ANTI-MONEY LAUNDERING AND COUNTERING TERRORIST FINANCING GROUP POLICY

Approved by the Board of Directors

Summary

REVISION	REASON / REVISION CHANGES	DATE
Rev. 1	First issue	13th May 2022
Rev. 2	In order to provide more details regarding the checks and controls carried out for AML&CTF purposes.	14th Oct 2025

Main Internal Regulatory References
• Prevention and Risk Management of the use of the Financial System for the purpose of Money Laundering Proceeds from Criminal Activities and to Finance Terrorism, PA REG 05, PA REG 06, PA REG 10, PA REG 19; • Self-assessment of the risk of money laundering and terrorist financing, PA REG 13; • Operating Instruction IO REG 01 Business partner monitoring: reputation requirements and compliance procedures AML; • No Business Third Parties Due Diligence, PA REG 12; • Supplier qualification, PA PSS 02; • "Handling reports" Procedure (Whistleblowing).

1 Glossary and definition

Acronym/Term	Definition
AML Function	The AML Function is the organizational unit responsible for preventing and managing money laundering and terrorist financing risks, through policies, monitoring, reporting, and advisory activities, ensuring compliance with applicable regulations.
BoD	Board of Directors, which have the broadest management powers for the pursuit of the corporate purpose and being supported by Board Committees with advisory, proposing and investigating responsibilities.
Business Relationship	Business Relationship means a business, professional or commercial relationship which is connected with the professional activities of an AML obliged entity and which is expected, at the time when the contact is established, to have an element of duration.
Concessionaire	Entity authorized with at least one gambling license.
Corporate (Customer)	Non-natural persons (legal entities and legal arrangements) generally with separate and distinct identity from their owners and controllers, but not exclusively.

Acronym/Term	Definition
Customer	Any legal or natural person (including government, corporation, trust, fund, private person etc.) with whom the Group enters into a business relationship to undertake business activities, where the Group provides services and products to the other person, also on a continuous basis. Refer to local Compliance if there is any doubt or question regarding the applicability of the requirements.
Customer Due Diligence	Customer due diligence includes the identification and verification of the Customer's and the other relevant parties' identity, the assessment of the purpose and intended nature of the Business Relationship and the ongoing monitoring of the Business Relationship.
Customs and Monopoly Agency	Agenzia delle Dogane e dei Monopoli (ADM, the Italian Customs & Monopoly Agency).
Enhanced Due Diligence	Any specific due diligence required by these requirements to effectively manage Customers that present higher risk level.
Financial Intelligence Unit (FIU)	A central governmental office that obtains information from financial reports, processes it and then discloses it to an appropriate government authority in support of a national anti- money laundering effort. The activities performed by an FIU include receiving, analyzing and disseminating information and, sometimes, investigating violations and prosecuting individuals indicated in the disclosures.
Group AML & CTF Standards (or Group Standards)	The Group AML & CTF Standards set out in this Group Policy are the minimum measures to be adopted by Group Legal Entities to ensure the consistent implementation of Group-wide anti-money laundering and countering the financing of terrorism policies and procedures and the robust and effective management of money laundering and terrorist financing risk within the Group.
Group	Lottomatica Group, composed by the Group Entities.
Group Entity	Any company belonging to the Group and falling within the scope of application of this policy.
High-Risk Third Countries	Third-Country jurisdictions (i.e., non-EU jurisdictions) which have strategic deficiencies in their national AML & CTF regimes that pose significant threats to the financial system of the Union as identified by EU Commission in order to protect the proper functioning of the internal market.
INA	Internal Audit.
Know Your Customer (KYC)	The due diligence that Group Entities must perform to identify its Customers and Third parties and, where applicable, to ascertain relevant information pertinent to doing financial business with them.

Acronym/Term	Definition
KYC and Transaction Monitoring tools	Tool which allow to obtain and verify the information for the Customers and Third parties identification and transactions.
ML/TF	Money Laundering / Terrorism Financing.
Money Laundering	Activity aimed at disguising the illicit origin of criminal proceeds and at creating the appearance that their origin is legitimate, including where the activities which generated the property to be laundered were carried out abroad.
On-line Gambling	Online gambling (or Internet gambling) is any kind of gambling conducted on the internet.
Politically Exposed Person (PEP)	Any person who holds (or has held) a prominent/important public position or a closely associated person or immediate family member of a person in such a position.
Personal Data	Any information directly or indirectly relating to an identified or identifiable natural person.
Physical Betting	Physical betting is any kind of bets collected at physical point of sales.
REG	Regulatory Compliance, AML & Quality Function.
Reputational Risk	The potential losses arising from a deterioration or a negative perception of the Group Entity's or Group's reputation in respect of its Customers, Counterparties, Shareholders and Supervisory Authority.
Risk Based Approach	The approach whereby obliged entities identify, assess and understand the ML/TF risks to which subjects of assessment are exposed and take AML & CTF mitigation measures that are proportionate to those risks.
Screening Tool	Tool activated for, preferably automated, screening of Customers and business partners against updated databases (e.g., OFAC; UN; EU; PEP; Adverse Media)
Suspicious Activity	Unusual Customer behavior or activity that raises a suspicious that it may be related to money laundering or to the financing of a terrorist activity: may also refer to a transaction that is inconsistent with a Customer's known economic capacity, personal activities, or the normal level of activity for that kind of account.
Terrorism financing	The provision or collection of funds carried out by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out acts of terrorism. The funds used in terrorist financing may be obtained from legal as well as illegal activities.
Third Country	A Country other than an EU Member State.
Third Party acting on behalf of the Group	Third party acting on behalf of the Group could include concessionaries, consultants, advisors, service providers, suppliers and includes outsources who manage any AML & CTF activities.
Transaction	A Transaction is any transmission or movement of funds regardless the connection with an ongoing relationship, as well as the designation of one or more beneficiaries specifically identified or unambiguously identifiable.
VLT	A VLT is a video lottery terminal, a type of electronic gambling machine.

