

INVESTIGATION PROCEDURES



European
Investment Bank | Group

INVESTIGATION PROCEDURES

European Investment Bank Group Investigation Procedures

© European Investment Bank, 2025

All rights reserved.

All questions on rights and licensing should be addressed to publications@eib.org.

European Investment Bank
98-100, boulevard Konrad Adenauer
L-2950 Luxembourg

This document sets out the procedures for the conduct of investigations by the Investigations Division of the Inspectorate General of the European Investment Bank.

For further information on the EIB's activities, please consult our website, www.eib.org.
You can also contact our Info Desk, info@eib.org. Get our e-newsletter at www.eib.org/sign-up.

Published by the European Investment Bank.

Printed on FSC® Paper.

CONTENTS

- A. INTRODUCTION 1
- B. PURPOSE AND NATURE OF AN INVESTIGATION 2
- C. RECEIPT AND REGISTRATION OF AN ALLEGATION 3
- D. CONDUCT OF THE INVESTIGATION..... 4
 - D.1 Assessment 4
 - D.2 Investigation 5
 - D.3 Access to information 6
 - D.4 Personal data 6
 - D.5 Information from interviews 7
- E. OBSTRUCTION OF AN INVESTIGATION..... 8
- F. CONCLUDING AN INVESTIGATION AND FINDINGS 9
- G. NOTIFICATION TO AND INVOLVEMENT OF THE EUROPEAN PUBLIC PROSECUTOR’S OFFICE AND THE EUROPEAN ANTI-FRAUD OFFICE 11
- H. DATA PROTECTION – INDIVIDUAL RIGHTS AND INFORMATION DUTIES 12
 - H.1 General principles 12
 - H.2 Respect of the rights of data subjects 12
 - H.3 Personal data quality principle 13
 - H.4 Transfers of personal data outside the EIB Group 13
- I. OTHER MATTERS 14
 - I.1 Status reports 14
 - I.2 Retention policy 14
 - I.3 Allegation of fraud and misconduct by an Investigations Division staff member 14
 - I.4 Applicability and amendments to the Investigation Procedures 14
- ANNEX 1: EIB PROTOCOL FOR CONDUCTING COMPUTER FORENSIC OPERATIONS..... 15
 - Introduction 15
 - Article 1. Definitions 15
 - Article 2. Forensic laboratory of the Investigations Division 17
 - Article 3. Preparation of a digital forensic operation 17
 - Article 4. Conducting a digital forensic operation – general procedures 18
 - Article 5. Collection of data stored on a remote digital device 19
 - Article 6. Examination of data gathered during a digital forensic operation 19
 - Article 7. Final backup of results 20
 - Article 8. Assistance provided to EIB Group partners 20
 - Article 9. Retention period applicable to digital forensic evidence and work files 20

A. INTRODUCTION

1. This document sets out the procedures for the conduct of investigations (Investigation Procedures) by the Investigations Division of the Inspectorate General (Investigations Division) of the European Investment Bank (EIB).¹
2. The Investigation Procedures set forth herein:
 - a. are to be read in conjunction with the EIB Group policy on preventing and deterring Prohibited Conduct in EIB Group activities (EIB Group Anti-Fraud Policy), the EIB Group Fraud Investigations Division Charter ([Investigations Division Charter](#)), the [EIB Group Staff Code of Conduct](#), the [EIB Group Dignity at Work Policy](#) and the [EIB Group Whistleblowing Policy](#), as amended from time to time; and
 - b. apply to all investigations, internal or external,² conducted by the Investigations Division with respect to the EIB Group's activities and operations.
3. All investigative activities shall be carried out in full respect of the relevant provisions of the EU Treaties, the Charter of Fundamental Rights of the European Union, the applicable EU legislation and these Investigation Procedures. They shall be conducted in an independent and thorough manner, in compliance with the principles of legality, proportionality and confidentiality, and respect of presumption of innocence. All such activities shall be fair and impartial, with due regard to the rights of all persons or entities involved.

¹ The procedures are handled by the Investigations Division in compliance with, and without prejudice to, the Board of Governors' Decision of 27 July 2004 concerning the EIB's cooperation with the European Anti-Fraud Office (OLAF).

² For clarification purposes, the investigative principles and activities set forth by these Investigation Procedures apply to both external and internal investigations, unless specifically stated otherwise.

B. PURPOSE AND NATURE OF AN INVESTIGATION

4. The purpose of an investigation by the Investigations Division is to examine and determine the veracity of allegations or suspicions of:
 - a. prohibited conduct affecting EIB Group activities and operations, as defined in the EIB Group Anti-Fraud Policy;
 - b. breaches of the staff regulations or staff rules of the EIB or European Investment Fund (EIF),³ [EIB Group Anti-Fraud Policy](#), EIB Group Staff Code of Conduct⁴ and EIB Group Dignity at Work Policy (the “Underlying Policies”) involving persons under the scope of the Underlying Policies;
 - c. other matters referred to the Investigations Division under the Investigations Division Charter.
5. For the purpose of these Investigation Procedures, the matters described under 4(a) are referred to as “fraud” while the matters described under (b) and (c) above are referred to as “misconduct,” and collectively “fraud and misconduct.”
6. For cases relating to alleged breaches of the EIB Group Dignity at Work Policy, the Investigations Division refers the findings and evidence of its investigation for appropriate follow-up without making a qualification of the established facts, in accordance with the specific provisions therein.
7. For cases involving exclusively alleged breaches of the EIB Group Staff Code of Conduct that are not also covered by the EIB Group Anti-Fraud Policy or the EIB Group Dignity at Work Policy, following investigation, the Investigations Division refers the relevant evidence to the Office of the Group Chief Compliance Officer, or the EIF Chief Compliance Officer if the case involves EIF staff only, without making a qualification of the established facts. The Office of the Group Chief Compliance Officer, or the EIF Chief Compliance Officer, as appropriate, shall follow up accordingly.
8. All investigations conducted by the Investigations Division are administrative in nature. As part of the investigative process, the Investigations Division reports findings and makes appropriate recommendations, in line with the underlying policies.

