



EURASIAN RESOURCES GROUP SARL

ANTI-MONEY LAUNDERING POLICY

Compliance Policies - Policy 2.1- Anti-money Laundering

Originally approved by:	Board of Managers
Origin date:	August 24, 2014
Approved by:	Compliance Committee
Last revised date:	October 26, 2023
Policy owner:	Group Compliance Director
Contact:	Group Compliance Director

This document sets out ERG's Anti-Money Laundering Policy with which the Group, Perimeters, Regions, Group Companies and their Employees must comply. The Perimeters, Regions and Group Companies may implement stricter rules where necessary to comply with local requirements.

In this document, unless otherwise stated, capitalized terms have the meaning ascribed to them in the section 3 (Definitions) below.

1. Policy Objective

- 1.1. The purpose of this Policy is to provide clear rules on how to identify the risk of Money Laundering and/or Terrorist Financing, conduct risk assessments required under applicable regulations, avoid Money Laundering and/or Terrorist Financing within the Group Company's dealings, and/or properly manage a situation which could potentially involve the Group Company in Money Laundering and/or Terrorist Financing in order to maintain compliance with the ERG Code of Conduct, applicable Anti-Money Laundering Laws and other relevant laws and regulations.
- 1.2. This Policy should be read in conjunction with the ERG Code of Conduct, Supplier Code of Conduct, Conflict of Interest Policy, Anti-Bribery and Corruption Policy, Gift and Entertainment Policy, CSR Projects and Sponsorship Policy, Policy on Related Party Contracts, ERG Group Compliance Counterparty Due Diligence Framework ("CPDD Framework"), Compliance Counterparty Due Diligence Procedures of the Perimeters ("Perimeter CPDD Procedures") and other Company's policies and procedures.

2. Scope

- 2.1. This Policy applies to the Employees, Agents and Business Partners in all business dealings and in all jurisdictions in which the Group conducts business.
- 2.2. This Policy sets out the Group's zero-tolerance approach to Money Laundering, Terrorist Financing, and other such financial crimes, and ERG's process and procedures to prevent such crimes.
- 2.3. This Policy includes:
 - 2.3.1. ERG's principles to prevent Money Laundering and Terrorist Financing;
 - 2.3.2. How to identify and report suspicious activities;
 - 2.3.3. The responsibilities of Employees and their managers; and
 - 2.3.4. The consequences for those who do not comply with this Policy.

3. Definitions

Agent – means a third party (natural person or a company) authorised to negotiate, represent or act on behalf of the Group Company on strategic matters, including but not limited to negotiating with government agencies, customs and clearing agents and lobbyists. It does not include bona fide professional advice or services rendered to the Group Company in the ordinary course of business where the Agent has no ability to bind the Group Company or negotiate or speak for the Group Company.

AML/CFT – means Anti-Money Laundering / Combating the Financing of Terrorism.

Anti-Money Laundering Laws – means laws enacted by local authorities or supra-national organisations, however called, which deal with Money Laundering and Terrorist Financing.

Board of Managers – means the Board of Managers of Eurasian Resources Group S.à r.l.

Business Partner – means an individual or body incorporated/unincorporated with which Group Company does business or which performs services for or on behalf of Group Company, excluding Agents.

Company or ERG – means Eurasian Resources Group S. à r.l.

Compliance Committee – means the compliance committee of the Board of Managers.

Employee – means any employee, including but not limited to interns and part-time employees, director, executive or any other officer of any Group Company.

Group – means all Group Companies together.

Group Company – means ERG or its direct or indirect subsidiary in relation to which ERG exercises control.

Local Laws – means relevant local laws regarding Money Laundering and Terrorist Financing.

Money Laundering – means the process through which proceeds of crime, and their true origin and ownership, are changed so they appear legitimate and can then be retained permanently or recycled into further criminal enterprises. It is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts.

Perimeter – means an aggregate of several Regions and/or countries, in which the Group operates, including the international perimeter and the Kazakhstan perimeter.

Policy – means the present document titled “Anti-money Laundering Policy”.

Politically Exposed Person (PEP) – means an individual who is entrusted with Prominent Public Functions, other than as a middle-ranking or more junior official, and includes:

a “family member” of the PEP:

- a spouse or civil partner of the PEP;
- children of the PEP and the spouses or civil partners of the PEP’s children;
- parents of the PEP; and

a “known close associate” of the PEP:

- an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with the PEP;
- an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of the PEP.

Regions – means the regions in which the Group operates, including Africa, Brazil, Kazakhstan region and other regions.

Terrorist Financing – means the provision or collection of funds from legitimate or illegitimate sources with the intention or in the knowledge that they may be used to carry out any act of terrorism, whether or not those funds are in fact used for that purpose.

Tipping off – means the conduct of informing or letting know – intentionally or not – a third party about their suspicious activity being investigated and/or reported to a regulating authority.