2 Introduction

2.1 Objectives and Purpose

Lottomatica Group, as a leading group operating in the regulated gaming market, recognizes the strategic importance of maintaining a robust and harmonized Anti-Money Laundering and Counter-Terrorist Financing (AML & CTF) control framework.

Lottomatica Group has adopted a governance and compliance model that reflects the highest international standards, ensuring scalability and applicability to different markets.

The Group parent company, Lottomatica Group S.p.A., is listed on the regulated Euronext Milan stock exchange and therefore it is subject to the supervision of the Italian Securities and Exchange Commission (CONSOB). It undergoes statutory audits performed by some of the major global audit firms; within the scope of these audit procedures, specific quarterly assessments are conducted on AML & CTF-related controls by the Anti Financial Crime Department of the audit firm aimed at evaluating the level of reliability of the anti-money laundering and counter-terrorist financing control system.

This integrated and rigorous approach ensures that Lottomatica maintains full compliance with the applicable laws, while also aligning with international standards and guidelines (FATF Recommendations, EU AML Directives, EBA Guidelines).

The purpose of this Policy is to establish a clear, operationally effective AML & CTF architecture, aligned with international best practices and compliant with both supranational and national regulations. It aims to:

- define a comprehensive risk-based approach applicable across all Group Entities;
- assign clear roles and responsibilities for the implementation, oversight and enforcement of AML & CTF controls;
- set out the minimum standards and methodological principles for customer due diligence (CDD), enhanced due diligence (EDD), transaction monitoring, screening and suspicious activity reporting;
- provide employees, contractors, business partners and relevant third parties with practical guidance to recognize and manage AML & CTF risks in their daily operations;
- promote a corporate culture of compliance, professional ethics and accountability in line with the Group's sustainability strategy and stakeholder expectations.

The scope of this Policy includes the full spectrum of the Group's gaming operations, encompassing amusement and entertainment machines, betting services across physical retail networks and remote gambling platforms (including online and mobile channels). It also applies to cross-border activities and new business lines that may emerge through innovation or acquisition.

In addition, there are other local policies and procedures concerning Customer due diligence obligations and transaction management which must be followed to help the management of the legal, regulatory, reputational, financial and other risks, under the responsibility of each Group Entity for the correspondent Country of residence/operativeness.

The Policy is subject to regular review and continuous improvement, ensuring its alignment with

evolving regulatory landscapes, technological developments and emerging financial crime typologies.

2.2 Policy Approval, Oversight and Review

This Group AML & CTF Policy is formally approved by the Board of Directors of Lottomatica Group S.p.A. and is subject to a comprehensive review at least once per year or more frequently where material changes in regulation, risk exposure or operational scope occur.

The Group Regulatory Compliance, AML & Quality Director is delegated to provide the Group with common Group AML & CTF Standards and detailed guidance to support an effective implementation of this Policy informing the Board of Directors on the initiatives taken.

Responsibility for maintaining, updating, and disseminating this Policy lies with the Group Regulatory Compliance, AML & Quality Director who is delegated by the Board of Directors to act as the central reference person in charge of defining Group-wide AML & CTF standards and operational guidelines. The Director ensures that all relevant internal stakeholders are aligned with applicable laws, regulatory expectations and industry best practices, while providing timely reporting and strategic updates to the Board of Directors and senior management.

The review process includes:

- Evaluation of the policy's effectiveness in managing financial crime risks;
- Assessment of alignment with supranational and national AML & CTF developments;
- Collection of feedback from Supervisory Bodies and the Group Internal Audit function;
- Incorporation of lessons learned from incidents, inspections or regulatory feedback.

Policy updates are communicated promptly through appropriate governance channels and kept available to all staff.

2.3 Scope of Application and Enforcement

This Policy sets out minimum AML & CTF standards that apply across all business units and Entities of the Group, ensuring a consistent and risk-sensitive framework for the identification, mitigation and management of financial crime threats.

The provisions of this Policy are binding upon:

- all the Group Entities and related executive bodies and employees;
- their gambling service providers including business partners and retailers on a physical network and on-line gambling operators that offer games with cash prizes.

The Group adopts a zero-tolerance approach toward non-compliance with AML & CTF laws, internal policies and ethical standards. Any deliberate or negligent violation may result in disciplinary measures, up to and including termination of contract or legal action, in accordance with internal codes and applicable legislation.

2.4 Local Requirements

If local laws, regulations, policies or standards are stricter than the Group AML & CTF Standards set out in this Group Policy, the stricter standard prevails.

Where a Third Country law does not allow the implementation of this Group Policy or any conflict is identified with the principles and requirements in this Policy, Regulatory Compliance, AML & Quality Director must be immediately informed, which in turn has to perform an evaluation of the conflict of law and identify risk mitigation factors.

