AML POLICY

1 GENERAL TERMS

Money laundering (hereinafter, - ML), Terrorism Financing (hereinafter, - TF), and tax crimes undermine, among others, the stability and integrity of financial systems, the efforts by governments to ensure sustainable development of their economies and their ability to collect adequate public revenues. The EU, its institutions, and its bodies are strongly committed to the fight against ML/TF both within the EU and globally. Since the first AMLD in 1990, the EU has developed a solid and continually evolving regulatory framework for countering and combatting ML/TF.

Kepler Group places great emphasis on integrity and good governance and is committed to the highest standards of AML-CFT.

In fulfilling its public policy mission, Kepler Group applies BBP principles[1], as contemplated in the Kepler Group Statute and the Kepler Group Rules of Procedure. Although the Kepler Group is generally subject to EU Legislative Acts and Guidelines, to the extent determined by the BBP Guiding Principles.

Accordingly, Kepler Group applies as BBP the general principles and standards set out in EU law, notably the AMLD[2] and for interpretation purposes, takes into account international standards such as the FATF recommendations. The Kepler Group hence requires its counterparties (those receiving financial support from the Kepler Group) to comply with applicable laws in the field of AML-CFT.

Against this background, Kepler Group continuously monitors and enhances the effectiveness of its compliance standards and controls. It hence aims to mitigate the risk of misuse of funds from Kepler Group or from other sources for the purpose of activities that are illegal or abusive in relation to applicable laws.

The Kepler Group AML-CFT Policy establishes the key principles governing AMLCFT and related integrity aspects in relevant Kepler Group professional activities. It is applied through respective Kepler Group implementing procedures.

The Kepler Group AML-CFT Policy supersedes the “Kepler Group Anti-Money Laundering and Combating the Financing of Terrorism Framework” and applies when establishing a business relationship, as well as to all new or renewed operations where Kepler Group entities provide professional activities, as detailed in the implementing procedures.

All Persons subject to this Policy are responsible for adhering to the Kepler Group AMLCFT Policy and its implementing procedures, as applicable.

2 SCOPE

2.1 Objectives

The Kepler Group AML-CFT Policy and its implementing procedures establish principles and measures designed to prevent the Kepler Group and Persons subject to this Policy from being used for or connected with ML, TF or other criminal activities[1].

Adherence to the Kepler Group AML-CFT Policy also aims, among others, at preventing Kepler Group from being exposed to reputational damage and financial loss as a result of non-compliance with applicable AML-CFT standards.

2.2 Applicability

This Policy is applicable to the professional activities of Kepler Group entities, as detailed in the applicable implementing procedures.

This Policy shall apply to all Persons subject to this Policy.

The responsibilities of Kepler Group entities' Management Bodies include, setting, approving, and overseeing the implementation of adequate and effective internal governance and internal control frameworks such as this Policy, to ensure compliance with applicable requirements. In the context of countering ML/TF, this also includes setting the risk appetite, monitoring against risk exposures and taking decisions in respect of granting finance and establishing business relationships.

2.3 Definition of Money Laundering

Money laundering[4] is intentionally engaging in:

1) the conversion or transfer of property, or financial assets, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

2) the concealment or disguise of the true nature, source, location, disposition, movement, or rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

3) the acquisition, possession or use of property, or financial assets knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

4) the participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in the foregoing points.

2.4 Definition of Terrorist Financing

Terrorism Financing is the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used, or in the knowledge that they are to be used (in full or in part) to commit or to contribute to the commission of any of the offences referred to in Articles 3 to 10 of Directive (EU) 2017/541 of 15 March 2017 on combatting terrorism.

Where TF concerns any of the offences laid down in articles 3, 4 and 9 of Directive (EU) 2017/541, it shall not be necessary that the funds be in fact used, in full or in part, to commit or to contribute to the commission of any of those offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used.

3 THREE LINES OF DEFENCE FRAMEWORK

The internal management of ML/TF risks and controls of the Kepler Group entities follows the three lines of defense model for addressing and managing risk.

Business lines, as the first line of defense, take risks and are responsible for their operational management directly and on a permanent basis, as detailed in the implementing procedures.

In the AML-CFT context, the Kepler Group compliance functions constitute the second line of defense and perform, among others, risk-based monitoring of the first line of defense controls, set standards and provide guidance, support and counsel on ML/TF risk tolerances. The involvement of the compliance functions shall be commensurate to identified ML/TF risk factors.

Internal Audit represents the third line of defense. It independently reviews the first two lines of defense, assesses the adequacy and effectiveness of AML-CFT controls, and provides assurance to the Kepler Group Boards of Directors on the sound management of AMLCFT risks.

