GROUP AML/CFT AND SANCTIONS POLICY

Anti-Money Laundering, Counter-Terrorist Financing and Targeted Financial Sanctions

FDJ UNITED

TABLE OF CONTENTS

Objectives and scope.....3

Definitions.....4

Governance and management commitment.....5

AML/CFT and sanctions risk assessment.....6

ML/TF prevention and detection measures.....7

Information Retention and Data Protection.....8

Reporting and cooperation with authorities.....9

Sanctions screening and asset-freezing measure.....10

Training, controls and continuous improvement.....11

Regulatory references.....12

This policy sets out the FDJ UNITED Group framework for preventing, detecting and managing the risks of money laundering, terrorist financing and the non-implementation or evasion of targeted financial sanctions across its activities.

It applies to FDJ UNITED and its AML/CFT obliged entities, in France and internationally, proportionately to their activities, risk exposure and local regulatory obligations. It provides a common reference framework for employees and equivalent staff, and a basis for expectations applicable to relevant third parties including retailers, payment partners, suppliers and service providers.

The policy covers the Group's lottery, gaming and betting activities, digital channels, retail distribution networks, payment services and other diversified services where applicable.

The main objectives are to:

- promote a strong culture of integrity, vigilance and accountability;
- ensure a harmonised, risk-based and proportionate AML/CFT and sanctions framework across the Group;
- prevent, detect, analyse and report suspicious activity to the competent Financial Intelligence Units and authorities;
- ensure compliance with applicable AML/CFT, sanctions and asset-freezing requirements in each jurisdiction;
- support effective governance, internal control, training, record-keeping and continuous improvement.

Money laundering is the process by which the proceeds of criminal activity are concealed, converted, transferred or used in order to disguise their illicit origin or give them an appearance of legitimacy.

Terrorist financing refers to the provision, collection or use of funds or economic resources, directly or indirectly, with the intention or knowledge that they may be used to finance terrorist acts, organisations or individuals.

Targeted financial sanctions and asset-freezing measures are restrictive measures adopted by competent authorities, including the United Nations, the European Union and, where applicable, national authorities, requiring the freezing of funds and economic resources of designated persons or entities and prohibiting the making available of funds or economic resources to them.

The Group applies a risk-based approach: measures are calibrated according to the nature, scale and complexity of the activity, the customer profile, products and services, distribution channels, transaction patterns and geographic exposure.

Risk factors relevant to Group activities

- products and services: lottery, betting, online and land based gaming, poker and payment services;
- distribution channels: retail network, online and mobile channels, intermediaries and partners;
- transaction characteristics: stakes, deposits, withdrawals, payment instruments, frequency, velocity, unusual patterns and thresholds;
- customer characteristics: identity of individuals or legal entities, identification of the beneficial owners where relevant, politically exposed person status and adverse information;
- geography: country of residence, origin or destination of funds, high-risk third countries and sanctions exposure.

The Group's AML/CFT and sanctions framework relies on clear governance, senior management commitment and documented responsibilities at Group and entity levels.

At Group level, FDJ UNITED defines the common principles, minimum standards and methodological framework. It oversees the consistency and effectiveness of arrangements implemented by relevant entities, while respecting local legal and supervisory requirements.

Each relevant entity is responsible for implementing an AML/CFT and sanctions framework adapted to its own risk profile and regulatory obligations, including the designation of competent persons responsible for implementation, compliance oversight and reporting to the competent Financial Intelligence Unit where required.

Group governance principles

- senior management oversight and regular reporting on key AML/CFT and sanctions risks;
- clear allocation of roles and responsibilities between business teams, compliance, risk, legal, security, internal control and internal audit;
- coordination through Group-level committees and working groups to share information, methodologies, incidents and remediation plans;
- independent controls and audit work to assess the adequacy and effectiveness of the framework;
- documented policies and procedures, approved, distributed and regularly updated.

The Group performs and maintains a risk assessment framework covering money laundering, terrorist financing and sanctions risks. This framework is designed to identify inherent risks, assess mitigating controls and determine residual risks requiring action plans.

Each relevant entity prepares and updates its own risk classification, consistent with the Group methodology and considering local regulations, products, services, channels, customers, transactions and geographic exposure.

Risk assessments are reviewed regularly and when significant changes occur, such as new products, new jurisdictions, acquisitions, regulatory developments, changes in payment methods or material incidents.

Outcome of the assessment

- risk-based customer due diligence and transaction monitoring scenarios;
- prioritised remediation plans for the most significant risks;
- adapted training, controls, staffing and tools;
- regular reporting to management and relevant governance bodies.

The Group implements prevention and detection measures designed to ensure that customers, transactions and business relationships are appropriately understood and monitored, in accordance with applicable laws and regulations.

Know Your Customer and customer due diligence

Relevant entities identify and verify customers and, where applicable, beneficial owners, before establishing a business relationship or carrying out occasional transactions when required by law or risk-based procedures. Customer information is kept up to date throughout the relationship.