³ The fact that the Investigations Division may investigate allegations or suspicions of breaches of the EIB and EIF Staff Regulations/EIB and EIF Staff Rules does not mean that any potential breach of the EIB and EIF Staff Regulations/EIB and EIF Staff Rules must be investigated by the Investigations Division. If the facts are already established by other means, a disciplinary procedure may be initiated in case of breach of the EIB and EIF Staff Regulations/EIB and EIF Staff Rules on the basis of a report established by the relevant service as set out under Article 1.1.1 of Annex XI to the Staff Rules and without resorting to an investigation carried out by the Investigations Division.

⁴ Breaches of the relevant governing body Code of Conduct as applicable from time to time will be investigated in accordance also according to the Operating Rules of the Ethics and Compliance Committee.

C. RECEIPT AND REGISTRATION OF AN ALLEGATION

9. Allegations of fraud and misconduct can be referred to the Investigations Division from any source within or outside the EIB Group, including allegations from anonymous or confidential sources. The Investigations Division shall respond to all such reports as set forth below. The Investigations Division may also open cases of its own volition.⁵
10. Whenever the Investigations Division receives an allegation of alleged fraud and misconduct, it will acknowledge receipt of such allegations within five working days and to the extent feasible.⁶
11. After the acknowledgement of receipt, the Investigations Division will, where appropriate and possible, contact the person reporting an allegation of fraud and misconduct to obtain as much additional relevant information concerning the allegation as possible. The Investigations Division will seek to obtain, as appropriate, further information from the anonymous reporting person, while maintaining the anonymity of the reporting person, in compliance with the EIB Group Whistleblowing Policy,⁷ if applicable.
12. The Investigations Division will record allegations of the above forms of fraud and misconduct in the Investigations Division case management system under an assigned case number and title, as described under section D.1 below.

⁵ For example, arising out of press reports of Prohibited Conduct or identified through its proactive detection function or following operational analysis.

⁶ The Investigations Division of the Inspectorate General will acknowledge receipt of reports when the details of the sender are provided and/or known.

⁷ The EIB encourages the reporting of suspected breaches of EIB Group policies through its [whistleblowing platform](#).

D. CONDUCT OF THE INVESTIGATION

D.1 Assessment

13. During the assessment, the Investigations Division will obtain as much preliminary information concerning the allegation as possible. This should include but is not limited to:
 - a. a complete description of the alleged wrongdoing;
 - b. where relevant, any alleged connection to the EIB Group’s financing or other activities and an estimate of the funds at risk, if any;
 - 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. any concerns regarding possible reprisals or personal security; and/or
 - g. any other relevant information.
14. As part of the assessment of the case, the Investigations Division will seek to determine whether:
 - a. the allegation falls within the scope of any of the Underlying Policies and whether the allegation is sufficiently serious or corroborated to warrant the opening of an investigation;
 - b. an investigation is feasible, based on the time of events in question, the level of detail of the information received, the availability of necessary records or witnesses, and other relevant information;
 - c. an investigation is feasible taking into account the need for the efficient use of the Investigations Division’s resources and for the proportionality of the means employed.
15. As part of the assessment, the Investigations Division may conduct research and analysis as it considers appropriate, given the nature of the allegation. This may include but is not limited to: information research in open sources; and a review of internal and external databases, directories and internal information repositories. To undertake the effective assessment of allegations, the Investigations Division shall have complete and unrestricted access to all case-related documents within the EIB Group, as detailed in paragraph 18 below.
16. The Investigations Division will seek to objectively evaluate the reliability of the source, and the credibility and veracity of the information provided.
17. All information received concerning allegations that are not EIB Group-related shall be deemed “prima facie non-case,” and shall be closed at the assessment stage with the approval of the head of the Investigations Division. All information received concerning allegations that are EIB Group-related shall be the subject of an assessment. If an investigation is not warranted, the matter shall be closed at the assessment stage with the approval of the head of the Investigations Division.
18. The head of the Investigations Division, after consideration of all relevant information, takes the decision on the opening of an investigation. Such investigations are governed by section D.2 below.

19. The head of the Investigations Division shall make available information regarding the allegation and its assessment upon request to appropriate parties, including the president, the EIF chief executive, the EIB and EIF secretaries general, the EIB Audit Committee, the EIF Audit Board, the EIB and EIF heads of Human Resources, the Group chief compliance officer and EIF chief compliance officer, the European Public Prosecutor's Office,⁸ the European Anti-Fraud Office⁹ and the external auditors. The head of the Investigations Division may also communicate such information to its operational partners, such as the European Union Agency for Law Enforcement Cooperation (Europol) and national authorities.