2.5 Group and Local AML & CTF Procedures

This Policy is intended to outline the minimum necessary requirements to be met by all Group Entities and a high-level description of the roles, responsibilities and AML requirements at Group level.

This Policy is therefore complementary to any procedures issued locally and designed to manage AML & CTF risk within the Group, to which reference should be made for the specific activities to be carried out in order to prevent the risk of money laundering and countering the financing of terrorism.

3 AML & CTF essentials

3.1 The Criminal Offense of Money Laundering

To ensure effective implementation of this Policy, it is essential that all employees and relevant third parties acting on behalf of the Group fully understand key AML concepts.

Money laundering is defined as the process through which individuals or entities seek to conceal the illicit origin of proceeds derived from criminal activity and reintroduce them into the legitimate financial system.

Under international and national laws, money laundering may include not only the handling of illicit funds, but also the mere possession, transfer or transformation of assets known to originate from unlawful sources.

This process typically unfolds in three distinct stages:

- **Placement:** the initial introduction of illicit cash or value into the financial system, often through deposits, wagers or purchases of gambling services;
- **Layering:** the creation of complex transaction chain, often involving cross-border transfers, currency conversions or asset purchases, to obscure the origin of the funds and hinder traceability;
- **Integration:** the reintroduction of laundered funds into the legitimate economy, typically through acquisition of legal assets, investments or further business activity, making detection difficult.

In the context of the gambling industry, this may include:

- use of gambling platforms to introduce cash of illegal origin;
- placement of criminal proceeds through betting or casino activity with minimal risk of loss;

- withdrawal of “cleaned” funds via winnings or refunds;
- use of third-party identities to obscure true ownership.

Lottomatica considers all three classical phases of laundering — placement, layering and integration — in its risk analysis and designs controls accordingly.

3.2 Financing of Terrorism

Terrorism financing involves providing or collecting funds, by any means, with the intention or knowledge that they will be used to support terrorist acts or organizations. Unlike money laundering, the origin of such funds may be lawful; the criminality lies in their destination. This characteristic requires different risk indicators and detection strategies.

Examples in gambling may include:

- use of accounts with abnormal betting activity for micro-transfers;
- linking multiple small-value transactions to avoid suspicion;
- use of anonymous or prepaid tools to finance illicit causes.

3.3 Legal Relevance of Knowledge and Suspicion in AML & CTF

The concepts of suspicion and knowledge play a pivotal role in the architecture of anti-money laundering systems, as they represent the legal thresholds for both preventive duties and potential criminal liability.

These elements underpin the responsibility of obliged entities to detect and report activities that may be connected to money laundering or terrorist financing, even in the absence of direct proof.

In practice, the law imposes two key obligations:

1. to report *knowledge* or reasonable *suspicion* of money laundering/terrorist activities;
2. to ensure that personnel and systems do not ignore or overlook red flags, which could imply constructive or imputed knowledge.

In the context of anti-money laundering obligations, *knowledge* refers to the demonstrable awareness that certain funds or assets originate – directly or indirectly – from criminal activity.

For example, an employee who is aware that a customer is depositing funds that derive from the sale of illegal drugs or obtained through fraud, deception or corruption, is considered to possess knowledge of the criminal origin of those funds.

Such knowledge creates an immediate legal obligation to act in accordance with internal procedures, including escalation to the AML function which is in charge to make proper analysis and investigations for Suspicious Activity Report (SAR) purposes.

For Lottomatica, this means:

- ensuring that monitoring systems are robust enough to detect risk indicators;
- training staff to avoid underestimating atypical behavior;
- establishing escalation protocols that ensure no information is ignored or overlooked.

On the other hand, a *suspicion* exists when a person, based on experience, professional

judgment and available data, has a reasoned concern that a customer, transaction or behavior may be linked to criminal activity.

Suspicion is not equivalent to certainty or proof; it is a subjective, preventive alert level, meant to trigger internal analysis or escalation.

In gambling environments, suspicion may be triggered by:

- disproportionate bets or winnings compared to income profile;
- rapid deposits and withdrawals without real gaming intent;
- use of multiple identities or accounts under the same IP or device;
- transactions structured to avoid mandatory checks (e.g., splitting cash-ins).

Personnel are trained to recognize such anomalies and escalate them through the Group's reporting mechanisms, in line with internal procedures.

3.4 Integration into Group Controls

These concepts are embedded into Lottomatica's AML & CTF Programmes as follows:

- suspicion is the threshold for triggering internal reviews, alerts and Suspicious Activity Reports (SARs);
- knowledge is addressed through robust training, procedural transparency, audit trails, and accountability checks, ensuring that no employee or system can "unknowingly" ignore red flags.

This approach reflects both the regulatory framework and the Group's commitment to act with the highest degree of diligence and ethical responsibility in identifying and disrupting potential ML & TF activity.

4 Governance Structure and Allocation of Responsibilities

Lottomatica Group adopts a multilevel governance model to ensure the effective implementation, oversight and accountability of its Anti-Money Laundering and Counter Terrorist Financing (AML & CTF) Framework.

This model reflects a clear separation of roles, independence of control functions, and direct reporting to the highest corporate bodies.

4.1 Board of Directors of Lottomatica Group S.p.A.

The Board of Directors holds ultimate responsibility for the approval, supervision and strategic direction of the Group's AML & CTF Policy. Its duties include:

- approving the Group AML & CTF Policy and any significant amendments;
- reviewing reports on AML & CTF risks, incidents and trends;
- ensuring that adequate resources, systems and governance structures are in place;
- promoting a Group-wide culture of integrity and regulatory compliance.

