisions of this Policy. They will apply the principle of proportionality to adapt the governance framework to the idiosyncrasy of their structure of governance bodies, committees, and departments, as well as their principles of action, methodologies, and processes to the content of this document.

This integration may entail, among other decisions, the approval of a single internal policy by the company. This approval will be necessary in those companies that need to adapt the content of these Principles to their own specific situation, whether in terms of the subject matter, the jurisdiction or the significance of the risk in the company. In this case, the compliance function in Codere in each country will seek to align these policies with the corporate policy in a way that is consistent throughout the Codere Group.

6. General Provisions, Applicable standards and regulations

These Principles shall be always governed by the pertinent legislation in force and any legislation amending or replacing it in the future

In the case of companies subject to foreign jurisdictions or supplementary industry regulations, the policies and procedures that these companies develop shall consider not only their own regulations, but the consolidated obligations contained in the law, if they do not contradict the specific requirements in the relevant jurisdiction or industry regulation.

Lastly, each Group company shall develop the necessary rules, guidelines or procedures to ensure the effective implementation, execution, and observance of these Principles.

The AML model assigns roles and responsibilities. The AML function is therefore not an exclusive task of the specialist technical units. Instead, the first line of defense is the first filter within the obliged entity and must hold a key role in managing this type of risk.
The AML function is integrated within the Compliance Function. Codere Group Companies in each countries have a person responsible for the AML function within the entity, and a technical AML unit if necessary.

7. AML Prevention Model

The Group applies an AML model based on the following provisions:

- Risk Assessment
- Due diligence
- Detection, control and examination of transactions
- Reporting of suspect transactions
- Control of lists of Sanctions and notification of detections
- Retention of documentation
- Training

7.1 Risk assessment

Codere's AML Model is based on the previous understanding of the ML risks to which the Group is exposed because of its activity, considering risk factors including those relating to customers, suppliers, countries or geographic areas, products, services, transactions or delivery channels.

For this reason, each obliged entity in each country carries out a risk assessment at least once a year, which constitutes the necessary basis for identifying areas for improvement in each entity's AML control framework and establishing, if necessary, additional mitigating measures to strengthen it.

To maintain a proper control and prevention framework with a risk-based approach, Group Companies must be categorised in accordance with their level of risk to guarantee the application of greater supervision of companies, segments, channels, jurisdictions or products with higher levels of risk.

7.2 Due Diligence

Codere Group implements due diligence measures with respect to clients, suppliers and any counterparties and retains the documentation on the AML obligations.

In general, Codere obliged entities apply due diligence measures:

- Before establishing a new business, relationship or executing one-off transactions
- which allow them to know and, when applicable, verify the source of funds and the purpose of the business relationship
- periodically, so that the available client information is updated

The due diligence measures shall not, in any case, entail a violation of rights in the jurisdictions where the Group company performs its activities.

The due diligence is a dynamic process and establishes a compliance framework at Group level which may vary in accordance with the levels of risk in certain segments or activities, depending on exposure to risk at any given time. The due diligence shall comply with international standards with a special focus on guaranteeing that proper knowledge of the customer and suppliers and their activities is always available.

The due diligence process shall always be applied with a risk-based approach and shall ensure that the measures applied are appropriate to the underlying risk of money laundering, the financing of terrorism or sanctions.

Segmentation by level of risk

Codere Group segment clients and suppliers according to the level of ML risk they present. The risk rating is kept up to date as a result of continuous monitoring of the business relationship, determining the type and completeness of the due diligence measures with respect to the client and supplier.

Clients and supplier who present a higher risk profile are subject to an enhanced due diligence process and to senior management approval (i.e. PEPs)

Los clientes y proveedores que presentan un perfil de riesgo más elevado están sujetos a un proceso de debida diligencia reforzada y a que se escale su aprobación (por ejemplo: PEP).

At a minimum, the Group companies shall use the following customer classification, based on the level of risk identified:

Persons who cannot be approved. Business relationships with natural or legal persons included in the national or international sanctions lists or those to whom it has not been possible to apply the due diligence measures, as well as any other case provided for by a legal regulation or by the internal policies, shall not be accepted.

