European Investment Bank Group

Anti-Money Laundering and Combating Financing of Terrorism Framework

(“EIB Group AML-CFT Framework”)
Anti-Money Laundering and Combating Financing of Terrorism Framework

(“EIB Group AML-CFT Framework”)
Contents

1. Introduction ........................................................................................................... 3

2. Scope .................................................................................................................... 3
   2.1. Objectives ........................................................................................................ 3
   2.2. Applicability .................................................................................................... 3
   2.3. Definition of “Money Laundering” .................................................................... 3
   2.4. Definition of “ Financing of Terrorism” .............................................................. 4

3. Counterparty Due Diligence – Risk-Based Approach ........................................ 4
   3.1. Identification and Verification of Identity of Counterparty ............................... 4
   3.2. Identification and Verification of Identity of Beneficial Owner(s) ................. 4
   3.3. Establishment of Purpose of Business Relationship ....................................... 4
   3.4. Ongoing Monitoring ....................................................................................... 4

4. Reporting obligations ....................................................................................... 4

5. Roles and Responsibilities of EIB Group Governing Bodies and Staff .......... 5

6. Sanctions/Restrictive Measures Requirements .............................................. 5

7. Record Retention .......................................................................................... 5

8. Data Protection ............................................................................................... 5

9. Training ............................................................................................................ 6

10. Review ............................................................................................................... 6

Data Protection Statement for EIB Group AML-CFT Requirements under the EIB Group AML-CFT Framework ........................................ 7
1. INTRODUCTION

The European Investment Bank Group (“EIB Group”), consisting of the European Investment Bank (“EIB”) and the European Investment Fund (“EIF”), places great emphasis on integrity and good governance and is committed to the highest standards of anti-money laundering (“AML”) and combating the financing of terrorism (“CFT” and, together with AML, “AML-CFT”) in line with the principles and standards of applicable EU legislation, best banking practices and applicable market standards including, where relevant, other international financial institutions’ standards.

This “EIB Group Anti-Money Laundering and Combating Financing of Terrorism Framework” (“EIB Group AML-CFT Framework”) establishes the key principles regulating AML-CFT and related integrity aspects in EIB Group activities, is complemented by detailed operational procedures implemented by the EIB and EIF for their respective daily operations and should be read in conjunction with the EIB Group Codes of Conduct and other relevant EIB Group policies and guidelines (e.g. Anti-Fraud Policy, EIB Policy Towards Weakly Regulated, Non-Transparent and Uncooperative Jurisdictions, EIF Policy towards Offshore Financial Centres, Whistleblowing Policy), as amended and supplemented from time to time.

Adherence to the EIB Group AML-CFT Framework and its implementing procedures is the shared responsibility of all EIB Group staff and members of governing bodies.²

2. SCOPE

2.1. Objectives

The EIB Group AML-CFT Framework and its implementing procedures are intended to establish principles designed to prevent the EIB Group, its governing bodies, staff and counterparties from being used for, or connected with, Money Laundering, Financing of Terrorism or other criminal activities.³

Adherence to the EIB Group AML-CFT Framework is also aimed at preventing the EIB Group from being exposed to reputational damage or financial loss for non-compliance with applicable AML-CFT standards.

2.2. Applicability

This EIB Group AML-CFT Framework is applicable to EIB Group operations and activities, as detailed in the applicable implementing procedures from time to time in force.

2.3. Definition of “Money Laundering”

“Money Laundering” is:
(i) the conversion or transfer of property, 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 activity to evade the legal consequences of his action;

¹ Art. 12 of the EIB Statute requires compliance with “Best Banking Practices”, which entails complying with the EU’s AML-CFT Directives insofar as they are applicable to EIB Group activities (Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (“Directive 2005/60/EC”), as well as Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of ‘politically exposed person’ and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (“Directive 2006/70/EC”). Art. 18(1) of the EIB Statute requires that EIB funds be “employed as rationally as possible in the interests of the Union”.

² For the purposes of this Framework governing bodies means the EIB Management Committee and the EIF Chief Executive.

³ See definition in Art. 3(5) Directive 2005/60/EC, as amended and supplemented from time to time.
(ii) the concealment or disguise of the true nature, source, location, disposition, movement, 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;
(iii) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
(iv) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.4

2.4. Definition of “Financing of Terrorism”

“Financing of Terrorism” is the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.5

3. COUNTERPARTY DUE DILIGENCE – RISK-BASED APPROACH

The EIB Group applies the following counterparty due diligence measures, as determined on a risk-sensitive basis taking into account the type of counterparty, business relationship, product or transaction and country of operation.6

3.1. Identification and Verification of Identity of Counterparty

The EIB Group identifies and verifies the identity of its counterparties with which it enters into a business relationship.

