PA REG 01

ANTI-MONEY LAUNDERING AND COUNTERING TERRORIST FINANCING GROUP POLICY

Approved by the Board of Directors

Table of contents

REVISION	REASON / REVISION CHANGES	DATE
Rev. 1	First issue	13th May 2022

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 06; • 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 10; • 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
Additional Background Check	Search conducted using an external media provider to identify reputational, legal and/or regulatory issues that may be associated with a Customer/Third party such as negative information, sanctions issues, PEPs, etc.
AML/CTF	Anti-Money Laundering & Counter-Terrorism Financing.
AML/CTF Program	The AML/CTF Program is a comprehensive framework or set of initiatives aimed at the mitigation of the risks. The AML/CTF Program must provide at least for: • written policies and procedures (with clear roles and responsibilities) • identified key control mechanisms • training programs • an effective line of communication to report misconducts • a disciplinary system

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.
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 & GRC.
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.
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 (referred to as “Group”), whose parent company is Lottomatica S.p.A., is the first Italian group operating in the legal gaming market and one of the major players in Europe.

The Group’s international growth foresees the provision of services to a diverse client base in Countries with varying degrees of financial crime risk and with different regulatory regimes, identifying and implementing the mitigation measures in order to manage potential legal, regulatory, and reputational risks in money laundering and terrorist financing. Failure to manage the risks may harm Group’s reputation and could lead to legal or regulatory actions.

This Policy is intended to provide a high-level framework to enable the Group Entities exposed to AML/CTF risk to identify potential money laundering and terrorist financing risks and to assist them in determining how to manage those risks.

This Policy also provides general information to all employees and the Third parties acting on behalf of the Group on the measures taken by Group Entities to identify, mitigate and manage money laundering and terrorist financing risks and it establishes minimum standards for the Entities’ AML and CTF Programmes.

This document defines roles and responsibilities, tasks, high-level AML requirements and operating methods (i.e. procedures, screening activities) for the prevention and management of the risk of the use of the financial system for the purpose of laundering of the proceeds of criminal activities and the financing of terrorism within the scope of gaming and gambling industries through the amusement and entertainment machines, the bets collected at points of sale/collection of the physical network as well as on-line gambling through the internet and other electronic or telecommunication networks.

The AML & CTF Group Policy is constantly updated and available to all staff, in accordance with the regulatory framework.

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.

2.2 Approval and Review

This Group Policy is subject to the approval by the Board of Directors of Lottomatica S.p.A. and at least annually reviewed or confirmed.

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.

2.3 Scope of Application

The minimum standards set out in this Policy cover specific AML requirements and common AML & CTF requirements.

This Policy is addressed to:

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

The Group adopts a zero-tolerance approach against individuals who attempt to or breach external and internal provisions related to AML/CTF.

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 mitigants.

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 Roles and Responsibilities

To ensure compliance with all the applicable AML / CTF laws as well as the provisions of this Policy, the Group assigns roles and responsibilities to all levels of the organization.

3.1 Board of Directors

The Board of Directors of Lottomatica SpA (“BoD”), as parent company of the Group, adopts strategic decisions regarding the management of ML/TF risks for the entire Group; it reviews and approves the guidelines and Group procedures on AML & CTF.

The Board of Directors also ensures that roles and responsibilities regarding the prevention of the use of the financial system for the purposes of AML/CTF are clearly and appropriately defined, guaranteeing that the operational and control functions are distinct and that these functions are performed by qualitatively and quantitatively adequate resources.

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.

3.2 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.

3.3 Supervisory Board

Within the scope of its powers and responsibilities, the Supervisory Board oversees compliance with the rules contained therein and the publications of the required reports.

Reports can be made jointly with other corporate bodies or departments.

3.4 Group Regulatory Compliance, AML & Quality Function

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 optimise 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.

3.5 AML Committee or Local Risk Equivalent Committee/Function

The Anti-Money Laundering Committee, hereinafter "AML Committee", or the Local Risk Equivalent Committee/Function, is convened regularly with the aim to carry out the following activities:

- analyse suspicious transactions produced by the Group Entities' transaction monitoring tools as well as any reports of potentially suspicious transactions received from staff or from business partners;
- evaluate the anomalous positions and transactions found through in-depth analyses performed by AML teams;

- inform the Suspicious Transaction Reporting Delegate of the transactions to be reported to the local FIU.

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.

3.6 Suspicious Transaction Reporting Delegate

The Suspicious Transaction Reporting ("STR" in hereinafter) Delegate assumes the role of the STR contact person and is responsible for ensuring that:

- any suspicious transaction is submitted to the Anti-Money Laundering Committee (or Local Risk Equivalent Committee/Function) for evaluation;
- the draft and record-keeping of the minutes of the Anti-Money Laundering Committee (or Local Risk Equivalent Committee/Function) meetings;
- suspicious transactions as assessed by the Anti-Money Laundering Committee (or Local Risk Equivalent Committee/Function) 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.

3.7 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/CFT policies, controls and procedures.

3.8 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 AML/CTF Risk Based Approach: controls and monitoring for risk mitigation

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 AML Group requirements

5.1 Customer Risk Classification

The Groups adopts a risk-based approach to Customer classification. Customers' ML/TF risk must be assessed according to the local regulations to determine whether entering or continuing a business relationship with them is permitted.

The identification of the Customers takes place through appropriate KYC and Transaction Monitoring tools which allows the acquisition of information related to: i) Customer's identification data ii) the date of the gambling transaction, iii) the value of the transactions and iv) the mean(s) of payment used.

All Customers are classified by the single entity according to the AML/CTF Group Standards. Risk level factors include:

- Duration of relationship with Customer;
- PEP - whether the Customer poses a high ML risk because they are a Politically Exposed Person (PEP);
- Negative news - when there is serious relevant negative information concerning the Customer that may impact the Group's reputation;
- Terrorism and Sanctions - where there is a higher risk that the Customer may be associated with terrorism or sanctioned activities considering the location or business.

A local procedure should be adopted in order to put on hold the process in case of potential match. The AML local team/Function is responsible for carrying out the necessary checks to determine whether any match is true or a false positive.

5.2 Customer Due Diligence Measures (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 regulation for each sector as explained below (VLT, on-line gambling, physical betting).

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.

5.3 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 favour 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.

6 Screening

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 an automatic screening tool[1], the Group screens Customers and other relevant persons or entities (i.e. business partners, suppliers, for legal persons the analysis includes all

[1] See the definition in Chapter 1 of this Policy "Glossary and definition"

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 Reporting Obligations

7.1 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.

7.2 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 AML/CTF Common Requirements

8.1 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.

8.2 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.

8.3 Training

Employees and Third parties acting on behalf of Group must be trained on the AML regulation, the content, meaning of and requirements set forth by this Policy and its related procedures.

Therefore, all Group Entities must provide adequate training and awareness initiatives in order to ensure appropriate knowledge on these subjects.

The training activities based on regulatory guidelines are constantly updated.

8.4 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.

8.5 Management Information and Reporting

The Group ensures an 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.

8.6 Due Diligence on Third Parties

Group and each entity must conduct adequate controls and due diligence on the Third parties and business partners (e.g., suppliers, counterparties, companies to be acquired) with whom they enter into business to avoid engaging with subjects involved in ML/TF matters.

Before establishing the business relationship and periodically depending on the risk rating, Third parties or business partners (including Ultimate Beneficial Owner) must be subject to sanction, PEP and adverse media screening as formalized in this Policy.

Any negative news (including sanctions' matches) must be escalated to the entity's AML function and to Group's AML if needed to determine whether to maintain or cease the relationship.