Any shortcomings and findings emerged as a result of the controls carried out at various levels must be brought promptly to the BoD's attention.

4.2 Boards of Statutory Auditors

The Boards of Statutory Auditors monitors compliance with the law and the completeness and adequacy of anti-money laundering controls. In exercising its powers, the Board uses internal departments to carry out the necessary checks and assessments and uses information flows from the other company bodies, from the Group Regulatory Compliance, AML & Quality Director and from the other internal control departments to ensure that an effective internal control system for the mitigation of the ML & TF risks is maintained over the time.

It assesses the suitability and the effective implementation of the procedures for risk mitigation, Customer due diligence, information retention and reporting of suspicious transactions.

The members of the Board of Statutory Auditors, in addition to supervising compliance with the relevant regulations, are required to communicate to the legal representative or his / her delegate the operations considered suspicious of which they become aware in the exercise of their duties. Furthermore, the Board must transmit the facts that can integrate serious, repeated, multiple or systematic violations of the provisions regarding anti-money laundering always learnt in the exercise of their duties to the sector Supervisory Authority, the Administrations and Bodies concerned.

4.3 Supervisory Board

The Supervisory Board (OdV) is an independent body established pursuant to Legislative Decree 231/2001 which provides for the administrative liability of companies in cases of violations that may be committed by senior or subordinate subjects in the interest or to the advantage of the company.

The OdV has the primary responsibility of overseeing the effective implementation, adequacy, and updating of the Organizational Model adopted by the Lottomatica Group, intended as an instrument to mitigate risks - including money laundering and terrorist financing - from which administrative liability may arise for the company.

The mission of the Supervisory Body includes:

- monitoring the Model's implementation and verifying compliance with its provisions;
- reporting the need for updates to ensure the Model remains current and effective;
- overseeing training and awareness efforts across the organization regarding the Model;
- to fulfill its duties, the O.d.V. conducts planned activities such as:
    a. periodically reviewing business operations to identify areas at risk of offenses under the Decree and recommending updates or integrations as needed;
    b. assessing the Model's ongoing validity and, in coordination with relevant departments, promoting any actions required to maintain its effectiveness;
    c. proposing adjustments to the Model in response to changes in the company's organizational structure, operations, or applicable legislation;

d. verifying that high-risk activities are carried out correctly and in compliance with the Model, also by coordinating with the departments involved;

e. reviewing delegated powers of signature and authorization to ensure they are consistent with defined responsibilities and suggesting modifications if necessary;

f. examining actions taken by those with signing authority and the related reporting to the delegating body to confirm alignment with assigned duties;

g. suggesting to the BoD the implementation, integration, or amendment of operational and control procedures to ensure proper execution of business activities.

The Supervisory Board works closely with the Compliance functions, Internal Audit and the Group's AML Department, promoting a corporate culture grounded in compliance, integrity, and transparency.

4.4 Group Regulatory Compliance, AML & Quality Director

The Group Regulatory Compliance, AML & Quality Function is established in the form of an independent organizational unit and it is headed by the Group Regulatory Compliance, AML & Quality Director that ensures the guidance and coordination of the shared resources within the Group for Anti-Money Laundering and Counter-Terrorism Financing purposes, also through the issuance of group-wide AML & CTF Standards, Guidelines and procedures.

The Group Regulatory Compliance, AML & Quality Function verifies on an ongoing basis that the group-wide AML & CTF Standards and procedures are coherent to effectively prevent and contrast the violation of laws and regulations related to the prevention of money laundering and terrorism financing.

The Group Regulatory Compliance, AML & Quality Director is independent and he is responsible for:

- Identifying the applicable AML & CTF laws and regulations for the Group and ensuring compliance with AML & CTF requirements;
- Guaranteeing the update of the procedures for the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; • coordinating the AML & CTF risk assessment for the Group Entities in scope in order to assess the money laundering and terrorist financing risk to the entire Group;
- Accessing to data and information available locally;
- Monitoring the adequacy of the overall AML & CTF program, also through the performance of sample controls in coordination with Group Audit and the evaluation of any procedural changes in order to optimize the anti-money laundering management;
- Defining, in coordination with other Group Functions, the AML & CTF training for the Group, providing targeted training to relevant staff members to enable them to identify money laundering and terrorist financing risk indicators;
- Defining Group AML & CTF Standards, in particular for the application of the risk-based approach, the management of the Customer due diligence, suspicious transactions reporting and testing controls in accordance with the provisions of this Policy;

- Promptly inform and report to the BoD and the control bodies of any facts of which he becomes aware in the context of the duties relating to anti-money laundering and the related activities carried out in the reference period.

In addition, the Group Regulatory Compliance, AML & Quality Director is in charge of appointing the members of the Anti-Money Laundering Committee.

The Group Regulatory Compliance, AML & Quality Function is promptly informed by each business units in relation to any relevant fact related to Money Laundering/Terrorism Financing ("ML & TF") matters and must have direct access to any information and systems may be needed in order to prevent and/or manage ML & TF risks in the Group.

It has access to all Suspicious Activity Reports sent to the FIUs and provides guidelines in order to ensure coordination and alignment of the reporting process within the Group.