3.2. Identification and Verification of Identity of Beneficial Owner(s)

Whenever the EIB Group is required to identify a counterparty, it takes reasonable risk-based measures to verify the identity of the beneficial owner(s) i.e. the individual(s):
- who (ultimately) own(s) or control(s) the counterparty or its assets; or
- on whose behalf the transaction is carried out or the business relationship with the EIB Group is established.

3.3. Establishment of Purpose of Business Relationship

The EIB Group takes reasonable measures to duly assess the purpose, economic rationale and overall AML-CFT and related integrity aspects of the business relationship in order to avoid being involved in business relationships structured for the purposes of criminal activities or co-financed through funds of possibly illicit origin.

3.4. Ongoing Monitoring

Ongoing monitoring (including monitoring of transactions) is implemented on a risk-sensitive basis to detect possible Money Laundering, Financing of Terrorism or related integrity risks arising throughout the life of the business relationship.

4. REPORTING OBLIGATIONS

Under the Whistleblowing Policy, the Anti-Fraud Policy and the applicable Codes of Conduct, any member of the EIB Group staff or governing bodies is required to report any suspected incidents of illegal behaviour in the activities of the EIB Group, serious misconduct or serious infringement of the Bank rules, policies or guidelines, or any action that is or could be harmful to the mission or reputation of the EIB Group immediately after becoming aware of the matter.

Suspicions of Money Laundering or Financing of Terrorism in the activities of the EIB Group must be reported for assessment and investigation, as appropriate, to the Fraud Investigations

4 Art. 1(2) Directive 2005/60/EC, as amended and supplemented from time to time.
6 See Directive 2005/60/EC (Art. 8), as amended and supplemented from time to time.
Division of the Inspectorate General, which will work in close cooperation with the Head of the relevant compliance function within the relevant EIB Group entity.

The Whistleblowing Policy and the applicable Codes of Conducts stipulate that the EIB Group must ensure confidential treatment for members of EIB Group staff and governing bodies who make *bona fide* reports of suspicions of Money Laundering and Financing of Terrorism and that such members of staff and governing bodies will enjoy the assistance and protection of the EIB Group.

Informing the counterparty/counterparties or other third parties that a suspicious transaction is being reported or investigated is prohibited ("no tipping off").

5. **ROLES AND RESPONSIBILITIES OF THE EIB GROUP GOVERNING BODIES AND STAFF**

All members of EIB Group staff and governing bodies are under an obligation to implement the principles laid down in this EIB Group AML-CFT Framework in accordance with the operational terms established in the implementing procedures.

EIB Group staff with counterparty-facing transaction execution/monitoring responsibilities are the first line of defence and first-line detectors for (i) identifying suspicions of criminal activities in relation to counterparties or transactions and (ii) reporting them immediately in accordance with Article 4.

6. **SANCTIONS/RESTRICTIVE MEASURES REQUIREMENTS**

The EIB Group takes appropriate measures to avoid funding individuals or entities included in the sanctions lists, economic, financial and trade restrictive measures or arms embargoes published by the European Union and United Nations, as amended and supplemented from time to time.

7. **RECORD RETENTION**

Records must be kept of all transaction data and data obtained for the purpose of identification, as well as of all documents related to AML-CFT. 7

8. **DATA PROTECTION**

Personal data submitted to the EIB Group under the EIB Group AML-CFT Framework and its implementing procedures are processed under the supervision of the Group Chief Compliance Officer ("GCCO") (the data controller) for the sole purpose of EIB AML-CFT, and in accordance with (EC) Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ("Data Protection Regulation").

Data subjects are entitled to access, rectify and block such data ("rights of access"), and may exercise their rights by contacting the EIB Group by email (ccco@eib.org), or telephone (+352 43 79 88 00) (attn.: Group Chief Compliance Officer). Data subjects also have the right of recourse to the European Data Protection Supervisor at any time.

Detailed provisions relating to the application of Data Protection Regulation for AML-CFT purposes are available under Annexe 1.

