



Anti-Money Laundering and Combating Financing of Terrorism Framework

12 October 2016



Anti-Money Laundering and Combating Financing of Terrorism Framework

("EIB Group AML-CFT Framework")

Revised version: 12 October 2016

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. On-going Monitoring	4
4. Reporting of Suspicious Circumstances or Transactions	4
5. Sanctions/Restrictive Measures Requirements	5
6. Roles and Responsibilities of EIB Group Governing Bodies and Staff	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 practices¹ 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, and 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 with 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 bodies².

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 activities³.

Adherence to the EIB Group AML-CFT Framework also aims at preventing the EIB Group from being exposed to reputational damage and financial loss in relation to 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 the processing of criminal proceeds to disguise their illegal origin⁴ and is also defined as participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from criminal activities.

¹ Art. 12 of the EIB Statute requires compliance with “**Best Banking Practices**”. The Best Banking Practices require compliance with AML-CFT EU Directives to the extent that these are applicable to EIB Group activities (Directive (EU) 2015/849 of the European Parliament and 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, (“Directive (EU) 2015/849”) and repealing Directive 2005/60/EC of the European Parliament and of the Council (the 3rd AMLD) and Commission 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 (4) Directive (EU) 2015/849, as amended and supplemented from time to time.

⁴ See definition in Art. 1 (3) Directive (EU) 2015/849, as amended and supplemented from time to time.

2.4. Definition of “Financing of Terrorism”

“**Financing of Terrorism**” means 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 terrorist acts.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 the counterparties with which it enters into business relationships on the basis of documents, data or information obtained from reliable independent sources.

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

Whenever the EIB Group is required to identify a counterparty, it takes reasonable 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, intended nature, 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. On-going Monitoring

On-going 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 of Suspicious Circumstances or Transactions

Any member of EIB Group staff or governing bodies who knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activities or related to Financing of Terrorism shall on their own initiative immediately report to the Inspector General and to the Head of the relevant Compliance function within the EIB Group entity, who shall assess the case and inform when appropriate the competent Financial Intelligence Unit (“**FIU**”) or national authorities in accordance with applicable EIB Group procedures. The EIB Group shall take appropriate measures to protect any member of the EIB Group staff or governing bodies who reports suspicions of Money Laundering or Financing of Terrorism from being exposed to threats or hostile action.

⁵ See definition in Art. 1 (5) Directive (EU) 2015/849, as amended and supplemented from time to time.

⁶ See Directive (EU) 2015/849 (Art. 13), as amended and supplemented from time to time.

It is prohibited to inform the counterparty(ies) or other third parties that a suspicious circumstance or transaction is being, will be or has been reported or investigated (“**no-tipping off**”).

5. Sanctions/Restrictive Measures Requirements

The EIB Group takes appropriate measures to avoid funding individuals or entities included in, or subject to, 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.

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

All members of EIB Group staff and governing bodies are under an obligation to implement the principles established 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, operations or transactions and ii) reporting them immediately to the Inspector General and to the Head of the Compliance function responsible for their respective EIB Group entity.

7. Record Retention

Records must be kept of all transaction data and data obtained for the purposes 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**”). The processing of personal data for the purposes of AML-CFT is considered by the 4th AML Directive to be a matter of public interest and as such, the processing is lawful for the purposes of the Data Protection Regulation⁸.

Data subjects are entitled to access, rectify and, for duly justified reasons, block and erase these data (“**Rights of the Data Subject**”), and may exercise their rights by contacting the EIB Group by email (occo@eib.org), or telephone (+352 43 79 88 00) (attention of 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 the Data Protection Regulation for AML-CFT purposes are available in Annex 1.

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

⁸ Article 5 (a): “*processing is necessary for the performance of a task carried out in the public interest (...)*”.

9. Training

Adequate AML-CFT training, including on the processing of personal data, 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

The 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, the GCCO regularly consults with peer international financial institutions and EU bodies and closely monitors relevant developments at international level, including through participation 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.

Data Protection Statement for EIB Group AML-CFT Requirements under the EIB Group AML-CFT Framework⁹

Dated: 12 October 2016

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 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. The processing of personal data for the purpose of AML-CFT is considered by the 4th AML Directive to be a matter of public interest and as such, the processing is lawful for the purposes of the Data Protection Regulation¹⁰.

Data subjects include persons who directly or indirectly own counterparties (or potential counterparties) of the EIB Group, as well as persons entrusted with control and management of such legal entities (e.g. beneficial owners, shareholders, chairpersons, chief executive officers, boards of directors, management committees, supervisory boards, local authority councils 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 date¹¹. When data are requested for the purposes 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 processes 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 Directive (EU) 2015/849, controls on data subjects 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. when applicable, qualification of the data subject as a "politically exposed person"¹² or possible administrative and criminal records or proceedings in connection with criminal activities).

Such data subjects are entitled to access, rectify and, for duly justified reasons, to block and erase these data ("**Rights of the Data Subject**"), and may exercise their rights by contacting the EIB Group by email (occo@eib.org), or telephone (+352 43 79 88 00) (attention of Group Chief Compliance Officer). Data subjects also have the right of recourse to the European Data Protection Supervisor at any time.

⁹ All terms defined in this statement have the same meaning as terms defined in the EIB Group AML-CFT Framework.

¹⁰ Article 5 (a): "*processing is necessary for the performance of a task carried out in the public interest (...)*".

¹¹ Data quality is also ensured 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 on-going monitoring throughout the life of the business relationship, without using profiling techniques.

¹² See definition in Art. 3 (9) Directive (EU) 2015/849 as amended and supplemented from time to time.

Restrictions to such Rights of the Data Subject 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 the GCCO on a case by case basis and will only be applicable for as long as necessary. The data subject, to the extent possible under the Data Protection Regulation, will be informed of the reason why his/her rights are restricted.

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 OLAF¹³) as well as, on the basis of a case by case analysis, national authorities including FIUs.

¹³ European Anti-Fraud Office



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