Persons with a higher-than-average risk. acceptance of these persons is in any event subject to the application of enhanced due diligence measures and shall require senior approval.

Everyone else, and entities, shall be subject to normal or simplified diligence measures as specified in the applicable law or in internal rules or procedures.

Formal Identification

The standards and procedures that implement these Principles must guarantee that Group's companies properly identify all customers and supliers in accordance with the applicable law and jurisdiction, which shall include, in any case, the verification of their identity through valid documents.

Under no circumstances shall business relationships be continued with persons who have not been identified, and products or services may not be contracted anonymously, through encryption or in a fictitious format.

Prior to the establishment of business relationships or transactions, the real party

involved must be identified. This obligation implies that, in the event of indications or certainty that customers or suppliers are not acting on their own behalf, precise information must be compiled to ascertain the identity of the parties on behalf of which they are acting. There must also be sufficient documentation to accredit authorisation for their actions.

Knowledge of the activity and assets

Before a business relationship is established by a Group company, it shall gather, at a minimum, information on the professional or business activity of the customer and suppliers the source of their funds or assets.

In regulatory frameworks, it is often necessary to balance the need for oversight with the realities of diverse operational scales and risk levels. One way to achieve this balance is through exemptions for certain clients or providers from stringent requirements. Exemptions are not granted arbitrarily; they are based on specific criteria that must be met by the client or provider. By applying criteria such as the nature and scale of operations, compliance history, and risk assessment.

And depending on the level of risk assigned to customers and suppliers, further measures may be applied, consisting of verification by means of documents and reliable external sources of the information, especially in connection with their professional or business activity, the origin of the funds or assets and any other relevant information in accordance with internal procedures and regulations.

7.3 Detection, control and examination of transactions

Group companies must have the resources for detecting, controlling and examining transactions. These resources shall be applied based on risk, and in any case shall entail the three basic scenarios of detection of transactions:

- Internal reporting of indications by Group employees
- Detection of potential suspect transactions through the alert systems established.
- (systems at each Group company and/or centralised systems).
- Notifications by supervisory bodies or police or court authorities.

The detection of suspect transactions entails a detailed and comprehensive analysis aimed at determining the effective existence of signs of money laundering and the financing of terrorism. The methodology for performing this analysis must be set out in a specific procedure known as the Special examination procedure. This analysis shall in any case be centralised at a unit common to all Group companies operating in the same jurisdiction.

The monitoring system shall conduct a review of activities on the basis of the standards identified at any given time by the law and best practices.

7.4 Monitoring of operations and reporting of suspicious transactions

Codere Group has procedures and tools in place for continuous monitoring of the clients and suppliers' business relationships and one-off transactions, to detect possible signs of money laundering or terrorist financing, and to notify the local Financial Intelligence Unit of the transactions presenting reasonable signs or suspicion of being related to money laundering or terrorist financing.

Specifically, supervisory bodies shall be notified of any transactions showing any ostensible inconsistencies in relation to the nature or volume of activity of past operations of customers.

The decision to report shall be taken in a centralised fashion in each jurisdiction by the persons or bodies designated on the Compliance Function to this end, and the report shall be made by the official representative with the competent authorities. The report shall in any case contain information on the decision taken with respect to continuation of the business relationship, and the grounds for this decision.

Notwithstanding the report through indications, the company shall immediately take further measures to manage and mitigate risk, and this must take account of the risk of disclosure.

Group employees must refrain from carrying out any transactions with respect to which there are indications or certainty of links to money laundering or the financing of terrorism.

Group employees, management or agents shall not disclose to the customer or to third parties that information has been reported to internal control bodies or to the supervisory body, or that transactions are being examined or may be examined to ascertain if they involve money laundering or the financing of terrorism.