4. Policy Principles

- 4.1. The Group does not engage in transactions which it knows, or suspects, involve Money Laundering or Terrorist Financing. It is also contrary to the Group's principles and policies for any Group Company, Employee, Agent or Business Partner to engage in any transaction which they know or suspect that involves Money Laundering or Terrorist Financing.
- 4.2. The Group adopts a risk-based approach in identifying and assessing areas in which it has higher level of exposure in relation to Money Laundering and Terrorist Financing in the conduct of its business activities.
- 4.3. The Group has in place policies, controls and procedures to mitigate Money Laundering and Terrorist Financing risks to which it is exposed in the conduct of its business activities.
- 4.4. Ongoing monitoring and assessments of risk areas are undertaken by the Group to ensure its policies, controls and procedures are adequate and sufficient to prevent Money Laundering and Terrorist Financing occurring in the conduct of the Group's business activities.
- 4.5. All Employees, Group Companies, Agents and Business Partners must observe and comply with the Company's controls, policies and procedures in the conduct of business.
- 4.6. Management of each Region and/or Group Company must ensure that the Group Companies, Employees, Agents and Business Partners under their management comply with the Group's controls, policies and procedures, and with the Local Laws.

5. Identifying Money Laundering and/or Terrorist Financing

- 5.1. The process of Money Laundering and/or Terrorist Financing involves 3 main stages:
 - 5.1.1. Placement – first, the funds originated from illegal and/or criminal proceeds are placed in the financial system;
 - 5.1.2. Layering/staging – once the money is placed, there will be a series of activities which will serve to distance the funds from its source; and
 - 5.1.3. Integration – in the third stage, the funds will be reintegrated to the economy through legitimate transactions.
- 5.2. Each of these stages do not necessarily happen subsequently, therefore an AML/CTF risk assessment must consider a combination of actions, conducts and patterns which could raise a suspicion or indication of Money Laundering and/or Terrorist Financing.
- 5.3. Whilst it is not possible to identify all scenarios and factors that might pose Money Laundering and/or Terrorist Financing risks, the following list is an indication of factors that might be considered suspicious:
 - 5.3.1. Secrecy in relation to a counterparty and/or transaction;
 - 5.3.2. Overly complicated transaction structures;

- 5.3.3. Requests for payments of substantial sums in cash or large cash deposits;
 - 5.3.4. Over-payment of invoices and subsequent requests for refunds;
 - 5.3.5. Movement of funds overseas, particularly in high-risk countries or tax heavens;
 - 5.3.6. Overly complicated financial and/or corporate structures;
 - 5.3.7. Poor business records or internal accounting controls;
 - 5.3.8. Transactions involving Politically Exposed Persons suspected of involvements with cases of bribery, corruption, fraud, embezzlement and other types of misuse of public resources;
 - 5.3.9. Requests for payments in jurisdictions other than that of the counterparty;
 - 5.3.10. Entities related to businesses such as multilevel marketing, pyramid businesses, gambling and other similar activities; and
 - 5.3.11. Apparent absence of transactions or activities by the counterparty or of assets owned by it, which would be expected in the respective business.
- 5.4. In order to mitigate these risks, the following must be observed by all Employees:
- 5.4.1. Counterparty due diligence and identity checks must be properly performed, documented and recorded, as set out in the CPDD Framework and Perimeter CPDD Procedures on third parties with whom the Group Company wishes to engage, including but not limited to, customers, suppliers, Agents and Business Partners;
 - 5.4.2. Reporting of any known or suspected of Money Laundering and/or Terrorist Financing, as set out in the section 6 below; and
 - 5.4.3. Transactions should be carried out by bank transfer and Group Companies should, insofar as possible, not accept or pay cash for any goods or services other than de minimis amounts or where banking facilities are not easily accessible. Any cash transactions should be properly in accordance with petty cash procedures, documented and reviewed periodically by the Head of Compliance of the Perimeter and/or Region.
- 5.5. It is the responsibility of the Group Compliance Director to define minimum requirements for such due diligence and screening procedures.

6. Reporting knowledge or suspicions of Money Laundering and/or Terrorist Financing

- 6.1. In jurisdictions where Group Companies are subject to regulation under Local Laws, the Group Compliance Director, the Head of Compliance of the Perimeter or Region and the Head of Region and/or Head of Group Company shall ensure the appointment of an appropriately qualified and sufficiently senior Employee to any AML/Compliance officer positions required under Local Laws and ensure that the Employees are appropriately trained and resourced to ensure compliance with this Policy and Local Laws including, without limitation, the development and implementation of any specific AML/CTF policies and/or procedures required under Local Laws.
- 6.2. Any knowledge or suspicion of Money Laundering and/or Terrorist Financing must be immediately reported to the Group Company's respective representative of the Legal Department ("Legal Counsel") and/or Head of Compliance of the Perimeter or Region/AML Officer and all affected contracts and payments must be immediately suspended.
- 6.3. Upon notification of a suspicious transaction, the Legal Counsel and/or Head of Compliance of the Perimeter or Region/AML Officer must conduct a full investigation and assessment of the suspicious

transaction and advise whether the Group Company can proceed with the transaction. Such investigations must include an assessment of the risks posed by the counterparty and in conducting the transaction.

