ANTI-MONEY LAUNDERING POLICY

Compliance Policies - Policy 2.1- Anti-money laundering

Approved by	The Board of Managers
Origin Date:	August 24, 2014
Last Revised Date:	May 5, 2015
Policy owner(s):	Acting Group Head of Compliance
Contact(s):	CPDD Manager

In this document, the "Company" or "ERG" means Eurasian Resources Group S.a.r.l. and includes, where applicable, all subsidiaries.

1. Policy Objective

1.1. The policy's objectives are:
1.1.1. to protect Company reputation by ensuring that the Company business or assets are not used for money-laundering or terrorism financing;
1.1.2. to provide Company employees with clear requirements and universal guidelines on prohibition of transactions involving money-laundering or terrorism financing. The policy, however, is not intended to list all applicable legal requirements.

1.2. The policy sets out:
1.2.1. the Company position on prohibition of transactions involving moneys-laundering and terrorism financing;
1.2.2. roles and responsibilities in ensuring compliance with applicable local Anti-Money Laundering, Proceeds of Crime or Terrorism Financing laws and regulations as well as with this Policy.

2. Scope

2.1. This policy applies to:
2.1.1. the Company, its business and agents;
2.1.2. all employees (including temporary or contract staff and their relatives); and
2.1.3. all business dealings in all jurisdictions within which the Company conducts business.

3. Definitions

3.1. The Board – the Board of Managers of Eurasian Resources Group SARL.
3.2. Money laundering - the process of transformation of proceeds of crime into legitimate money or other assets.
3.3. Terrorism financing - providing funds or other assets to terrorist organisations, which are identified as such by relevant government authorities or supra-national bodies under applicable laws.
3.4. Anti-Money Laundering Laws - laws enacted by local authorities or supra-national organisations, however called, which deal with money laundering and terrorism financing.

4. Policy Statements

4.1. The Company does not knowingly engage in transactions involving money laundering or terrorism financing.
4.2. It is contrary to the Company's policy for any business unit, employee or agent acting on behalf of the Company to knowingly engage in any transaction involving money laundering or terrorism financing.
4.3. Business Unit management must ensure that the entities and staff under their management comply with relevant local laws regarding money laundering or terrorism financing.
4.4. If any concerns or claims are raised by any governmental, supra-national or regulatory authorities or any other third parties with regard to money laundering or terrorism financing in relation to the conduct of business by the Company, the Group General Counsel must be advised immediately.
4.5. If the Company employee has concerns around activities of other Company employees or a third party, which could breach this Policy, they are encouraged to report such concerns to their general

counsel or compliance officer or to Company management as per the Whistleblowing and Investigations Policy.

4.6. Failure by a member of staff to comply with this policy may lead to disciplinary action being taken against them, which may include termination of employment. Also, depending on the jurisdiction, anyone who becomes involved with an activity which they know, or have reasonable ground to suspect, is related to the proceeds of crime may be guilty of money laundering and be subject to criminal prosecution.

4.7. In order to identify third-party risks, due diligence should be performed on all third parties the Company is going to deal with including, but not limited to customers, suppliers and agents.

4.8. The Group General Counsel should define minimum requirements for such due diligence and screening procedures

4.9. Any suspicions of money-laundering or terrorism financing should be immediately reported to respective legal counsel or compliance officer and no contract or payment can be made until clearance is received from the legal or compliance officer. Upon assessment legal counsel or compliance officer should advise whether the transaction should be conducted or not.

4.10. Special care should be taken around confidentiality of reporting on suspicious transactions as some jurisdictions may provide for “tipping-off” offences if any potential investigation into suspicious activity is prejudiced.

4.11. Upon notification of a suspicious transaction a legal or compliance officer should assess the risks of dealing with a counterparty and conducting of the transaction and, if required by local law, a disclosure should be made to relevant authorities.

4.12. Business Units should generally not accept or pay cash. Any transactions should be carried out by bank transfer.

4.13. Employees should seek immediate legal advice in the event of any concerns or doubts regarding money laundering or terrorism financing.

4.14. All employees should be given trainings on Code of Business Conduct, which include main principles of anti-money laundering requirements. It is employee responsibility to undergo such training when provided by the Company

4.15. Group General Counsel should coordinate such Group-wide trainings, however it is the responsibility of each Business Unit Head to ensure that staff likely to be dealing in the key areas of concern undergo such trainings on a timely and regular basis.

5. Responsibilities

5.1. The Board is responsible for establishing this Policy.

5.2. The Compliance Committee of the Board is responsible for oversight of compliance with this Policy.

5.3. The Group Chief Executive, supported by the Group General Counsel, has responsibility for implementing this policy in accordance with the requirements of the Board.

5.4. The Business Unit Heads are responsible 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.

5.5. It is the responsibility of each Business Unit Head to ensure that their respective employees and all third party service suppliers acting on behalf of the Company are made aware of this policy.

5.6. It is the responsibility of each Company employee to comply with the terms of this policy.

6. Monitoring

6.1. The Group General Counsel should periodically, but not less than quarterly, report on the status of Anti-Money Laundering to the Compliance Committee of the Board.

6.2. The Regional Management is responsible for effective implementation of this Policy in their respective areas of responsibility and should make sure that adequate controls are implemented to ensure on-going compliance.

6.3. Internal Audit should periodically review compliance with this Policy and report any deficiencies and respective recommendations to the Group Management and the Compliance Committee of the Board.