Enhanced due diligence is applied where higher risks are identified, including politically exposed persons, high-risk jurisdictions, unusual transaction behaviour, adverse information, complex or opaque structures and situations involving heightened sanctions or terrorist financing risks.

Transaction monitoring and alert handling

Relevant entities maintain monitoring arrangements to detect atypical or suspicious transactions and behaviours. Alerts are analysed by specialised teams and may lead to documented closure, enhanced review, customer restrictions, account closure, suspicious activity reporting or other measures permitted by law.

Retail and online channels

Physical points of sale are subject to onboarding, authorisation and control arrangements designed to ensure partner integrity and compliance with applicable rules. Online activities rely on registration, identity verification, account certification, payment method controls and behavioural monitoring. Controls are adapted to each entity’s products and risk exposure.

Customer and transactional information, supporting documents and records collected as part of due diligence measures, control results, alert analyses, and decisions to close cases or submit reports shall be retained for the periods required under applicable laws and regulations. These retention periods shall be determined taking into account, where relevant, local requirements, statutory limitation periods, and requests from competent authorities.

Records shall be retained in a manner that ensures the traceability of the due diligence measures performed, the analyses conducted, and the decisions made. The information retained must be accurate, relevant, accessible, and sufficiently documented to be made available to competent authorities within the required timeframe.

Personal data shall be collected and processed only to the extent necessary to comply with anti-money laundering, counter-terrorist financing, and financial sanctions obligations. Such processing shall comply with applicable data protection principles, including lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

Access to this information shall be strictly restricted to authorised employees and functions, in accordance with the need-to-know principle.

Where an entity subject to AML/CFT obligations knows, suspects or has reasonable grounds to suspect that funds, transactions or activities may be linked to money laundering, terrorist financing or sanctions evasion, the matter must be analysed without delay in accordance with internal procedures. Where the suspicions cannot be ruled out following the investigation, a report must be submitted to the Financial Intelligence Unit within the timeframes prescribed by local regulations.

Employees must report any unusual or suspicious situation through the designated internal reporting channels and provide all information necessary for its assessment. Under no circumstances may they inform the customer or any unauthorised third party of the existence of an analysis, a report or a request for information from an authority. The Group strictly protects the confidentiality of internal reports, analyses and decisions, in accordance with applicable tipping-off prohibitions.

The Group cooperates fully with competent authorities and responds diligently to legally valid requests, in compliance with local requirements, confidentiality obligations and applicable rights. Communications with authorities shall be handled by authorised functions in a secure and traceable manner, and the information disclosed shall be limited to what is necessary to address the request.

The Group implements measures to comply with applicable targeted financial sanctions and asset-freezing obligations. These measures include screening of relevant customers, counterparties and, where appropriate, partners and third parties against applicable sanctions lists.

Potential matches are reviewed promptly by trained teams. Confirmed matches, asset-freezing obligations or prohibitions on funds or economic resources being made available are handled in accordance with applicable legal requirements, internal escalation procedures and reporting obligations to competent authorities.

Sanctions controls are regularly reviewed to reflect changes in applicable lists, regulatory expectations, business activities and Group exposure.

The Group ensures that employees and equivalent staff receive regular AML/CFT and sanctions training proportionate to their roles and exposure. Targeted training is provided to teams involved in customer onboarding, transaction monitoring, investigations, reporting, sanctions screening, controls and management oversight.

The internal control framework is based on the three lines of defence: operational controls by business teams, oversight and permanent controls by compliance and control functions, and periodic independent reviews by internal audit.

Findings from controls, audits, incidents, regulatory changes and supervisory feedback are used to strengthen procedures, tools, training and governance. Remediation plans are tracked until completion and reported to appropriate governance bodies.

This policy should be read in conjunction with the following sources and with applicable local requirements.

Reference	Relevance
FATF Recommendations	International standards on anti-money laundering, countering terrorist financing and proliferation financing.
Directive (EU) 2015/849, as amended	Current EU AML/CFT framework until replacement by the new AML package according to applicable timelines.
Regulation (EU) 2024/1624 (AMLR)	Directly applicable EU rulebook setting harmonised AML/CFT requirements for obliged entities. **Applicable in 2027**
Directive (EU) 2024/1640 (AMLD6)	Rules for national AML/CFT systems, supervision, FIU cooperation and registers, to be transposed by Member States.
Regulation (EU) 2024/1620 (AMLA Regulation)	Establishes the EU AML/CFT Authority and its supervisory and coordination role.
Applicable national laws and regulations	Local requirements in the jurisdictions where Group entities operate, including sector-specific gambling, payment and sanctions obligations.

Document owner: Group AML/CFT and Sanctions Compliance.

September 2026

LA FRANÇAISE DES JEUX
SIÈGE SOCIAL 3-7 QUAI DU POINT DU JOUR
92100 BOULOGNE-BILLANCOURT
01 41 10 35 00
WWW.FDJUNITED.COM

FDJ UNITED