D.2 Investigation

20. In order to gather evidence as part of an investigation, the Investigations Division may:
- a. access all EIB Group premises and all archives, systems and repositories;
 - b. review and copy any relevant EIB Group documentation;
 - c. review and copy documentation kept by relevant parties such as borrowers, promoters, financial intermediaries, or other primary counterparties benefiting from a financing, guarantee or investment operation from the EIB Group, contractors, subcontractors, consultants, suppliers, beneficiaries (as the case may be), tenderers, and in general any relevant persons or entities involved in EIB Group-financed activities (referred to herein as "Operations-Related Parties"), according to the provisions of the EIB Group financing agreement involved and the EIB Guide to Procurement;
 - d. conduct inspections of any EIB Group premises and record the results photographically or otherwise;
 - e. collect relevant information in the framework of operational meetings or by requesting written comments;
 - f. conduct on-site inspections of any EIB Group projects or activity-related works, structure, facility or other property relevant to an investigation, according to the provisions of the related financing agreement, and record the results photographically or otherwise;
 - g. carry out digital forensic operations, in accordance with the EIB Protocol for Conducting Computer Forensic Operations (Annex 1);
 - h. carry out fact-finding missions as necessary and required;
 - i. interview persons reporting allegations of fraud and misconduct, witnesses and/or the subject(s) of the investigation as deemed necessary;
 - j. consult other parties including those undertaking relevant audits or investigations; and/or perform any other investigation activity deemed necessary.
21. The Investigations Division will not pay a witness for information. It may pay or reimburse reasonable and approved expenses incurred by a witness as the result of his or her cooperation with it.
22. The Investigations Division may seek the advice or assistance of other departments inside the EIB Group, and/or may engage outside consultants and subject matter experts to assist in an investigation.
23. With regard to documents and digital files that may be required as evidence in administrative or other proceedings, the Investigations Division shall:

⁸ The European Public Prosecutor's Office is responsible for investigating, prosecuting and bringing to judgment before the competent national courts of the participating Member States crimes against the financial interests of the European Union, in accordance with Regulation (EU) 2017/1939 of 12 October 2017. For more information, please consult: <https://www.eppo.europa.eu/>.

⁹ The European Anti-Fraud Office carries out administrative investigations for the purpose of protecting the financial interests of the European Union, and may issue disciplinary, administrative, financial and judicial recommendations for action to be taken by EU institutions, bodies, offices and agencies, and by the competent authorities of the Member States concerned, in accordance with Commission Decision of 28 April 1999 and Regulation (EU, Euratom) No 883/2013, as amended. For more information, please consult: https://ec.europa.eu/anti-fraud/home_en.

- 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 and digital files in the condition they were received; and
- c. be able to determine when and where the document or digital file was obtained, by whom and from whom.

D.3 Access to information

24. In the context of its investigative activities, the Investigations Division shall have full access to all relevant information, documents and personal data, including electronic data, within the EIB Group, in accordance with the applicable procedures including, whenever relevant, procedures on data protection and the EIB and, respectively, the EIF data protection officer's involvement, described below in paragraph 25.
25. In the context of investigations related to EIB Group projects and operations, the Investigations Division shall have the right to copy and examine the relevant books and records, including electronic data, of the relevant Operations-Related Parties or other counterparties and partners, as appropriate.¹⁰

D.4 Personal data

26. With regard to personal data, the Investigations Division shall:
 - a. Obtain such data:
 - i. from the most reliable source reasonably available, meaning the location or facility that maintains the most complete, accurate and current data;
 - ii. in a manner which, 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;
 - b. be able to identify when, where and how the data were obtained, by whom and from whom.
27. With regard to electronic communications, the Investigations Division will access potentially relevant personal data also when they are stored and processed in a digitalised form (including email/files/data created, copied or received by a member of EIB Group governing bodies or staff using any part of the EIB Group's IT system), subject to a necessity and proportionality assessment on processing such data conducted by the Investigations Division in consultation with the EIB data protection officer for EIB matters and the EIF data protection officer for EIF matters, and with the written approval of the EIB director general of Human Resources for EIB matters and the EIF chief executive for EIF matters.

¹⁰ As defined in Section 4 of the EIB Group Anti-Fraud Policy.

D.5 Information from interviews

28. Regarding all interviews conducted by the Investigations Division, both within and outside the EIB Group, including interviews of the subject of an investigation:
- a. Interviews shall be conducted:
 - i. in the language in which the interviewee and investigators are comfortable, or otherwise with the assistance of an interpreter; and
 - ii. by at least two investigators.
 - b. Prior to the start of an interview, the interviewee shall be informed about his/her status (person reporting allegations of fraud and misconduct, witness or subject of the investigation), his/her right to be assisted by a person of his/her choice,¹¹ his/her duty to cooperate, and that the record of interview may be used in administrative, disciplinary or any other (related) proceedings.
 - c. Prior to the start of an interview, the subject of the investigation shall be informed, in general terms, of the allegation with respect to which the interview is taking place and of his/her rights and obligations during the interview, along with the right not to incriminate him/herself.
 - d. Prior to the start of an interview, a witness shall be informed, in general terms, of the reason for the interview and of his/her rights and obligations.
 - e. If during the course of an interview it becomes apparent that a witness is in fact a subject of the investigation, the interview shall be ended. The interviewee shall be informed that he/she will be treated as a subject and informed of his/her rights and obligations.
 - f. The Investigations Division may provide a copy of the record of interview for review and signature by the interviewee, especially in cases where the testimony of the witness is likely to be critical to key issues.
 - g. Subjects of the investigation suspected of fraud and misconduct shall always be provided with either:
 - i. an electronic copy of the interview recording; or
 - ii. a written/typed copy of the record of interview for review and signature.
 - h. Interviews may be recorded electronically only with the knowledge of the interviewee. In the interests of efficiency and proportionality, the Investigations Division may decide to conduct an interview by video conference, if appropriate.