7.5 Control of lists of Sanctions and notification of detections

To ensure compliance with the restrictions imposed by programmes of Sanctions, Group companies must:

- Identify and follow the Sanctions programmes established by the United Nations (UN), the European Union (EU), OFAC and any applicable local programmes in the jurisdictions in which the Group companies operate.
- Assess the risks associated with the activities related to the Sanctions Programmes to determine the risks of taking part or being involved in activities that are restricted or forbidden by Sanctions.
- Abstain from agreeing to or participating in operations or transactions with sanctioned individuals.
- Enforce prohibitions and restrictions when executing transactions, payments or business relationships, and abstain from executing them when they entail violating a Sanctions programme.
- Implement internal control procedures and prevention mechanisms for proper compliance with the obligations of Group companies.

7.6 Retention of documentation

Codere Group companies shall establish documentation conservation measures which meet the legal requirements applicable in each jurisdiction.

7.7 Training

Creating awareness of the risks associated with these crimes is a key feature of the fight against money laundering and the financing of terrorism.

Codere Group companies must define, maintain and apply employee training programmes to ensure a proper level of awareness among all staff members, as required by law, and must establish measures to guarantee mandatory training in anti-money laundering, counter terrorist financing and Sanctions for all staff members (including senior management and governance bodies) on a regular basis in accordance with the level of risk their activities carry within the company.

The ML/TF and Sanctions training programmes of every company in the Codere Group shall be validated by the Compliance unit at Codere Group once said programmes have

been validated by the company's training and compliance departments. A record shall be kept of the training given, its content, and the employees who received and successfully completed the training.

7.8 Independent reviews

To verify compliance with anti-money laundering and counter-terrorist financing obligations and to assess the effectiveness of the internal control measures implemented to mitigate this risk, the AML programs of obliged entities are periodically subject to independent reviews by the Internal Audit area or external auditors. Similarly, the mitigation and control environments for this risk are subject to verification by the Compliance Testing function.

7.9 Consolidated risk management

Codere Group believes that the best way to combat the risks associated with the Prevention of Money Launderingand Terrorist Financing is to manage said risks in a uniform manner, and to manage all the information related to the handling of these risks at a Group level, regardless of the jurisdiction in which the Group companies operate.

The principle of aggregate or consolidated management is thus one of the mainstays of the prevention model, and coordinates the efforts of all Group companies uniformly, and assesses and manages risk in an aggregate fashion.

Thus, all companies making up the Group shall keep Compliance Unit regularly informed of high-risk relationships, data on sensitive activities and their associated risks, responding rapidly to any information requests that may be issued by Codere Group in its management of regulatory and reputational risk in connection with money laundering, the financing of terrorism and Sanctions.

In any case, these obligations are understood without prejudice to strict compliance with the regulations applicable, most particularly regulations concerning data protection and privacy. Codere Group companies shall take the necessary steps to protect and uphold the confidentiality and privacy of all data thus reported between Group companies.

8. Implementation of the Policy

The Compliance Fuction in each country proactively endeavours to ensure the application and effectiveness of this Policy and disseminates the content hereof among the people to whom it is addressed, all without prejudice to the responsibilities assigned to other bodies and divisions of the Company and, if appropriate, the administrative and management bodies of the country subholding companies and head of business companies and the respective compliance units of these companies.

9. Monitoring, Follow-up & Supervision

The Compliance Unit shall be responsible for the continuous monitoring and followup of the provisions of this Policy.

It will also be responsible for promoting actions for its appropriate dissemination and knowledge.

The Internal Audit department shall review the adequacy and effectiveness of the measures applied, issuing the corresponding report to be submitted to the Audit Committee.

10. Approval, effective date and updating

This Policy shall enter into force on the date of its approval by the Board of Directors of the Company.

This Policy shall be kept up to date over time. To this end, it must be reviewed on a regular annual basis, and on an extraordinary basis, and in any case as soon as possible, when there are variations in the strategic objectives or an external or internal regulatory change that implies its updating or modification.

The Company`s Compliance Unit is responsible for assessing any proposal for modification.

11. Revision of the Policy

The Compliance Committee shall regularly review the contents of the Policy, ensuring that it reflects the recommendations and best international practices from time to time in effect, and shall propose to the Company's Board of Directors those amendments that contribute to the development and ongoing improvement thereof, taking into account any suggestions or proposals made by the Compliance Unit.

This Policy was approved by the Board of Directors on March 17, 2025.