



European Investment Bank Group  
**Investigation Procedures**



**PROCEDURES FOR THE CONDUCT OF INVESTIGATIONS  
BY THE FRAUD INVESTIGATIONS DIVISION  
OF THE INSPECTORATE GENERAL  
OF THE EIB GROUP  
("Investigation Procedures")**

## CONTENTS

	<b>Page</b>
A) Introduction	3
B) Purpose and Nature of an Investigation	3
C) Receipt and Registration of an Allegation	3
D) Notification to/Involvement of OLAF	4
E) Conduct of the Investigation	
(i) Generally	4
(ii) Sources of Information	5
(iii) Documents	6
(iv) Electronic and Personal Data	6
(v) Information from Interviews	6
F) Obstruction of an Investigation	7
G) Concluding an Investigation and Findings	7
H) Data Protection - Individual rights and information duties	
(i) General principles	8
(ii) Respect of the rights of data subjects	8
(iii) Personal data quality principle	9
(iv) Transfers of personal data outside EIB	9
I) Other Matters	
(i) Status Report	9
(ii) Retention Policy	9
(iii) Allegation of misconduct by IG/IN staff member	9
(iv) Updating the Investigation Procedures	10
 Annex 1: EIB Protocol for conducting computer forensic operations	 11

## A) Introduction

1. This document sets out the “Procedures for the Conduct of Investigations” by the Fraud Investigations Division of the Inspectorate General (IG/IN) of the European Investment Bank Group (EIB)<sup>1</sup>.
2. The Procedures set forth herein:
  - a. Are to be read in conjunction with the “Policy on Preventing and Deterring Prohibited Conduct in European Investment Bank Activities” (Anti-Fraud Policy);
  - b. Apply to all investigations conducted by IG/IN in the EIB and EIB’s activities; and
  - c. Are applicable to the EIF with provision to be made for its separate governance structure.

## B) Purpose and Nature of an Investigation

3. The purpose of an investigation by EIB’s Fraud Investigations Division (IG/IN) is to examine and determine the veracity of allegations or suspicions of Prohibited Conduct affecting EIB activities or alleged misconduct involving members of governing bodies or staff, to report its findings, and make appropriate recommendations.<sup>2</sup>
4. All investigations conducted by IG/IN are administrative in nature.

## C) Receipt and Registration of an Allegation

5. IG/IN accepts reports of suspected corruption, fraud, collusion, coercion, obstruction, money laundering and financing of terrorism (collectively “Prohibited Conduct”<sup>3</sup>) from any source within or outside the EIB, including complaints from anonymous or confidential sources. IG/IN may also open cases of its own volition, for example arising out of press reports of Prohibited Conduct. IG/IN shall respond to all such reports as set forth below.
6. If the complainant is anonymous or insists on anonymity, IG/IN should request that he or she contacts IG/IN again at an agreed date/time in the future to respond to possible further questions based on the results of the initial review.
7. The Head of IG/IN shall promptly record the information in the IG/IN case management system, where possible, including:
  - a. The date of receipt of the information;
  - b. The identity of the complainant, if disclosed;
  - c. A brief summary of the allegation, including the type of wrongdoing or misconduct alleged (e.g. product substitution, bid rigging, etc.) and the parties alleged to be involved;
  - d. The connection to the EIB, if any, including the description and location of the project or operation involved;

<sup>1</sup> The procedures are handled by IG/IN in compliance with and without prejudice to the Board of Governors’ Decision on 27 July 2004 concerning EIB’s cooperation with OLAF.

<sup>2</sup> The Ethics and Compliance Committee is responsible for assessing conflicts of interest of a member of the Management Committee or Board of Directors.

<sup>3</sup> Definition of “Prohibited Conduct” is available in the [EIB’s Anti-Fraud Policy](#).