¹¹ The interviewee cannot be assisted by another person who is also a witness or who is a subject in the same investigation.

E. OBSTRUCTION OF AN INVESTIGATION

29. With regard to internal investigations, obstruction of an investigation by an EIB Group member of staff or governing bodies failing to comply with his/her duties and obligations under the relevant policies of the EIB Group, including by knowingly making false statements and allegations or by any attempt to hinder or impede the investigation, amounts to misconduct and will be referred for potential disciplinary action, in accordance with the applicable rules at the EIB Group.
30. With regard to external investigations, any individual, organisation, firm or entity found to have engaged in Prohibited Conduct under the form of an obstructive practice, as defined in the EIB Group Anti-Fraud Policy, will be subject to available remedies under the same policy and may be excluded from participating in EIB and EIF operations and activities in accordance with the provisions and process set out in the EIB Exclusion Policy.

F. CONCLUDING AN INVESTIGATION AND FINDINGS

31. For investigation of cases under the scope of this procedure, the standard of proof that shall be used by the Investigations Division to determine whether a report/allegation has been substantiated shall be whether the information, taken as a whole, shows that an investigative finding of an alleged instance of fraud and misconduct is more probable than not.
32. Once the investigation activities have been completed and prior to drawing conclusions referring to the subject of the investigation, the Investigations Division shall inform the respective subject of the relevant facts concerning her/him and invite her/him to comment on those facts. These comments may be provided in the context of an interview or in writing.
33. As soon as the investigation is finalised or the Investigations Division refers the findings to other competent services of the EIB Group or to the competent national authorities or relevant EU institutions, offices, bodies and agencies and international organisations, the Investigations Division may inform the person reporting allegations of fraud and misconduct and the subject of the investigation about the outcome of its investigation, in compliance with its confidentiality obligations. Such information may be provided whenever possible and if deemed appropriate.¹²
34. For cases where findings were referred to other services within the EIB Group for further action, the respective services shall also notify the Investigations Division of the outcome of the respective case.
35. Investigation reports 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, digital 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;
 - d. information that has been corroborated to the extent possible by other reliable sources, including other witnesses, documents, or data;
 - e. reasonable and credible inculpatory as well as exculpatory information.
36. Investigation reports may include the Investigations Division's:
 - a. opinions on the perceived credibility and behaviour of the witness(es) and the subject(s) 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. The relevant EIB Group services shall report to the Investigations Division on the measures undertaken to implement these recommendations within the established deadline.
37. Where the head of the Investigations Division determines that an allegation of fraud and misconduct requires follow-up action, the findings shall be appropriately documented and referred to the relevant office or authority within and/or outside the EIB Group for further action.

¹² In the context of whistleblower reports, in line with the EIB Group Whistleblowing Policy, the whistleblower may request and be provided with feedback about the follow-up to the report.

38. If, after an investigation, the head of the Investigations Division determines that an allegation of fraud is not substantiated, the findings shall be documented and the case closed. At the conclusion of an investigation of allegations of misconduct, the findings are referred to the relevant EIB services for their appropriate action.
39. If during the assessment or investigation of the allegation, information has come to the attention of the Investigations Division which is relevant for other EIB Group services or within the mandate of external prosecution, investigation or anti-corruption offices, the head of the Investigations Division may refer this information in full respect of applicable data protection rules.
40. After a case is closed and new information is submitted to the Investigations Division, a new assessment in the meaning of section D.1 above will be opened to determine whether an investigation is appropriate and/or necessary.

G. NOTIFICATION TO AND INVOLVEMENT OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE AND THE EUROPEAN ANTI-FRAUD OFFICE

41. The Investigations Division shall refer cases for criminal investigation to the European Public Prosecutor's Office and shall assist and support its investigations and prosecutions, in accordance with the working arrangement between the European Public Prosecutor's Office, and the EIB and the EIF,¹³ and in accordance with Article 24(1) of the European Public Prosecutor's Office Regulation.¹⁴
42. The referral of cases to the European Anti-Fraud Office and their further coordination shall be made in accordance with the administrative arrangement between the European Anti-Fraud Office and the EIB and the EIF,¹⁵ and in accordance with Article 8(2) of the European Anti-Fraud Office Regulation.¹⁶ Where the Investigations Division refers a case to the European Public Prosecutor's Office as referred to in point 38, the copy of the report to the European Public Prosecutor's Office is provided to the European Anti-Fraud Office.

¹³ [working-arrangement-eppo-eib-eif-7-december-2021.pdf](#).