4.5 AML Committee

The Anti-Money Laundering Committee, hereinafter "AML Committee", is convened regularly with the aim to support the Suspicious Transaction Reporting Delegate ("STRD" in hereinafter) to analyze the positions selected following to the application of AML&CTF procedures for which the STRD considered it appropriate that certain positions be subjected to specific technical assessments.

The frequency of the meetings is such as to ensure timely fulfilment of the reporting obligations. Where a shorter term is not provided for by local regulations, the frequency of the Committee's meetings is set on at least a monthly basis, except for particularly urgent situations that require more frequent meetings.

4.6 Suspicious Transaction Reporting Delegate

The Suspicious Transaction Reporting Delegate assumes the role of the STR contact person and is responsible for ensuring that:

- coordinate the analysis of the positions selected through the application of the AML&CTF procedures;
- "Submit to the Anti-Money Laundering Committee the positions he deems appropriate for specific technical assessments, and ensure the drafting and record-keeping of the Committee's meeting minutes;
- Suspicious transactions are reported to the FIU. In this context, the STR Delegate can make use of employees specifically appointed;
- The STR feedback carried out by the FIU is acknowledged.

4.7 Other Group Entities' Functions involved

Other corporate functions are involved in various capacities, as part of their operating activities, in maintaining the anti-money laundering measures according to the activities specified within the AML & CTF procedures.

The Internal Audit Department independently performs the verification of the relevant AML/CTF policies, controls and procedures.

4.8 Employees and Third Parties acting on behalf of the Group (Whistleblowing)

It is the responsibility of all employees, third parties acting on behalf of the Group, outsourcing service providers and business partners, in the performance of their duties, to perform the necessary measures to prevent and mitigate the ML & TF risks and to exercise professional due diligence and good faith in pursuit of the rigorous application of the Group AML & CTF Policy and of any relevant local requirements and internal rules and procedures.

It is particularly important that all "front office" personnel or gambling service providers make themselves aware of all restrictions applicable to their business and remain vigilant to the related risks applying to their client relationships and transactions and report any anomalous activity.

Protection against money laundering and the financing of terrorism can only be as good as the weakest control performed within the Group and failure to enforce AML practices in one entity might expose the whole Group to exploitation by criminals and resulting in regulatory/reputational risk.

Employees should always be alert to potential situations of money laundering and terrorist financing and manage those situations in accordance with this Policy, the Procedure set by the Group Entity they belong to and any relevant local rules.

Where an employee becomes aware of corrupt behaviour, money laundering or other potential abuse of internal procedures or code of conduct, he/she should immediately report that suspicion through the appropriate channel *(Whistleblowing).* Failure to comply with any breach of this Policy may give rise to disciplinary action against the relevant employee, in addition to the sanctions contained in the local laws and regulations. In serious cases, such action may include termination of employment.

Lottomatica Group, in fostering a corporate culture based on ethical behaviour and good corporate governance, provides employee with adequate communication channels to report unacceptable conduct within the Group and verifies and monitors the reputation requirements, the financial/equity soundness and the quality standards of the Third parties who act on behalf of the Group.

In addition, the procedures and control systems ensure the verification of possession and control over the permanence, during the relationship, of the legal and reputation requirements of the business partners.

4.9 Internal Audit and Independent Review

The Internal Audit function plays a critical role in assessing the effectiveness, adequacy, and integrity of the AML & CTF Framework within Lottomatica Group. As part of the Group's three lines of defense model, Internal Audit provides independent assurance to the Board of Directors and Senior Management.

Key responsibilities include:

- periodic AML audit plans: the Internal Audit function develops an annual risk-based audit plan, approved by the Audit Committee, which may include AML processes and systems

across the Group entities;

- operational effectiveness testing: reviews include sample testing of CDD/EDD files, transaction monitoring outcomes, escalation logs, and SAR processes;
- control design and implementation review: evaluating whether AML policies, internal procedures and automated systems are appropriately designed, implemented and followed by first and second-line functions;
- regulatory compliance checks: ensuring that the Group's AML & CTF controls remain compliant with the latest applicable laws, regulations and guidance at supranational and national levels;
- reporting: findings and recommendations are reported to the relevant local management, the Group Regulatory Compliance, AML & Quality Director and the Board-level committees.

The Internal Audit function operates with unrestricted access to AML-related data and personnel and is granted full independence to carry out its duties effectively.

5 AML Group requirements

5.1 Risk-Based Approach (RBA) to AML & CTF Compliance

All employees must always be aware, both in setting up the organization and in the daily operations, of the ML/TF risks to which they are exposed based on their roles and risk-based approach framework.

Group Entities should ensure that, supported by the AML & CTF Risk Assessment results, they have the appropriate resources, policies, procedures and controls to mitigate the risks identified. To this end, the AML & CTF Risk Assessment process provides an inherent risk evaluation for each Entity and the evaluation of the mitigation measures implemented.

Adequate procedures aimed at identifying objective and consistent safeguards that allow the analysis and assessment of risks are adopted, also taking into consideration information elements relating to the characteristics of the Customers, the geographical area of operation, the channels and therefore also the Third parties with whom business relations are maintained.

5.2 Customer Risk Classification

Lottomatica Group employs a comprehensive and risk-sensitive approach to customer classification, grounded in the principles of the Risk-Based Approach (RBA) and in full alignment with local, EU, and FATF standards. The purpose is to assess and continuously update the ML & TF risk associated with each business relationship, be it with individual (B2C) customers or corporate (B2B) partners.