- e. Any other information that IG/IN considers significant;
  - f. Assign a name and case number to the issue, for tracking purposes; and
  - g. Prepare and assign the investigation file to one or more investigators.
8. If the Head of IG/IN decides that the information is not EIB related or a *de minimis* case, he shall promptly record the decision of Prima Facie Non-Case in the case management system; the number of prima facie non-cases will be included in the IG/IN “Annual Report of Fraud Investigations”.
9. The Head of IG/IN shall make the information regarding the allegation and its evaluation available upon request to appropriate parties, including the President and the Vice President responsible for investigations, the Secretary General, the Audit Committee, OLAF and the external auditors.

#### **D) Notification to and Involvement of OLAF**

10. (i) *With regard to external investigations*: If the Head of IG/IN has grounds to suspect that there is Prohibited Conduct in an EIB financed-project or activity, he shall promptly notify the European Anti-Fraud Office (OLAF) and provide it with the necessary information<sup>4</sup>. IG/IN will continue its administrative investigation pending the decision of OLAF to open an investigation. If OLAF decides to open an investigation, IG/IN will closely cooperate with OLAF investigators appointed to the case. If OLAF decides, for any reason, not to open an investigation, the Head of IG/IN can nevertheless decide to continue the investigation.

(ii) *With regard to internal investigations*: if the Head of IG/IN has grounds to suspect that there is misconduct by an EIB/EIF member of governing bodies or staff, he shall promptly notify OLAF and provide it with the necessary information. If OLAF decides to open an internal investigation, IG/IN will provide OLAF investigators with all assistance they require. This may include access to personal data and electronic data available in Bank systems, preparation of and participation in interviews etc. If OLAF decides, for any reason, not to open an investigation, the Head of IG/IN can nevertheless decide to continue the investigation.

#### **E) Conduct of the Investigation**

##### **(i) Generally**

11. To the extent feasible, IG/IN should contact the complainant to acknowledge receipt of the complaint and to obtain as much other information concerning the allegation as possible, such as:
- a. A complete description of the alleged wrongdoing or misconduct;
  - b. The alleged connection to the EIB’s financing or other activities and an estimate of the funds at risk;
  - c. The names and locations of the persons or entities involved or who may have further information regarding the allegation;
  - d. The dates of the events in question;
  - e. The location and description of any relevant documents, data or records;
  - f. The basis for the complainant’s knowledge/motive;

<sup>4</sup> See Regulations 1074/1999 (Euratom) and 1073/1999 (CE) at: [http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l\\_136/l\\_13619990531en00010007.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/1999/l_136/l_13619990531en00010007.pdf)

- g. Any concerns concerning possible reprisals or personal security; and/or
  - h. Any other relevant information.
12. As soon as possible after registration of the case in the case management system, IG/IN shall seek to confirm that the alleged wrongdoing or misconduct involves an EIB operation (including EIB-financed projects within or outside the EU), or member of governing bodies or staff.
13. As part of the initial desk review of the case, IG/IN will seek to determine whether:
- a. The alleged wrongdoing or misconduct represents a sufficient material risk<sup>5</sup> to the EIB to justify an investigation; and
  - b. An investigation is feasible, based on the age of the events in question, the specificity of the information received, and the availability of necessary records or witnesses and other relevant information.
14. IG/IN will also seek to objectively evaluate the reliability of the complaint. This may involve, among other steps, reference to:
- a. EIB project, financing or other documents and files or data;
  - b. Prior complaints involving the suspected parties received by the EIB or OLAF;
  - c. Background checks of business and media databases; and
  - d. Other relevant sources of information.

## **(ii) Sources of Information**

15. As part of an investigation, IG/IN may:
- a. Review documentation kept by relevant implicated parties such as borrowers, promoters, contractors, subcontractors, consultants, suppliers and third parties, as applicable, according to the provisions of the EIB financing agreement involved and the EIB Guide to Procurement;
  - b. Conduct on-site inspections of any works, structure, facility or other property relevant to an investigation, and record the results photographically or otherwise;
  - c. Interview witnesses and/or the subject(s); and/or
  - d. Consult other parties including those undertaking relevant audits or investigations.
16. In particular, sources of information for an investigation shall include, but not be limited to:
- a. Documents of any type;
  - b. Electronic data;
  - c. Video, audio and photographic data;
  - d. The results of inspections and tests;
  - e. The investigator's observations; and
  - f. Information provided by witnesses (orally or in writing), including the subject of the investigation.
17. IG/IN will not pay a witness for information. It may pay or reimburse reasonable expenses incurred by a witness as the result of his or her cooperation with IG/IN.
18. IG/IN may seek the advice or assistance of other departments inside EIB, and/or may engage outside consultants and subject matter experts to assist it in an investigation.