¹⁴ [Council Regulation \(EU\) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office \(europa.eu\)](#).

¹⁵ The detailed framework for cooperation between the Investigations Division and the European Anti-Fraud Office is set out in the administrative arrangement between the European Anti-Fraud Office, the EIB and the EIF, dated 31 March 2016.

¹⁶ [Regulation \(EU, Euratom\) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office and repealing Regulation \(EC\) No 1073/1999 of the European Parliament and of the Council and Council Regulation \(Euratom\) No 1074/1999 \(europa.eu\)](#).

H. DATA PROTECTION – INDIVIDUAL RIGHTS AND INFORMATION DUTIES

H.1 General principles

43. Within the framework of assessments and investigations, the Investigations Division will process personal data in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Official Journal L295/39 of 21 November 2018) as amended, supplemented or substituted from time to time (referred to herein as the Data Protection Regulation (EU) 2018/1725).
44. For the protection of personal data, a number of technical and organisational measures have been put in place. Investigations Division premises are part of a secured physical area only accessible to Investigations Division staff and specifically authorised persons in order to prevent any unauthorised access to equipment and data. The IT systems used by the Investigations Division are subject to the relevant information security policies of the EIB Group, which include measures to protect the EIB Group IT infrastructure and systems.
45. 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 EIB Group¹⁷ and the relevant opinions issued by the European Data Protection Supervisor. Any natural persons involved in an investigation are entitled to access, rectify and (in certain circumstances) erase or restrict the processing of their personal data by contacting the data processing controller.¹⁸ They may also at any time contact the European Data Protection Supervisor.¹⁹

H.2 Respect of the rights of data subjects

46. Any natural person who is involved in an investigation shall be informed of the processing of personal data in an Investigations Division investigation procedure in accordance with Articles 15 and 16 of the Data Protection Regulation (EU) 2018/1725. Exceptions and restrictions may apply under Article 25 of that regulation and in accordance with the EIB internal rules concerning the processing of personal data approved by the EIB Board of Directors^{20 21} and respectively the EIF decision on internal rules concerning restrictions of certain rights of

¹⁷ In particular, the Data Protection Regulation (EU) 2018/1725.

¹⁸ The data processing controller may be contacted at the following addresses: investigations@eib.org for investigations related to breaches of the EIB Group Anti-Fraud Policy, dignityatwork@eib.org for investigations related to breaches of the EIB Group Dignity at Work Policy and ethics@eib.org for investigations related to breaches of the EIB Group Staff Code of Conduct.

¹⁹ www.edps.europa.eu.

²⁰ EIB decision of 6 February 2019 laying down internal rules concerning the processing of personal data by the Fraud Investigations Division within the Inspectorate General and the Office of the Chief Compliance Officer of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights: [EUROPEAN INVESTMENT BANK DECISION – of 6 February 2019 – laying down internal rules concerning the processing of personal data by the Fraud Investigations Division within the Inspectorate General and the Office of the Chief Compliance Officer of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights.](#)

²¹ EIB decision of 26 February 2019 laying down internal rules concerning the processing of personal data by the Personnel Directorate of the European Investment Bank in relation to the provision of information to data subjects and the restriction of certain of their rights: [eib decision on the processing of personal data en.pdf.](#)

data subjects in relation to the processing of personal data within the framework of activities carried out by the EIF.²²

H.3 Personal data quality principle

47. The Investigations Division shall ensure the respect of the data quality principle, as per Article 4 of the Data Protection Regulation (EU) 2018/1725, that personal data must be accurate and, where necessary, kept up to date, as well as adequate, relevant and limited to what is necessary in relation to the purposes of the investigation for which they are collected and further processed. In addition, data shall be processed fairly, lawfully, in a transparent manner and only for specified, explicit and legitimate purposes.

H.4 Transfers of personal data outside the EIB Group

48. Transfers of personal data by the Investigations Division may occur to its operational partners, including EU institutions, bodies, offices and agencies; notably the European Public Prosecutor's Office and the European Anti-Fraud Office, or Member State authorities, third country authorities or international organisations. Such transfers may take place during the Investigations Division's operational activities in writing, orally (by telephone or in person), or by any other means. Any such transfer must be made in accordance with Regulation (EU) 2018/1725. In making such a transfer in the context of a case, standard and appropriate data protection clauses shall be used by the Investigations Division.

²² [EIF Decision of 4 June 2020 on internal rules concerning certain restrictions of rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the European Investment Fund.](#)

I. OTHER MATTERS

I.1 Status reports

49. The Investigations Division shall submit periodic status reports for information to the Management Committee, Audit Committee, EIF Chief Executive, Audit Board and other parties as appropriate.

I.2 Retention policy

50. All documentation and information for cases shall be kept in a secure and confidential manner by the Investigations Division and shall be retained for up to ten years maximum from the date of closure of the case and related follow-up.

I.3 Allegation of fraud and misconduct by an Investigations Division staff member

51. Where necessary, arrangements will be made by the Inspector General on a case-by-case basis to investigate alleged fraud and misconduct on the part of any staff member of the Investigations Division.

