Anti-Money Laundering and Terrorist Financing Prevention Policy

ÖRIA

JUNE 30TH, 2022

Version	Reason for Change	Date	Author	Department
1.0	Original version of the Anti-Money Laundering and Terrorist Financing Prevention Policy	June 30th, 2022	Luciana de A. Trindade	Compliance

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION POLICY OF ORIA GESTÃO DE RECURSOS LTDA

1. INTRODUCTION

ORIA GESTÃO DE RECURSOS LTDA. ("ORIA") is a Private Equity & Venture Capital (PE&VC) investment manager focused solely on Information Technology (IT) assets and privately-held companies not quoted on Stock Exchanges and with limited liquidity.

ORIA is engaged solely in management of securities portfolio and is duly register under the category set forth in paragraph 1, item II of Brazilian Securities Commission (CVM) Instruction 558 of March 26, 2015 ("CVM Instruction 558/15") as a manager of Equity Investment Funds ("Funds") regulated under Brazilian Securities Commission (CVM) Instruction 578/16. The fiduciary management and custody of such funds are outsourced.

1.1 Purpose

The purpose of this Anti-Money Laundering and Terrorist Financing Prevention Policy (the "PLDFT") is to guide and establish guidelines regarding the prevention and combat of actions that may qualify as money laundering and/or terrorist financing, subject to the provisions of Law No. 9.613/1998, as amended from time to time, Law No. 13.260/2016, Law No. 13.810/2019, Brazilian Securities Commission (CVM) Resolution 50 ("CVM 50/21"), and other rules issued by the Brazilian Securities Commission (CVM) and by the Central Bank (BACEN) on the matter, as well as to the applicable international laws, being supplementary to the provisions of the Code of Ethics and of other internal policies.

All officers and employees are required to know and understand the terms of this Policy, as well as to seek to prevent and detect operations or transactions that show atypical features.

The knowledge of any evidence of criminal money laundering must be reported to the Compliance Department, which is in charge of verifying the reported information and, if applicable, after an analysis process, reporting it to regulators.

Through this Policy approved by the Executive Board, ORIA undertakes to develop and maintain effective processes, procedures, and controls for prevention, detection, and remediation with risk-based analysis reflecting local and international best practices.

2. CONCEPT

The term "money laundering" means concealment or disguise of the nature, origin, location, disposition, movement, or ownership of goods, rights, or valuables resulting directly or indirectly from crime.

Money laundering is understood as a set of commercial or financial transactions that seek to incorporate funds that originate from illegal acts into the formal economy by giving them a lawful appearance and making tracking difficult.

The activities of raising, intermediating, and investing own or third-party funds in local or foreign currency may be used in illegal financial transactions, which makes the financial system particularly vulnerable to money laundering.

Suspicious and/or attention-needed activities involve, for example, situations that:

I. Show features with respect to the parties involved, amounts, forms of performance, and instruments used or that, due to the lack of economic or legal basis, are somehow suspicious;

II. Maintain a relationship and transactions with politically exposed persons of Brazilian or foreign nationality;

III. Show evidence of circumvention of identification and registration procedures;

IV. Involve clients or transactions in which it is not possible to identify the ultimate beneficiary;

V. Originate from or are destined for countries or territories that insufficiently apply the recommendations of the Financial Action Task Force on Money Laundering Terrorist Financing (FATF/GAFI);

VI. Declare various bank accounts and/or change them regularly;

VII. Evidence a sudden and objectively unjustified change with respect to the types of transaction normally used;

VIII. Have a degree of complexity and risk incompatible with the technical qualification of the client or of its representative;

IX. In which it is not possible to keep registration data updated;

X. Involve an attorney-in-fact who has no apparent relationship.

3. SCOPE

This policy must be complied with by all employees of ORIA, particularly by personnel allocated to areas that maintain relationships with clients and third parties. Thus, each employee is responsible for identifying and reporting to the Officers or to the Compliance Department when any situation that may qualify as suspicious is found so that ORIA can timely take the appropriate measures.

The Executive Board is committed to providing financial, material, and human resources for the implementation, maintenance, effectiveness, and continuous improvement of the anti-money laundering and Terrorist Financing Prevention policy, procedures, and internal controls.