4 RISK MANAGEMENT

4.1 Risk Appetite

Under the Kepler Group Risk Management includes a risk appetite statement incorporating among other limits to the exposure to ML/TF risks, and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the relevant Risk Appetite Framework aspects.

4.2 Compliance Risk Assessment

For the management of ML/TF risks, the conduct Compliance Risk Assessments, as applicable to the Kepler Group. Their standards and principles follow the AMLD and best industry practices with regard to the risk dimensions and factors used to assess the ML/TF risk exposure and are adapted to the nature and size of each entity. These results are also consolidated on a Group level. To this end, the Kepler Group entities may also incorporate input from relevant EU-wide risk assessments.

4.3 Risk-Based Approach

While its entities do not open or manage accounts or accept deposits and are driven by public policy objectives, Kepler Group has adopted this Policy and its implementing procedures with the aim of applying AML-CFT measures to proportionally respond to the AML-CFT risks that it may be exposed to. Kepler Group applies a risk-based approach to AML-CFT when mitigating the ML/TF risk of its professional activities, taking into account, among others, factors such as the type of counterparty (including sector), business relationship, product or transaction and country of operation. The ML/TF risk associated with new products and significant changes applied to existing ones are identified, assessed and approved.

5 REPORTING OBLIGATIONS

Persons subject to this Policy are required to report, in line with the reporting channels set out therein, any alleged misconduct, breaches or any suspicions of ML/TF. Unlawfully informing prospective or existing Kepler Group counterparty(ies) or other third persons, that compliance concerns may be, or have been raised in relation to an operation and/or counterparty, and/or that an investigation has been, is being, or may be, carried out, including its outcome is prohibited (Tipping off). Tipping off a prospective or existing counterparty is a breach of professional duties and may constitute a criminal offence, therefore allegations of Tipping off may trigger the opening of an investigation/inquiry against the person who has tipped off the prospective or existing counterparty, which may result in disciplinary proceedings and sanctions and possible

referral to national authorities for criminal prosecution. Suspicions that funds, regardless of amount, may be the proceeds of criminal activities or related to ML or TF in the professional activities of the Kepler Group , must be reported for assessment and, if appropriate, investigation, to the Inspectorate General. Results of relevant assessments and investigations are shared with the Kepler Group Heads of Compliance in their capacity as
MLROs reporting ML/TF suspicions to the Financial Intelligence Unit (FIU), as appropriate.

5.1 Persons Subject to Reporting Obligations

The Kepler Group has in place a Memoranda of Understanding with respective regulatory authorities. The Heads of Compliance act as designated by the current legal regulations binding in the EU and EEA. In their capacity, the Heads of Compliance or their delegates report suspicions of ML/TF to Regulatory Authorities.

5.2 Inspectorate General

The Inspectorate General assesses, and if appropriate investigate, allegations of prohibited conduct, including ML/TF related to Kepler Group professional activities. It cooperates directly with and reports to the EPPO and OLAF. It may also refer suspected prohibited conduct to other competent authorities per the Kepler Group Anti-Fraud Policies.

6 SANCTIONS COMPLIANCE

The Kepler Group and its subsidiary legal entities are committed to comply with applicable sanctions provisions/regulations relating to its professional activities (EU, UN, and as determined by the Kepler Group , Sanctions Authorities outside the EU) as per the Kepler Group Sanctions Compliance Policy as periodically amended. Any arising financial penalties which may be applicable to the holders of the Accounts in Kepler Group must be forwarded to the Beneficiaries of the relevant Trading Accounts.

7 REVIEW

In respect of international standards and relevant EU Legislative Acts and Guidelines to the extent determined by the BBP Guiding Principles, this document remains in effect unless replaced by an updated version approved by the Kepler Group Boards of Directors. The EIB Head of Compliance maintains the Kepler Group AML-CFT Policy in cooperation with the EIF Head of Compliance and with the Kepler Group services concerned. The Heads of Compliance propose for approval by the

relevant decision-making bodies any appropriate updating, taking into account international standards and relevant EU Legislative Acts and Guidelines to the extent determined by the BBP Guiding Principles.

LEGAL BACKGROUND

[1] The EIF applies Best Market Practice (BMP).

[2] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (5th AMLD) and Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (4th AMLD).

[3] See definition in Art. 3 (4) AMLD.

[4] See definitions in Art. 1 (3) and (4) AMLD.

[5] See definition in Art. 1 (3) AML Directive.

[6] See definition in Art. 1 (5) AMLD, together with Art. 11 of Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.