I.4 Applicability and amendments to the Investigation Procedures

52. These procedures shall replace and repeal the Investigation Procedures approved by the Management Committee on 27 March 2013. They shall take effect on the day of their publication. They shall also apply to assessments and investigations in progress on that date.
53. These procedures shall be further amended and updated as appropriate. Amendments may be necessary, based on:
 - a. changes to the EIB Group Anti-Fraud Policy, EIB Group Staff Code of Conduct, EIB Group Whistleblowing Policy or EIB Group Dignity at Work Policy;
 - b. revision of the European Anti-Fraud Office's Guidelines on digital forensic procedures;
 - c. experience gained in implementing the procedures;
 - d. the evolution of best practices.

ANNEX 1: EIB PROTOCOL FOR CONDUCTING COMPUTER FORENSIC OPERATIONS

Introduction

The EIB Protocol for Conducting Digital Forensic Operations comprises internal rules, which are to be followed by staff of the EIB's Inspectorate General Investigations Division with respect to the identification, acquisition, imaging, collection, analysis and preservation of digital evidence. The aim of this protocol is to establish rules for conducting digital forensic operations in a manner that ensures the integrity and the chain of evidence to be admissible in administrative and judicial procedures.

The purpose of a digital forensic operation is to secure potential digital evidence by creating forensic image(s) of digital media relevant for an Investigations Division investigation. As digital forensic operations often involve the collection of large amounts of data, including personal data, they may be invasive of privacy. This protocol is therefore also designed to help ensure compliance with data protection provisions in the context of digital forensic operations.

In cases where the European Anti-Fraud Office or the European Public Prosecutor's Office

- i. have competence to investigate but request digital forensic support by the Investigations Division; or
- ii. do not have competence to conduct an investigation, but the Investigations Division does; or
- iii. decide not to investigate, and the Investigations Division is competent

the Investigations Division will deploy its own digital forensic capacity. In the exceptional cases where the Investigations Division lacks specific equipment or expertise, it may rely on the assistance of suitably qualified external service providers.

This protocol has taken internationally approved standards and good practices into account, such as the ISO Standard 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence, adopted in October 2012, and the APCO Good Practice Guide for Digital Evidence published by the UK Association of Chief Police Officers in March 2012. This protocol also takes into consideration the European Anti-Fraud Office's Guidelines of Digital Forensic Procedures and the General Principles for Digital Evidence endorsed by the Conference of International Investigators.

Article 1. Definitions

- 1.1 Digital forensics: The application of digital investigation and analysis techniques to perform a structured examination of digital storage media, while maintaining a documented chain of evidence, for the purpose of gathering information admissible in evidence in a court of law or in administrative procedure. It focuses on identifying, acquiring, processing, analysing and reporting on collected data gathered from computer systems, digital devices or other storage media.
- 1.2 Chain of evidence: Refers to detailed documentation and a logical explanation of the status of potential digital evidence at every point in time from the moment of collection, acquisition or seizure of the evidence to the moment the evidence is presented in court or used in the context of administrative procedure.
- 1.3 Digital forensic examiner: Investigations Division staff or external consultants with specialised technical expertise and extensive training to perform digital forensic operations and prepare related reports.

- 1.4 Digital forensic operation: A technological inspection, acquisition and examination of digital media and/or their contents, carried out by digital forensic examiners using forensic equipment and software tools. The objective is to locate, identify, collect and/or acquire and preserve data which may be relevant to an investigation, and may be used as evidence in administrative, disciplinary and judicial procedures.
- 1.5 Preview: A first inspection of a digital medium or a digital storage location using an appropriate forensic tool to establish whether it may contain data potentially relevant to the investigation.
- 1.6 Digital forensic triage: This is a part of the forensic examination process. There are two types of forensic triage, the live triage and the post-mortem triage. The primary goal of the triage is a rapid understanding and extraction of the data gathered during the digital forensic operation. In particular, the live triage focuses on the identification and extraction of relevant data, and the post-mortem triage more on the ranking of evidence in a relevant order.
- 1.7 Digital forensic collection: The process of gathering data from physical devices and/or logical data from digital media that contain potential digital evidence. Forensic data collection targeting only a subset of data, active data on a logical partition or cloud service can be stored in a logical image file.
- 1.8 Digital forensic acquisition: The acquisition process, performed in a forensically sound manner making sure the data are acquired in the order of volatility, including the acquisition of any data (including deleted data) stored on a digital medium through a forensic imaging process.
- 1.9 Digital forensic image: The forensic copy of original, unaltered data contained on a digital storage medium, acquired during a digital forensic operation and stored in binary forensic image format including compression, encryption, error-checking, case metadata and a unique hash value. A digital forensic image can also be a bitwise copy, often referred to as raw image, and a calculated hash value.
- 1.10 Hash value: A “digital fingerprint” of the data, which helps to verify the integrity of data and of a digital forensic image as an acquired dataset. It is a fixed length computational result generated from a string of data (files, directories, an entire hard disk, etc.) using a specific mathematical algorithm that creates a unique value.
- 1.11 Digital forensic evidence file: A complete set of unaltered electronic data created by the digital forensic examiner during the digital forensic acquisition operation. This includes all digital forensic images, including logical and/or physical images with the collected data linked to a specific investigation case file.
- 1.12 Digital forensic work file: A copy of the digital forensic image(s) and data collected on which all searches and analyses are carried out in the Investigations Division forensic laboratory. This includes files created by the forensic software used, such as log files, index files, recovered files, expanded compound files (archive files, past files, database files, etc.), files exported from forensic images, bookmarks, handover of digital media notes, and reports.
- 1.13 Security copy: A copy of the digital forensic evidence and work files for the purpose of having a backup copy in case of loss, destruction or a compromised original digital forensic image.
- 1.14 In-house backup copy: A copy of the digital forensic evidence and work files stored in the Investigations Division’s archives, which is made by the digital forensic examiner upon return to the office.
- 1.15 Digital device: A device containing digital data (a file server, a computer hard disk, a CD/DVD, a USB memory stick, a smartphone, a SIM card, flash memory cards, all electronic appliances equipped with storage, etc.).
- 1.16 Cloud service provider: A service provider that offers remote storage, EIB cloud services, and/or software services accessible via a network or/and via the internet.
- 1.17 Internet service provider: An organisation that provides services for accessing, using or participating in the internet.