4. ACTIVITIES OF COMPLIANCE

To ensure compliance with the practices set forth in this Policy, the Compliance Department will conduct periodic risk analysis and require all providers of services to the funds under its management to have in place and comply with strict policies in compliance with the applicable laws and regulations for the purpose of identifying clients, gathering relevant information, maintaining up-to-date records, assessing and

monitoring clients and transactions, and identifying the ultimate beneficiary of any and all transactions.

In order to identify potential evidence of money laundering or terrorist financing practices by clients and other individuals and legal entities directly or indirectly involved in the proposed transaction or in events prior the inception of the relationship with ORIA, the Compliance Department may conduct independent surveys of negative entries on digital media and available restrictive lists in order to establish whether or not the relationship with the client may pose potential risks to ORIA.

In addition, the Compliance Office is responsible for:

(i) Developing and implementing tools and procedures that support the anti-money laundering and Terrorist Financing Prevention strategies of ORIA;

(ii) Submitting reports to management on assessments of any relevant money laundering risks that it has identified or been informed of;

(iii) Deciding whether any relevant risks in terms of compliance and money laundering require additional monitoring or the opening of an investigation;

(iv) Interacting with regulators and reporting any suspicious activity under applicable law;

(v) Training Employees, keeping records of such training materials, and developing and promoting campaigns and activities to support Employees in detecting suspicious transactions;

(vi) Auditing and ensuring that dealers and administrators of funds managed by ORIA comply with the provisions of this Policy and have adequate and sufficient internal rules and procedures to identify and combat money laundering and terrorist financing actions; and

(vii) Keeping all procedures for submission to regulators documented as required.

5. ASSET IDENTIFICATION PROCESS (Investees)

In Equity Investment Funds ("FIPs"), the manager must perform detailed due diligence on potential companies before submitting them for approval to its Executive Committee and deciding to commit capital.

Such due diligence may be carried out directly by ORIA or through contracted specialized companies or law firms and may include, for example, an analysis of the corporate structure of the target company, detection of entries in restrictive lists or negative media – either with respect to the company itself or to its main shareholders and managers –, or any other means that may be suited to the specifics of each case.

The analysis of the counterparty of a given transaction may also be the subject of due diligence, with special attention being given to structures in which a same party or group of related or connected parties are on different ends of the transaction or perform roles that depend on or suffer interference from one another.

ORIA must also verify, internally or through third-party contractors, before and periodically after the investment, whether (i) the company or its ultimate beneficiaries or officers are included in trading restriction lists such as the World Bank Group Listing of Ineligible Firms and Individuals, The Financial Conduct Authority (FCA UK), and other internationally recognized sanctions lists such as those of the UN and OFAC, (ii) any of such individuals are PEPs, and (iii) there is any public information that raises suspicions regarding the good faith of such individuals which should be further investigated.

The due diligence report is reported to the Executive Committee of ORIA, which takes its results into account to make a decision on whether or to make the investment and/or design an action plan to address issues arising from the due diligence.

As the assets below are subject to compliance with various regulatory obligations, ORIA is exempt from conducting additional due diligence under this Policy with respect to the following assets:

(i) Assets that have been the subject of initial and secondary public offerings registered under the rules issued by the Brazilian Securities Commission (CVM);

(ii) Assets that have been the subject of public offerings with restricted efforts exempt from registration under the rules issued by the Brazilian Securities Commission (CVM);

(iii) Assets issued or traded by a financial institution or similar entity;

(iv) Assets issued by securities issuers registered with the Brazilian Securities Commission (CVM);

(v) Assets of the same economic nature as those listed above when traded abroad, as long as (a) they are listed on stock, commodities, and futures exchanges or registered in a registration, custody, or settlement system duly authorized in their countries of origin and supervised by a local authority recognized by the Brazilian Securities Commission (CVM) or (b) their existence has been ensured by third parties duly authorized to perform custody activities in signatory countries of the Treaty of Asunción or in other jurisdictions or supervised by a local authority recognized by the Brazilian Securities Commission (CVM).

In cases ranked as high risk, ORIA must ask the target company or individual, as the case may be, to authorize a more in-depth investigation of PLDFT-related issues – when such authorization is required or desirable – so that ORIA can request any additional information that is not publicly available. The decision to carry out such further investigation will be made by the Executive Committee of ORIA.

If illegal practices are identified in investees, or if an investee becomes part of a sanctions list, ORIA will demand immediate actions, which may include (i) holding the officers of the investee liable, with suspension of the executive and reporting to the relevant authorities, (ii) enforcement of the provisions of the shareholders' agreement, if any, and (iii) recommendation for the Fund to sell its interest or acquire interests from another party in the investee, among other measures to be considered in each case.