---

<sup>5</sup> Factors to be considered include the operational, financial and reputational risk to the EIB and its activities.

**(iii) Documents**

19. With regard to documents that may be required as evidence in administrative or other proceedings, IG/IN shall:
- a. Attempt to identify and use the original document or, if the original is not reasonably available, reliable copies;
  - b. Preserve, as far as reasonably practical, all documents in the condition they were received; and
  - c. Be able to identify when and where the document was obtained, by whom and from whom.

**(iv) Electronic and Personal Data**

20. With regard to electronic data, IG/IN shall:
- a. Obtain such data:
    - i. From the most reliable source reasonably available; i.e. the location or facility that maintains the most complete, accurate and current data;
    - ii. In a manner that, as far as reasonably practical, protects its integrity, and which ensures that the data has not been altered, tampered with or corrupted in any manner; and
  - b. Be able to identify when, where and how the data was obtained, by whom and from whom.
21. With the prior written approval of the Director of Personnel and the EIB's Data Protection Officer (DPO), and in accordance with applicable laws, rules, regulations, policies and procedures, IG/IN may access and copy potentially relevant electronic data (including email/data created, copied or received by an EIB member of governing bodies or staff using any part of the EIB's IT system) and personal data in accordance with the protocol for conducting computer forensic operations attached as Annex 1. In doing so, IG/IN will inform the Director of Personnel and the DPO of the reasons why this access is required for the investigation, whilst protecting the identity of sources and persons concerned.

**(v) Information from Interviews**

22. As regards all interviews conducted by IG/IN, both within and outside EIB, including interviews of the subject of an investigation:
- a. Interviews shall be conducted:
    - i. In the language in which the witness and investigator are comfortable, or otherwise with the assistance of an interpreter; and
    - ii. By two investigators, if IG/IN deems appropriate.
  - b. Prior to the start of an interview, the interviewee shall be informed about his/her right to be assisted by a person of his/her choice and that the record of interview may be used in administrative, disciplinary or other (related) proceedings;
  - c. IG/IN shall promptly prepare a written record of the interview;
  - d. IG/IN may, in its discretion, provide a copy of the record of interview for the witness to review and sign, especially in cases where the testimony of the witness is likely to be critical to key issues;
  - e. Members of staff or of the governing bodies suspected of misconduct shall always be provided with a copy of the record of interview to review and sign; and
  - f. Interviews may be recorded electronically, with the knowledge and consent of the witness.



**F) Obstruction of an Investigation**

23. *With regard to internal investigations:* If the investigative findings indicate that a member of staff or of the governing bodies:
- a. Made a knowingly false statement to IG/IN in a complaint or during the course of an investigation;
  - b. Failed to comply with his or her obligation to cooperate in an investigation, as required by the EIB applicable Codes of Conduct and the Anti-Fraud Policy; or
  - c. Otherwise attempted to hinder, impede or obstruct the investigation;

IG/IN shall refer the matter to the President and Director of Personnel for appropriate and proportionate disciplinary action.

24. *With regard to external investigations:* As defined in the EIB Exclusion Procedures, an “obstructive practice” is: (a) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, or (b) acts intended to materially impede the exercise of the EIB’s contractual rights of audit or access to information or the rights that any banking, regulatory or examining authority or other equivalent body of the European Union or of its Member States may have in accordance with any law, regulation or treaty or pursuant to any agreement into which the EIB has entered in order to implement such law, regulation or treaty.

Any individual, organisation, firm or entity engaging in Prohibited Conduct (including an “obstructive practice”) may be subject to exclusion pursuant to the EIB’s Exclusion Procedures.