- 1.18 Traffic data: Data collected about an individual's use of an electronic network. This data could concern the routing, timing and duration of a communication.

Article 2. Forensic laboratory of the Investigations Division

- 2.1 The Investigations Division's digital forensic laboratory is a physically isolated and secure office within the Investigations Division, devoted to digital forensic services. It includes the location where the digital forensic evidence and work files are stored, and the consultation area for the investigators and operational analysts.
- 2.2 The file server and the forensic workstations operate on their own network, called the Digital Forensic Network, which is fully isolated from the EIB's network and has no internet connection.
- 2.3 Access to this laboratory is restricted via electronic access control and logged by badge readers to Investigations Division-authorized operational staff that have a need to know. Access logs are reviewed periodically.
- 2.4 Access to the data stored within the Digital Forensic Network is restricted through dedicated user management, ensuring that each Investigations Division staff member is granted appropriate data access rights based on their role and the specific need at the time.

Article 3. Preparation of a digital forensic operation

- 3.1 Conducting digital forensic operations and examinations is a resource-intensive process. Given the limited availability of forensic computing resources, careful planning is essential to make these operations more efficient, operationally effective, and achievable with the resources that are available.
- 3.2 At the very outset of an investigation, all sources of digital evidence potentially relevant to the investigation should be identified and preserved. As digital evidence can be temporary, acting swiftly is crucial.
- 3.3 During the planning stage, investigation staff must assess the added value that forensics can bring. Clear, achievable goals should be set, and investigators should outline as accurately as possible the scope of the planned operation. During the operation, further selective data capturing may be required. Where possible, live data examination preview can be used to refine the scope of the operation.

Article 4. Conducting a digital forensic operation – general procedures

- 4.1 Both internal and external digital forensic operations shall be conducted based on internal guidelines and workflows by the digital forensic examiner(s) under the coordination of an Investigations Division investigator. The investigator should typically be present at the start of the operation but does not need to remain present throughout. If possible, the digital forensic examiner should remain present for the duration of the digital forensic operation.
- 4.2 In general, the Investigations Division will act in line with the provisions of the Investigation Procedures. When providing digital forensic support to other national or international authorities, the Investigations Division will comply with the applicable laws and regulations of those authorities.
- 4.3 In compliance with applicable laws, rules, regulations, policies and procedures, the Investigations Division may locate, identify, collect, acquire and preserve data from physical devices, including: corporate devices provided to employees (such as notebooks, tablets, data storage carriers and mobile devices), cloud-based sources, and logical data from digital media. This data, which may be relevant to an investigation, can be used as evidence.
- 4.4 At the start of the digital forensic operation, the digital forensic examiner shall:
 - a) document and take photographs/screenshots where appropriate of all digital media, subject to the forensic operation, as well as the physical surroundings and layout;
 - b) make an inventory of the digital media. The inventory should be included in the Digital Forensic Acquisition Report and the photographs attached to it.
- 4.5 In general, the digital forensic examiner should conduct a full digital forensic acquisition of the devices referred to in 4.4. If feasible, the digital forensic examiner and the investigator should preview those devices together to assess whether they contain data potentially relevant to the investigation and whether a partial forensic acquisition is appropriate. If so, the digital forensic examiner may perform a partial forensic acquisition of the data. A short description of the contents and the case reference number added by the digital forensic examiner shall be recorded during the acquisition. After the acquisition, the digital forensic examiner should include the log files and the result of the acquisition into the Digital Forensic Acquisition Report.
- 4.6 The digital forensic examiner shall create a forensic duplicate (security copy) of the acquired data on site, whenever feasible and if time allows, and store it on a separate digital storage medium. The storage medium must be forensically prepared, ensuring it is free of any residual or pre-existing data. The digital forensic examiner must verify the integrity of the forensic copy using appropriate validation methods, such as hash verification.
- 4.7 At the premises, the digital forensic examiner shall draw up a Digital Forensic Acquisition Report documenting all activities relating to the access, acquisition, collection and storage of the data. The report shall list all digital forensic copies created along with their respective hash values. Any errors, damage, incidents and the remedial steps taken must also be recorded. If the digital medium was not acquired forensically, this shall be recorded. Any objections made during the digital forensic operation shall be recorded in this report. Any incident should be recorded during the digital forensic operation.
- 4.8 All persons actively involved in the digital forensic operation, including representatives of national authorities and EU institutions, shall be listed. The report shall be signed by the digital forensic examiner who conducted the digital forensic operation and, if applicable, by the on-site technical staff who assisted the Investigations Division in the execution of their duties. The digital forensic examiner shall give a copy of the report to the investigator and shall register the original immediately upon return to the office.
- 4.9 All devices containing information gathered during digital forensic operations must be transported in a secure manner (on hardware- or software-encrypted hard disks, in anti-static

plastic bags sealed with security seals, in protective carrying bags to avoid damaging the device(s) if time permits, etc.). These devices remain under the physical control of the Investigations Division staff (such as on their person or in hand luggage during air travel) at all times during the transport, to ensure the integrity of the chain of evidence. If both a digital forensic image and a security copy have been created, they should be carried by different members of staff, if possible.