6. IDENTIFICATION OF CLIENTS, EMPLOYEES AND THIRD PARTIES

6.1 Know Your Client ("KYC") and Anti-Money Laundering and Terrorist Financing Prevention

As the main activity of ORIA is the management of third-party assets, it is subject to several rules on "KYC" (Know Your Client) and identification and knowledge of investors or clients aimed especially at preventing and combating money laundering.

Given the role of the company, combating and preventing money laundering is a critical point; accordingly, the funds managed by ORIA must have reputable administrators and dealers that have their own KYC, Suitability, and anti-money laundering policies.

Dealers and administrators of the funds managed by ORIA must implement and maintain a register of all their clients and update at most every twenty-four (24) months, for a period of five (5) years, after the closing of each account.

ORIA will always take all necessary measures, whether reporting to regulators and authorities or internal sanctions in cases where there is any suspicion of money laundering. The Compliance Department will, in the performance of its duties:

i. Adopt control measures, in accordance with previously and expressly established procedures, that seek to confirm the registration information of clients or counterparties in order to prevent the use of the account by third parties and identify the ultimate beneficiaries of transactions, according to the nature of the transaction and the possibility of such identification;

ii. Record and advise the officer in charge of managing third-party assets if, in the registration analysis of the client, there is any suspicion regarding its economic/financial activities or if a politically exposed person (PEP) is identified;

iii. Keep a record of all transactions carried out by ORIA for a period of at least five (5) years after the date of their consummation;

iv. Strictly supervise transactions and relationships maintained by persons regarded as politically exposed whose portfolios are managed by ORIA, as defined under Brazilian Securities Commission (CVM) Instruction No. 617/2019, as amended from time to time, and make sure that their registration is up-to-date; and

v. Identify whether foreign investors whose portfolios are managed by ORIA are clients of a foreign institution supervised by a governmental authority similar to the Brazilian Securities Commission (CVM); if yes, anti-money laundering measures may be taken by such foreign institution, as long as access to data and procedures is ensured to the Brazilian Securities Commission (CVM).

Each Employee, particularly when involved in the client registration, monitoring, and relationship process, is required to notify the Compliance Department in case any activities suspicious of money laundering or terrorist financing are found.

6.1.1 Client Ranking

All clients must be internally ranked, which is performed by providers of service to funds managed by ORIA and by the Compliance Department, based on their risk potential to generate greater or lesser exposure according to the nature of their activities, demanding more or less due diligence according to the continuous assessment of their relationship and level of susceptibility to involvement in criminal money laundering and terrorist financing.

The risk level of the client must be defined, as a minimum, as high, medium, or low and periodically updated, with a focus on potential money laundering or terrorist financing practices. The result of the analysis will allow the client to be properly ranked for monitoring.

6.2 KYE – Know Your Employee

Employee activities and hiring are also a point of attention for this Policy. Thus, the activities developed by employees directly hired by ORIA and their history must be assessed, and only after that the hiring process may continue, based on the internal risk ranking and on the relevance of the information involved.

The procedures must ensure the identification and qualification of employees, and, if any inconsistency or risk factor is found, the recruitment area must forward the identified item to the Compliance Department for analysis and approval. After approval by the Compliance Department, the recruitment area may proceed with the applicant hiring process.

After the steps above, the employee will be ranked in a risk category. For higher-risk employees, supplementary procedures and actions must be adopted that involve in-depth monitoring and assessment measures and specific authority levels.

Such information must be kept up-to-date. Data updating frequency should be guided by the internal risk ranking, subject to any events that may imply an urgent need to change the risk ranking, and should not longer than five (5) years.

The "know-your-employee" process must also promote organizational risk culture through permanent training, as well as provide specific training to areas regarded as sensitive for the money laundering and terrorist financing risk management process.

All know-your-employee procedures must be available to regulators for access.

6.3 KYP – Know Your Partners

This is a procedure and control that must be adopted by the procurement areas of ORIA for the identification, qualification, and acceptance of third parties and must be compatible with this Policy, as well as aligned with the internal risk assessment, in order to prevent contracting of individuals or legal entities that are disreputable or suspected of involvement in illegal activities. For those that pose a greater risk, supplementary procedures, in-depth assessment measures, and specific authority levels must be adopted, according to the criticality of the entries or exceptions.