**G) Concluding an Investigation and Findings**

25. The standard of proof that shall be used by IG/IN to determine whether a complaint or allegation has been substantiated shall be whether the information, taken as a whole, shows that an investigative finding is more probable than not.
26. The findings of an investigation shall be based on:
- a. The most reliable factual information available, and reasonable inferences and conclusions drawn from established facts;
  - b. To the extent feasible, documents, electronic data, or tests and inspection results that have been authenticated as accurate by their authors, recipients, or custodians, or by other persons with direct knowledge of their authenticity;
  - c. To the extent feasible, statements from witnesses who have direct knowledge of the facts and circumstances in issue;
  - d. Information that has been corroborated to the extent possible by other reliable sources, including other witnesses, documents or data; and
  - e. Reasonable and credible exculpatory as well as inculpatory information.
27. Investigative findings may include IG/IN’s:
- a. Comments on the perceived credibility and behaviour of a witness, including the subject of the investigation; and
  - b. Recommendations for the appropriate action to address the issues under investigation or broader policy issues identified in the course of the investigation. EIB’s services shall report to IG/IN on the measures undertaken to implement these recommendations within the time specified.

28. Where the Head of IG/IN determines that an allegation has been substantiated and requires follow-up action, the findings shall be appropriately documented and referred to the relevant authorities within and/or outside the EIB for further action.
29. If, after reasonable investigation, the Head of IG/IN determines that an allegation has not been substantiated, the findings shall be documented in the case management system and the case closed. If during the evaluation or investigation of the allegation, information has come to the attention of IG/IN which is relevant for others inside or outside EIB, the Head of IG/IN may forward this information in full respect of applicable data protection rules.
30. The Head of IG/IN may re-open a case that has been closed if credible new information is received or if it is warranted by other circumstances.

## **H) Data Protection - Individual rights and information duties**

### **(i) General principles**

31. As noted in the Anti-Fraud Policy, the processing of personal data within the framework of these procedures shall be managed in keeping with the principles and rules provided for in the regulations applicable to the Bank<sup>6</sup> and the relevant opinions issued by the European Data Protection Supervisor (EDPS). Any involved persons are entitled to access, rectify and (in certain circumstances) block data related to him/her by contacting the data processing controller.<sup>7</sup> They may also at any time contact the EDPS.<sup>8</sup>

### **(ii) Respect of the rights of data subjects**

32. Any person who is involved in an investigation (as a suspect, witness or other), should be informed of the processing of personal data in an IG/IN investigation procedure in accordance with articles 11 and 12 of Data Protection Regulation (EC) 45/2001 unless the restrictions under Article 20 apply, in which case, IG/IN shall review from time to time whether the restriction is still applicable or whether the data subject shall be notified of the investigation.

### **(iii) Personal data quality principle**

33. IG/IN shall ensure the respect of the data quality principle as per article 4 of Regulation 45/2001, that is personal data must be accurate and, where necessary, kept up to date, as well as adequate, relevant and not excessive in relation to the purposes of the investigation for which they are collected and further processed. In addition, data shall be processed fairly and lawfully only for specified, explicit and legitimate purposes.

34. IG/IN's evaluation of information shall be based on the most reliable factual information available as well as established facts.

### **(iv) Transfers of personal data outside EIB**

<sup>6</sup> In particular Regulation (EC) No45/2001 of the European Parliament and of the Council of 18 December 2000 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 (Official Journal L8/1 of 12 January 2001)

<sup>7</sup> The data processing controller may be contacted at the following address: [investigations@eib.org](mailto:investigations@eib.org)

<sup>8</sup> [www.edps.europa.eu](http://www.edps.europa.eu)

35. Transfers of personal data by IG/IN may occur to its operational partners, whether EU institutions and bodies notably OLAF, Member State authorities, third country authorities, or international organizations, during the course of its operational activities by written instrument, e-mail, orally (by telephone or in person), or by any other means. Any such transfer must be proportionate, taking into account the nature of the data collected and further processed; data should be transferred only if necessary for the legitimate performance of tasks covered by the competence of the recipient. In making such a transfer in the context of a case, standard and appropriate data protection clauses should be used by IG/IN.