Customers are classified into risk tiers: high, medium, low or irrelevant based on a weighted evaluation of multiple factors:

- duration of relationship with customer;
- geographic risk based on country of origin or operation;
- product/channel risk (e.g., non-face-to-face interactions, e-wallets, anonymity features);

- behavioral indicators such as transaction frequency and value;
- presence of adverse media, criminal allegations or investigations;
- exposure to international sanctions or association with politically sensitive roles (PEPs).

The risk rating determines the level of due diligence required and the frequency of monitoring and review. Risk profiles are updated regularly, especially upon identification of triggers such as unusual transactions, media alerts, or changes in ownership or business activity.

5.3 Customer Due Diligence (CDD)

The Group Entity must conduct sufficient due diligence to identify Customers and, according to the risk-based approach principle, to understand the nature of the Customer's business and its expected activity. The Customer risk assessment and classification are essential parts of the risk-based approach to AML, allowing controls (such as due diligence measures and transaction monitoring) and valuable resources to be targeted at.

Generally, the AML Customer due diligence should include:

- Country risk;
- Industry risk;
- PEP and Sanctions risk;
- Reputational risk (e.g., negative and/or adverse media).

The CDD process must be performed:

- When there is suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- When there are doubts about the veracity or adequacy of previously obtained Customer identification data;
- When carrying out transactions whose value exceeds the amount of the maximum threshold provided by local regulations.

In addition, the ongoing monitoring of the business relationship including scrutiny of transactions must be undertaken throughout the course of the relationship.

CDD measures are implemented in accordance with the AML & CTF Group Standards, local and Group procedures to establish a proper business relationship.

Once the CDD process is concluded, the information is kept in order to monitor the activities and the transactions.

5.2.1 Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) measures shall apply to all Customers identified as Politically Exposed Persons ("PEP") and relationships that present higher ML & TF risks following a risk-based approach. Customers may represent an increased risk when they are the subject of negative information that may affect the Group's reputation. While it is not possible to formalize all types of negative information that may represent a reputation risk, allegations or convictions for financial crimes are of particular relevance.

However, the following circumstances must always be considered high risk:

- customers identified as Politically Exposed Persons (PEPs);
- persons subject to information request from a law enforcement agency for ML &TF reasons;
- the product or transaction might favor anonymity;
- the situation involves non-face-to-face business relationships or transactions (as in the case of remote casinos), without certain safeguards such as an electronic identification process;
- subject to sanctions, embargoes or similar measures issued.

EDD measures to high-risk relationships and transactions include:

- Verifying the Customer's identity with at least two government-issued Identification Documents.
- Obtaining additional information on the Customer (and on the Customer's beneficial owner);
- Obtaining additional information on the intended nature of the business relationship, where different from the acquisition of gaming services by individuals;
- Obtaining information on the source of funds and source of wealth of the Customer (and of the Customer's beneficial owner);
- Obtaining information on the reasons for the transactions;
- Obtaining approval of senior management for establishing or continuing the continuous business relationship;
- Conducting enhanced ongoing monitoring of those Business Relationships.

With reference to PEPs, intended as individuals who hold or have held prominent public functions within the last 12 months, including heads of state, ministers, judges, military leaders or executives of state-owned enterprises, their family members and close associates, given the higher exposure to corruption or abuse of power, their position is subject to the following measures:

- risk classification increase;
- EDD procedures;
- escalation to the central AML function for review and clearance;
- documented analysis and management decisions.

5.3 Business Partners DD (Third Parties)

The Lottomatica Group applies robust due diligence standards to all its business partners – including suppliers, franchisees, distributors, agents, affiliates, white-label operators and technology vendors – with the objective of preventing exposure to legal, regulatory, and reputational risks linked to money laundering or the financing of terrorism.

A structured risk assessment and onboarding process is conducted prior to establishing any business relationship. The key elements include:

- Company Registry Verification: obtaining and analyzing official documentation such as

chamber of commerce extracts, corporate registration certificates and evidence of current legal status and authorized representatives;

- Legal Documentation: suppliers included in the value chain (i.e. distributors, retailers), although in possession of personal Police licence, are asked to provide official criminal background certificates and declarations of pending charges for key management personnel and owners at onboarding. Furthermore, all suppliers are required to provide such documentation in case of increase of their risk level;
- Ultimate Beneficial Ownership (UBO) Identification: full transparency is required regarding the ownership chain and control structure. Screening of UBOs and directors is carried out to assess potential ML & TF risk factors;
- Sanctions and PEP Screening: All legal entities, UBOs, and executives are screened against international and national sanctions lists, politically exposed persons databases and global enforcement watchlists;
- Adverse Media Analysis: a comprehensive search is performed across internal and external databases, open sources (OSINT) and indexed media reports to detect any reputational risk indicators. This includes allegations of financial misconduct, regulatory breaches or unethical business practices.

Lottomatica executes extensive due diligence and ongoing monitoring on non-domestic partners, leveraging proper means of investigations (such as the “Orbis” database by Bureau van Dijk) to conduct detailed screenings and risk assessments across ownership structures, sanctions, PEP status, adverse media, and regulatory watchlists, ensuring comprehensive coverage of cross-border financial and reputational risks.

No business relationship may be initiated or renewed unless the due diligence is completed to the satisfaction of the Group AML function. For high-risk partners or complex ownership structures, enhanced due diligence (EDD) is triggered and final approval is escalated to Senior Management.