The activities developed by third parties must be assessed based on the internal risk ranking associated with them and on the relevance of the information involved.

Such information must be kept up-to-date. Data updating frequency should be guided by the internal risk ranking, subject to any events that may imply an urgent need to change the risk ranking, and should not longer than five (5) years.

All know-your-partners procedures must be available to the regulator for access.

6.4 PEP (Politically Exposed Persons)

In accordance with the definition set forth in Brazilian Securities Commission (CVM) Resolution No. 50/2021, PEPs are regarded as government agents that hold or have held, in the last five (5) years, in Brazil or in foreign countries, territories, and dependencies, any relevant public positions, jobs, or functions, as well as their representatives, relatives, and other close associates, including:

I - Holders of elective offices in the Federal Executive and Legislative Branches;

II - Holders of the following positions in the Federal Executive Branch:

- Minister or equivalente;
- Special officer or equivalent;
- Chief executive officer, vice president, and officer or equivalent of instrumentalities, public foundations, public companies, or government-controlled corporations; and
- Senior Management and Advisory Group (DAS) level 6 officer or equivalent;

III - Members of the National Council of Justice, of the Federal Supreme Court, and of the higher courts;

IV - Members of the National Council of Justice, of the Federal Supreme Court, of the higher courts, of the regional federal, labor, and electoral appellate courts, of the Superior Council of Labor Justice, and of the Federal Justice Council;

V - Members of the National Council of the Public Prosecution Office, the Federal Attorney General, the Vice Federal Attorney General, the Labor Attorney General, the Military Attorney General, the Deputy Federal Attorneys General, and State and Federal District Attorneys General;

VI - Members of the Federal Accounting Court and the Attorney General of the Public Prosecution Office with the Federal Accounting Court;

VII - State and Federal District governors, state chief justices, speakers of state and federal district legislatures, chief justices of State, Federal District, and Municipal accounting courts, and chairmen of Municipal accounting councils;

VIII - Mayors and speakers of City Councils of State capitals;

IX - Politically exposed persons also include persons abroad who are (i) heads of state or heads of government, (ii) high-ranking politicians, (iii) holders of high-ranking government positions, (iv) general officers and high-ranking members of the Judiciary, (v) high-ranking executives of public companies, or (vi) political party officials;

X - Politically exposed persons also include high-ranking officials of public or private international law entities.

7. RISK-BASED APPROACH

ORIA adopts a risk-based approach to money laundering and terrorist financing assessment so that the preventive measures implemented are directly proportional to the risks found.

This means that ORIA will carry out periodic risk assessments to monitor its service providers, using its best efforts to ensure that they follow the applicable national and international guidelines.

The risk assessment methodology must take into account (i) the trading environment, (ii) the formation of the price of the traded asset, and (iii) the counterparty to the transaction, as well as the investment mandates granted by the investment funds under its management, to rank transactions, as a minimum, as low-, medium-, or high-risk.

8. REPORTING OF SUSPICIOUS TRANSACTIONS

Due to the particulars of its activities, ORIA will, through its Compliance Department, conduct periodic risk analysis and require all service providers of funds under its management to have and comply with strict policies in compliance with applicable laws

and regulations for the purpose of monitoring, identifying, and reporting operations and transactions regarded as suspicious from an anti-money laundering and Terrorist Financing Prevention point of view.

If ORIA, within the scope of its activities, identifies operations or transactions regarded as suspicious, this will be reported to the relevant regulators, when applicable, in compliance with the legal and regulatory provisions. Reporting in good faith do not give rise to civil or administrative liability to ORIA or to its managers and employees.

Reporting must contain, as a minimum:

i. The date of inception of the relationship of the reporting party with the person carrying out or involved in the transaction or situation;

ii. A reasoned explanation of the warning signs found;

iii. The description and details of the features of the transactions carried out;

iv. A presentation of the information obtained through the due diligence processes set forth in art. 17 to qualify those involved, including whether or not they are politically exposed persons, and detailing the behavior of the reported person; and

v. The conclusion of the analysis, including a reasoned report characterizing the warning signs identified as a suspicious situation to be reported the Financial Intelligence Unit containing, as a minimum, the information defined in the other items of this paragraph.