- 6.4. In jurisdictions where Group Companies are subject to applicable Local Laws which set out specific requirements in relation to investigation, reporting and confidentiality of reporting, the relevant Local Laws shall be complied with.
- 6.5. When required by Local Laws, the Legal Counsel and/or Head of Compliance of the Perimeter or Region/AML Officer shall disclose the suspicious transaction to the relevant authorities.
- 6.6. In case it is decided that the transaction should be reported to the authorities, care should be taken around the confidentiality of the reporting process for suspicious transactions as, in some jurisdictions, Group Company may be liable for offences associated with prejudicing a Money Laundering and/or Terrorism Financing investigation if the subject of the suspicion is made aware of the disclosure or any associated investigation.¹
- 6.7. The Legal Counsel and/or Head of Compliance of the Perimeter or Region/AML Officer shall keep accurate records of all reported suspicious transactions and disclosures made to the relevant authorities.
- 6.8. If any concerns are raised and/or if civil or criminal law action is taken by any governmental, supra-national or regulatory authorities or any other third parties with regard to Money Laundering or Terrorist Financing in relation to the conduct of business by the Group, the Group Chief Legal Officer and Group Compliance Director must be advised immediately.

7. Responsibilities

- 7.1. The Board of Managers and the Compliance Committee are responsible for establishing this Policy.
- 7.2. The Compliance Committee is responsible for oversight of compliance with this Policy.
- 7.3. The Group Chief Executive Officer, supported by the Group Compliance Director, has responsibility for implementing this Policy in accordance with the requirements of the Board of Managers and/or Compliance Committee.
- 7.4. The Heads of Regions and Heads of Group Companies are responsible for the effective implementation of this Policy in their respective areas of responsibility and for establishing appropriate responsibilities, procedures, training and internal controls within their respective operations to ensure the consistent implementation of this Policy across all jurisdictions and compliance with its requirements.
- 7.5. It is the responsibility of each Head of Region and Head of Group Company to ensure that their respective Employees and all Agents and Business Partners are made aware of this Policy, and that Money Laundering and Terrorist Financing risks are properly assessed.
- 7.6. It is the responsibility of each Employee, Agent and Business Partner to comply with the terms of this Policy.

¹ According to the Financial Action Task Force (FATF), common Tipping off actions include:

- i. changing the way the company handles the counterparty;
- ii. informing other people not related to the investigation of the suspicions;
- iii. directly alerting them of a suspicion: <https://aml-cft.net/library/tipping-off/>

8. Non-compliance

- 8.1. Compliance with this Policy is mandatory to all Employees, Agents and Business Partners. Any non-compliance with this Policy must be documented and reported to the Compliance Committee.
- 8.2. Any Employee, Agent or Business Partner found to have violated this Policy may be subject to disciplinary action, and/or termination of employment or business relationship, as appropriate, as well as any administrative, civil or criminal liability under any applicable laws.
- 8.3. If any Employee, Agent or Business Partner is concerned that this Policy has been or may be contravened, they must report such concerns as soon as reasonably practicable to their line manager, HR, Legal, Compliance or ERG Hotline (Website – <https://erg.integrityline.org> or email to compliance@erg.net). For more information on how to report a concern, please see the phone numbers available on <https://erg.integrityline.org>.

9. Training

- 9.1. All Employees will receive training or awareness on this Policy and the ERG Code of Conduct, which include the main principles and requirements which must be observed in order to prevent Money Laundering and Terrorism Financing and other related compliance policies in accordance with a risk-based training programme.
- 9.2. New joiners will receive training as part of the induction process.
- 9.3. It is mandatory for all Employees to undergo such training when provided by the Group.
- 9.4. Existing Agents and Business Partners will also receive training on this Policy, Supplier Code of Conduct and other related policies in accordance with a risk-based training programme. New Agents and Business Partners will receive training as part of their onboarding process.
- 9.5. The Group Compliance Director will coordinate Group-wide training. However, it is the responsibility of the Head of Region and Head of Group Company to ensure that Employees working in high risk areas undergo such training on a timely and regular basis.

10. Monitoring and Audit

- 10.1. The Group Compliance Director shall periodically, but not less than annually, report on the status of compliance with this Policy to the Compliance Committee.
- 10.2. The Group shall arrange for periodical independent review of compliance with this Policy and report any deficiencies and respective recommendations to the Group management and the Compliance Committee.

11. Revision Process

- 11.1. This Policy shall be reviewed periodically (but not less than once every 2 years) and updated where needed to reflect any changes in the relevant law and/or business requirements.
- 11.2. All requests for amendments to this Policy shall be directed to the Policy owner.
- 11.3. Amendments to this Policy must be made in accordance with the internal documents of the Company.

12. Document Version Control

Version	Approved by	Date of approval	Comments
1.0	Board of Managers	24.09.2014	
2.0	Compliance Committee	26.10.2023	