The due diligence process is not a one-time activity but an ongoing obligation. Business partners are automatically monitored in order to ensure the maintenance of reputational requirements and their risk classification is kept updated. Significant ownership changes are subject to stricter analysis and investigations.

Ongoing Monitoring of reputational requirements

The AML framework of Lottomatica does not end with onboarding. A core component of the Group’s risk-based AML program is the continuous and dynamic monitoring of business partners over the full life cycle of the relationship.

The purpose of ongoing monitoring is to ensure:

- that any change in ownership structure is detected and promptly analysed;
- continuous screening against sanctions lists, PEP lists, and adverse media sources, especially when new UBOs or directors are added;
- deeper analysis in case of Authorities requests or investigations.

6 Sanctions and Risk List Screening

Lottomatica implements robust and automated screening protocols to prevent the establishment or continuation of relationships with sanctioned or high-risk individuals and entities.

Proper procedures and screening tools are implemented to ensure that the Group does not establish a relationship or provide any service to individuals and entities subject to international sanctions.

Through automatic screening tools, the Group screens Customers and other relevant persons or entities (i.e. business partners, suppliers, for legal persons the analysis includes all the natural persons who have management and representation powers, shareholders and beneficial owners) at least against the following databases:

- US sanctions lists (OFAC);
- OFSI's consolidated Sanctions List (UK);
- Consolidated list of EU financial sanctions and consolidated list of persons, groups and entities subject to EU financial sanctions;
- PEP screening.

Additionally, the Group Entities apply procedures for screening their Customers and Third parties against adverse media.

7 Self-Risk assessment Model

Group Risk Assessment represents a pivotal element in the strategy for preventing and combating money laundering and terrorist financing adopted by Lottomatica. Through a risk analysis that is conducted every six months, the aim is to identify, assess and mitigate the potential vulnerabilities that could expose the Group to any threats.

In line with current regulatory guidelines and industry best practices, Risk Assessment is a fundamental tool to ensure effective AML & CTF risk governance, ensuring that control activities are timely, targeted and proportionate to actual risks.

The Self-risk Assessment Model - implemented by Lottomatica with the support of PWC Anti Financial Crimes Dpt and independently assessed by KPMG as aligned to the best practices adopted by the financial sector - is applied to all companies belonging to Lottomatica Group; it is based on 135 indicators divided into 14 Risk Areas referred to each company, each industry and the overall vision.

The methodology for self-assessing the risk of money laundering and terrorist financing involves analysis, at the level of individual Group companies and at the consolidated level, along four lines: (i) calculation of the potential risk to which the Group is exposed; (ii) analysis of the effectiveness of the controls and risk mitigation measures adopted (vulnerabilities); (iii) determination of residual risk; (iv) identification of any remedial actions.

The results of the Self-Risk Assessment are reported in the AMLRO Report half-yearly drawn up by the Group Regulatory Compliance, AML & Quality Director and addressed to the BoD and Supervisory Bodies.

8 Suspicious Activity Reporting (SAR) process

8.1 Purpose and Importance

Lottomatica Group recognizes that timely and accurate reporting of suspicious activities is a cornerstone of an effective AML & CTF framework. Reporting Suspicious Activity Reports (SARs) is critical to assist competent Authorities in preventing and detecting money laundering, terrorist financing and other financial crimes. Failure to report suspicious transactions exposes the Group to significant legal, regulatory and reputational risks.

8.2 Identification of Suspicious Activity

Employees, contractors and third parties acting on behalf of the Group are required to remain vigilant for any behavior or transactions that appear unusual, inconsistent with the customer's profile or indicative of potential ML & TF. Examples include, but are not limited to:

- unusual transaction patterns or volumes inconsistent with known gambling behaviors;
- structuring or "smurfing" transactions to evade detection thresholds;
- use of third parties to conduct transactions without clear business rationale;
- involvement of high-risk jurisdictions or sanctioned entities;
- frequent cash deposits or withdrawals without clear source or purpose;
- sudden changes in betting behavior or withdrawal patterns;
- customers reluctant to provide or verify identity information.

8.3 Transaction Monitoring

The Group uses a risk-based approach to identify and monitor single transactions or patterns of transactions that present elements of suspicion.

On a regular basis, compliance personnel complete a review of those transactions selected by proper Key Risk Indicators determined by the risk assessment for that entity of the Group or anyway suspected to be connected to ML/TF activities. To facilitate this effort, data held by relevant departments and functions should be consulted, and such data should be shared and integrated to the extent feasible among those relevant departments and functions.

As warranted by the facts of any situation reviewed, compliance personnel may further review Third-party databases to determine the clients' business connections and history and any other information that will assist in explaining the transactions or in determining the source of funds used by the patron, in order to collect any information that is useful for a weighted assessment for the purposes of Suspicious Activity Reports ("SARs") and/or to terminate the relationship.

Circumstances warranting such review may include but are not limited to the following:

- Clients with large cash-in transactions with no cash-out transactions, which cannot be reasonably explained through transaction review (i.e., little or no gaming activity).
- Clients with large cash-out transactions with limited cash-in transactions, which cannot be reasonably explained through transaction review. Clients with large check cashing transactions and/or credit card advances with limited play.

- Clients with cash transactions, including aggregated transactions, that are just below the regulatory reporting threshold.
- Checks or wire transfers received for the benefit of the clients (or multiple clients) from Third parties whose connection to the client is suspect or unclear.
- Multiple transactions over a period of time with the apparent purpose of avoiding reporting requirements.
- A single payment received by the casino (e.g., negotiable instrument or wire transfer) for the benefit of clients if the casino cannot determine a relationship or business association between the source of the payment and the beneficiaries.