---

7 A 10-year retention period after the end of the business relationship or operation currently applies and will be reassessed after 2015 in cooperation with the European Data Protection Supervisor.
9. **TRAINING**

Adequate AML-CFT training is provided as appropriate to EIB governing bodies and staff. Such training is specifically provided to staff (including trainees and temporary personnel) responsible for carrying out transactions received or initiated by the EIB Group and/or for initiating and/or establishing business relationships.

10. **REVIEW**

GCCO keeps this EIB Group AML-CFT Framework under review in cooperation with the EIB Group services concerned and proposes for approval by the relevant EIB Group management body any appropriate updating in line with EU legal and regulatory development and best banking practices or applicable market standards, including, where relevant, other international financial institutions' standards.

For this purpose, GCCO regularly consults with peer international financial institutions and EU bodies and closely monitors relevant developments at international level, including by participating in the meetings of standard-setting institutions such as the Financial Action Task Force ("FATF") and the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes.
Annexe 1

DATA PROTECTION STATEMENT FOR EIB GROUP AML-CFT REQUIREMENTS UNDER THE EIB GROUP AML-CFT FRAMEWORK

Dated: 15 July 2014

Personal data submitted to the EIB Group under the EIB Group AML-CFT Framework and its implementing procedures are processed under the supervision of GCCO (the data controller) in accordance with (EC) Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (“Data Protection Regulation”).

The data categories which may be collected by the EIB Group in this context are mainly limited to identification data, data related to criminal activities and/or other miscellaneous business information, and will be collected exclusively for AML-CFT purposes.

Data subjects include the persons who directly or indirectly own as well as persons entrusted with control and management of counterparties (or potential counterparties) of the EIB Group (i.e. beneficial owners, shareholders, chairpersons, chief executive officers, board of directors, management committee, supervisory board, local authorities’ council or equivalent).

Personal data are collected from the data subject directly or via other publicly available sources (“open sources”) such as newspapers, specialised databases operated by the private sector, specialised external service providers or websites, and all reasonable steps are taken to keep such data accurate and up to date. When data are requested for the purpose of AML-CFT, supply by the data subject is mandatory. Failure to provide the requested data may cause the data subject (and if applicable the counterparty linked to such data subject) to delay the operational process of the EIB Group, or as the case may be, to be excluded from entering into a business relationship with the EIB Group.

In accordance with EU Directive 2005/60/EC, controls on the data subject include controls relating to due diligence requirements for counterparties (i.e. identity of the beneficial owner(s), ownership and control structure and purpose of the business relationship), as well as for the assessment relating to the risk-based approach (i.e. where applicable, qualification of the data subject as a “politically exposed person” or possible administrative and criminal records or proceedings in connection with criminal activities).

Such data subjects are entitled to access, rectify and block these data (“rights of access”), and may exercise their rights by contacting the EIB Group by email (occo@eib.org), or telephone (+352 43 79 88 00) (attn.: Group Chief Compliance Officer). Data subjects also have the right of recourse to the European Data Protection Supervisor at any time (edps@edps.europa.eu or +32 2 283 19 00).

Restrictions to such rights of access may be imposed in accordance with the provisions of the Data Protection Regulation (Article 20(1)) and more particularly for the prevention, investigation, detection or prosecution of criminal activities. Such restrictions if applicable are dealt with by GCCO on a case-by-case basis and would only be applicable for as long as necessary. The data subject would, insofar as possible under the Data Protection Regulation, be informed of the reason why his/her right of access is restricted.

8 All terms defined in this statement have the same meaning as terms defined in the EIB Group AML-CFT Framework.
9 Data quality is ensured also by recourse to automated solutions providing up-to-date data automatically selected by market providers. Automated tools have built-in functionalities to avoid confusion linked to e.g. homonymy and transliteration. Data provided by such tools are further screened and cross-checked by EIB Group staff to ensure the adequacy, accuracy and materiality of data in the course of the ongoing monitoring throughout the life of the business relationship, without using profiling techniques.
10 See definition in Art. 2 Directive 2006/70/EC.
Where applicable, the recipients of the data so collected are limited to members of the EIB Group governing bodies, EIB Group internal services, EU institutions and bodies (such as OLAF) as well as, on the basis of a case-by-case analysis, national authorities including Financial Intelligence Units.
Contacts

For general information:

Information Desk
📞 +352 4379-22000
📞 +352 4379-62000
✉️ info@eib.org

European Investment Bank
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg
📞 +352 4379-1
📞 +352 437704
www.eib.org