Reporting must be made within twenty-four (24) hours from the completion of the analysis that characterized the atypicality of the transaction, of the respective proposal, or even of the atypical situation detected as a suspicion to be reported to the Financial Intelligence Unit.

Reporting to the Council for Financial Activities Control (COAF) must be made without notice to the parties involved.

8.1. Reporting of No Occurrence

8.1.1. Brazilian Securities Commission (CVM) Segment

ORIA must annually carry out, through the mechanisms established in the agreement between the Brazilian Securities Commission (CVM) and the Financial Intelligence Unit, reporting of no occurrence when no situations, transactions, or transaction proposals that should be reported have been recorded in the previous calendar year.

9. INFORMATION CONFIDENTIALITY

All information on evidence or suspicions of money laundering and terrorist financing are confidential and should not, under any circumstances, be made available to third parties.

Reporting of suspected cases should not be disclosed to the client involved. Employees of the Compliance Department (within their responsibilities and roles) are authorized to participate in the identification and reporting process for submission to and exclusive use by regulators for analysis and investigation.

10. SANCTIONS IMPOSED BY UNITED NATIONS SECURITY COUNCIL (UNSC) RESOLUTIONS

ORIA must immediately comply, without prior notice to those sanctioned, with the measures established in UNSC sanctioning resolutions or with the designations of its sanctions committees that establish the freezing of assets of any value which are directly or indirectly held by individuals, corporations, or entities under Law No. 13.810 of 2019, without prejudice to its duty to comply with judicial freezing orders as also provided in such law.

Freezing refers to the prohibition to directly or indirectly transfer, convert, move, make available, or dispose of assets, which also applies to interest and other civil proceeds and income arising from the contract, in accordance with the provisions of art. 2, item II and art. 31, paragraph 2 of Law No. 13.810 of 2019.

ORIA must immediately report any freezing of assets and attempts to transfer such assets with respect to individuals, corporations, or entities sanctioned by a UNSC resolution or by designations of its sanctions committees, in accordance with art. 11 of Law No. 13.810 of 2019, to:

i. The Central Bank of Brazil, through the BC Correio system;

ii. The Brazilian Securities Commission (CVM);

iii. The Ministry of Justice and Law Enforcement (MJSP); and

iv. The Financial Intelligence Unit.

11. CLARIFICATION OF DOUBTS, APPROVAL OF EXCEPTIONS AND WHISTLEBLOWING

11.1 Doubts

In case of any doubts about any rule and/or its application to a particular situation, you are advised to contact your supervisor or the Compliance Department.

11.2 Approval of Exceptions

Any and all exceptions or exemptions from the application of the rules of this Policy depend on prior approval from the managers and from the Compliance Department.

11.3 Obligation to Report Violations

Any violation of any rule of this or of any ORIA Policies, laws, rules, or regulations, perpetration of fraudulent actions, including actions of third parties, or dishonesty on the part of any employee must be immediately reported to the Compliance Department in person or by email to compliance@oriacapital.com.br.

Cases involving harassment or intimidation for non-compliance with this Policy must also be reported to the Compliance Department.

Confidentiality of the identity of any person who reports a violation or evidence of violation will be safeguarded, except in cases where the disclosure of such information is legally or judicially required.

ORIA does not allow any form of retaliation for any whistleblowing in good faith from its employees or third parties.

12. TRAINING

The Compliance Department must conduct annual training with employees who have access to confidential/privileged information and who participate in the investment decision-making process.

Additional training on policies, internal rules, and laws may also be carried out jointly with employees in the event of a substantial change in the guidelines.

Employees involved in the client registration, monitoring, and relationship process must be trained so that they have the ability and understand the duty to notify the Compliance Department in the event of identification of suspected money laundering or terrorist financing activities.

13. CONSEQUENCES OF THE VIOLATION OF RULES, POLICIES AND REGULATIONS IN FORCE

This Policy prevails over any prior oral or written understandings, and its terms and conditions are binding on the Employees of ORIA.

Any violation of any of the provisions of this Policy or of any law or rule relating to our activities, as well as any failure to cooperate with an internal investigation, may result in disciplinary measures, such as warning, suspension, or termination with cause, depending on the severity and recidivism of the violation, without prejudice to the applicable civil and criminal penalties.

14. PERIODIC REVISION

This Policy must be periodically revised for adjustment and monitoring as required by regulators and by the best market practices, with approval from the Executive Board and from the Compliance Department.