A risk-based framework allows the post-execution monitoring of transactions to identify for further investigation those which may be suspicious. The implemented monitoring procedures should be supported by appropriate tools, preferably automatic, bearing in mind the type of service, transaction, activity, and amount involved.

8.4 Investigation and Reporting of Suspicious Activity

Each transaction, behaviour or pattern is analysed considering anomaly indicators which may differ depending on the sector (i.e., VLT, physical betting, on-line gambling) and it is assessed through:

i) objective elements (extent, nature and characteristics of the transaction);

ii) subjective elements (economic capacity and type of activity);

iii) geographical elements (ML/TF risk of the Country where the transaction / activity took place).

A suspicious transaction, behaviour or activity must be immediately reported to the local FIU.

All the selected transactions are subjected to structured analysis by the AML Team which processes, aggregates and integrates the data on the basis of the information available in the company information systems, drawing up a summary information sheet that is analysed by the members of the Anti-Money Laundering Committee (or a Local Risk Equivalent Committee) for the assessment of whether the transactions are actually worthy of reporting to the FIU.

The fact that information is being, will be or has been transmitted to the FIU or any other law enforcement agency shall not be disclosed to the Customer concerned or to other Third parties.

The Group takes all appropriate measures to ensure the confidentiality of the identity of the persons making the reports, ensuring that individuals, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

8.5 AMLRO Reports

The purpose the AMLRO reports is to inform the Board of Directors and Supervisory Bodies on the monitoring and risk management activities carried out in the semester of reference, highlighting the main critical issues that emerged, and the mitigation measures adopted, so as to ensure full compliance with the company's strategic guidelines and regulatory provisions.

The AMLRO Report is subject to approval by the Board of Directors.

9 AML Training and Awareness

The Lottomatica Group considers AML & CTF training a cornerstone of its compliance culture and a critical element in its risk mitigation framework. It is mandatory that all employees and Third Parties acting on behalf of the Group maintain a thorough understanding of their legal obligations, internal policies, and operational responsibilities related to the prevention of money laundering and terrorist financing.

To ensure this, the Group implements targeted and tailored training programs designed according to specific audience profiles:

- third parties involved in terrestrial operations receive training focused on risks and controls pertinent to physical gaming environments;
- employees engaged in online operations undergo specialized modules addressing the unique AML & CTF challenges of digital platforms;
- “AML Sensitive” corporate functions benefit from advanced training to deepen their awareness and capability in identifying and managing money laundering risks.

Training is delivered primarily through dedicated online platforms, enabling flexible and scalable access across all Group Entities. To validate the effectiveness of the training, participants are required to pass assessment tests with a minimum score of 80%, ensuring the acquisition of adequate knowledge and competence.

All Group Entities are responsible for implementing these training and awareness initiatives, which are regularly reviewed and updated to reflect regulatory developments and evolving risk scenarios, thus guaranteeing an appropriate and current level of AML & CTF knowledge across the organization.

To this end, all Group Entities are required to implement training and awareness initiatives aimed at ensuring an appropriate and up-to-date level of knowledge on these issues. Training activities are structured on the basis of the reference regulatory guidelines and are constantly updated to reflect the evolution of the regulatory framework and risk scenarios.

10 AML/CTF Common Requirements

10.1 Regulatory Escalation and Cooperation

Lottomatica is committed to full cooperation with all regulatory and law enforcement Authorities. Upon request, the Group shall promptly provide documentation, records and other assistance to support investigations. The Group maintains transparent communication with regulators and ensures timely updates on AML-related matters.

10.2 Record Keeping

The Lottomatica Group entities must implement and maintain procedures and systems that ensure compliance with the rules laid down by the code on the protection of personal data as well as the processing of the same for the purposes relating to the prevention of the use of the financial system and the purpose of laundering the proceeds of criminal activities and of terrorist financing. The retention method guarantees complete and timely access to all information as well as the integrity and confidentiality of data and information after their acquisition.

The procedures must ensure that information and documentation is readily available so that documents and information can be used in any investigation or analysis of possible money laundering or terrorist financing by the competent national Authorities.

10.3 Confidentiality and Data Protection

All SAR-related information is treated with the highest confidentiality and disclosed strictly on a need-to-know basis. Unauthorized disclosure of SARs or related investigations is prohibited and may result in disciplinary action.

10.4 Testing and Monitoring of Controls

Independent compliance testing activities are regularly carried out to review and assess local AML/CTF control system in compliance with the AML/CTF Standards and applicable laws.

These testing activities could be carried out directly by the Internal Audit (or equivalent function) that implement and execute controls to check AML activity.

10.5 Regulatory Tracking

Procedures must be implemented and maintained in order to ensure that:

- changes to relevant Group Standards, AML/CTF laws, regulations and guidance are identified and their impacts on the Group and each entity is analysed;
- AML/CTF Program is modified and updated to reflect any material impacts of those changes.

10.6 Management Information and Reporting

The Group ensures appropriate internal management information sufficient to allow the access and monitoring of the effectiveness of controls and that appropriate reporting about the AML & CTF program is provided to Group Regulatory Compliance, AML & Quality Director, on a periodic basis to assess the status of the AML/CTF program and the effectiveness of the AML systems and controls.