## **I) Other Matters**

### **(i) Status Report**

36. IG/IN shall submit a Status Report quarterly for information to the Management Committee, Audit Committee and OLAF.

### **(ii) Retention Policy**

37. All documentation and information for cases shall be kept in a secure and confidential manner by IG/IN and shall be retained for at least five years and up to ten years maximum from the date of closure of the case.
38. As regards allegations where the Head of IG/IN decides not to open a case ("Prima Facie Non Case") or a case closed because the allegations are not substantiated ("unsubstantiated cases"), documentation and information shall be retained for up to five years maximum from the decision not to open a case or the closure of the case.

### **(iii) Allegation of misconduct by an IG/IN staff member**

39. Where necessary, arrangements will be made by the Inspector General on a case-by-case basis to investigate an allegation of misconduct on the part of any staff member of IG/IN.

### **(iv) Updating the Investigation Procedures**

40. As with the Anti-Fraud Policy, these procedures shall be amended and updated as appropriate based on:
- a. Changes to the "Policy on Preventing and Deterring Prohibited Conduct in EIB Activities";
  - b. Experience gained in implementing the procedures;
  - c. The evolution of best practices;
  - d. Any other changes that the EIB judges necessary and appropriate.

## Annex 1: EIB Protocol for Conducting Computer Forensic Operations

### 1. Definition of Computer Forensic Examination

A Computer Forensic Examination is defined as a technological, systematic inspection of electronic equipment and its contents for information, which may be relevant to an ongoing investigation, and may eventually be used as evidence in court proceedings.

### 2. Principles on the use of computer forensic operations

2.1 There are currently no published formal computer forensic procedures agreed at an intergovernmental, international or European level.

2.2 In cases for which OLAF has competence to investigate, EIB will normally rely on OLAF's expertise, experts and equipment. It will follow strictly agreed OLAF procedures. In the exceptional case that OLAF would not have competence to conduct an investigation, or would decide not to investigate, EIB may rely on the assistance of experienced private companies. For those cases, EIB adheres to the following four general ACPO Computer Forensic Principles:

Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. (In addition, the person who gains access to original data held on a computer or storage media should justify the necessity for such access and obtain the approval of EIB's DPO prior to this access to the data).

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

2.3 Furthermore, EIB will follow good practice methods:

- All activity relating to the seizure, access, storage or transfer of digital data must be fully documented, preserved and available for review.
- The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.

### 3. Computer forensic procedures in case OLAF does not intervene

*3.1 Setting of achievable objectives*: Conducting computer forensic operations and examinations is also an extremely labour intensive and resourceful job. Considering that complexity and the scarcity of forensic computing resources, choices needed to make such operations more efficient and more operationally effective, involve the following planning:

1. Be specific about the added value of a forensic operation. Where, how and when can forensic examiners assist this investigation? Is it necessary?
2. Set achievable objectives beforehand. Investigators should accurately outline the scope of the envisaged operation at the preparatory stage. During the operation,

further selective data capturing may be necessary. Live data examination where possible may help target the scope of the operation.

3. Realise objectives set i.e. the operation must be feasible with the resources that are available.
4. Timely achievement of objectives set. Ensure that deadlines are met in time, to avoid jeopardising the whole operation e.g. expiry of the legal time limit.
5. Measure the outcome of a data acquisition or seizure e.g. that relevant material for and against the person was found and reference included in the final case report.

3.2. *Data Protection*: The data subject should be informed in writing that EIB adheres to Regulation (EC) 45/2001 and, as stated in the EIB's Anti-Fraud Policy and Investigation Procedures, EIB takes special care to ensure that all relevant data protection requirements are met in conducting forensic examinations.







## Contacts

For general information:

### Information Desk

☎ +352 4379-22000

☎ +352 4379-62000

✉ [info@eib.org](mailto:info@eib.org)

### European Investment Bank

98-100, boulevard Konrad Adenauer

L-2950 Luxembourg

☎ +352 4379-1

☎ +352 437704

[www.eib.org](http://www.eib.org)