Article 5. Collection of data stored on a remote digital device

- 5.1 The digital forensic examiner may determine that data of potential relevance to the investigation are stored remotely, including data stored in the EIB's cloud or on corporate devices provided by the EIB to its employees.
 - If potentially relevant data are held by an economic operator on a wide area network, the investigator shall ask the person or the economic operator concerned to download the data using his/her/its credentials.
 - If potentially relevant data (such as log files) are held by a cloud service provider (Hotmail, Gmail, Yahoo Mail, Dropbox, etc.) or an internet service provider, the Investigations Division may request the relevant provider to supply it with this information.
- 5.2 Where feasible, downloading data from remote locations, including cloud environments or EIB-provided devices, should be conducted in the presence of the digital forensic examiner. This ensures that the full set of data is captured and that it has not been filtered or altered. The collected data should then be stored in a logical file container to preserve timestamps and metadata as accurately as possible.

Article 6. Examination of data gathered during a digital forensic operation

- 6.1 Immediately after completing a digital forensic operation involving physical devices, the digital forensic examiner shall follow the defined backup and disaster recovery procedure. Forensic images acquired from these devices must be duplicated to create a backup copy. Only the physical devices themselves need to be placed in sealed envelopes or evidence bags, each labelled with unique identification numbers. The digital forensic images will be securely copied to a separate medium, and both the originals and copies of images will be stored in the Investigations Division's secured room, protected by access control.
- 6.2 The digital forensic examiner shall transfer the digital forensic image to the forensic file server. The file thus transferred becomes the forensic work file. The digital forensic examiner should inform the investigator as soon as the forensic work file is ready.
- 6.3 After the work file is ready, the digital forensic examiner should, in consultation with the investigator(s), perform a prioritising triage to rank the gathered evidence in a relevant order.
- 6.4 Once the forensic work file is available, the investigator shall formally submit a request to the digital forensic examiner through the case management system, phrasing it as requested action within the case. The investigator shall provide specific requirements to the digital forensic examiner and, if necessary, seek the assistance of the digital forensic examiner or operational analyst to identify data relevant to the investigation. The requirements should clearly describe the purpose of the search and the type of evidence or proof being sought. In response, and in conjunction with the investigator, the digital forensic examiner shall extract data from the digital forensic work file that matches the search criteria, making it available for the investigator in a read-only format.
- 6.5 Searching for potential evidence is a dynamic process and may involve several successive iterations. The search process could involve looking for traces of deleted data in unallocated

space, specifying keywords, or conducting more complex/advanced searches such as special expression or timeline searches.

- 6.6 The investigator, with the guidance of the digital forensic examiner, shall identify potentially relevant information using the facilities of the digital forensic laboratory, or the remote review capabilities it provides. The investigator may also request that the digital forensic examiner print or create an electronic copy of relevant files, which should be attached to the appropriate investigation case file. Any such transfer of data from the forensics laboratory to the investigator must be documented in the investigation case file to ensure protection of the chain of evidence.
- 6.7 Upon completion of the examination of the digital forensic work file, the digital forensic examiner shall prepare a Digital Forensic Analysis Report summarising the forensic actions undertaken and subsequent results, and listing the information provided to the investigator. This report must be attached to the appropriate investigation case file. The digital forensic examiner shall also maintain a separate Digital Forensic Log File documenting all actions performed on the digital forensic work file.
- 6.8 Any special categories of personal data as defined in Article 9(1) of Regulation (EU) 2018/1725 extracted as relevant during a digital forensic examination may only be further processed following an assessment of the applicability of one of the exceptions mentioned in Article 9(2) of Regulation (EU) 2018/1725.
- 6.9 Traffic and content data can only be collected in accordance with the European Data Protection Supervisor's Guidelines on personal data and electronic communications in the EU institutions.

Article 7. Final backup of results

- 7.1 When no further requests for digital forensic examination or operational analysis are anticipated or when the investigation is closed, the digital forensic examiner shall create backup copies of the digital forensic evidence and work files. These copies should be placed in sealed envelopes or evidence bags with unique identification numbers and processed in accordance with Article 6.1 above.
- 7.2 The backup copies will be stored in the Investigations Division's archives until the end of retention period. All copies shall be removed from the forensic file server.

Article 8. Assistance provided to EIB Group partners

- 8.1 The European Anti-Fraud Office, the European Public Prosecutor's Office, Europol, Member State national authorities, a third country judicial or administrative authority, or an international organisation may request digital forensic assistance from the Investigations Division. Such assistance may be provided, within the competence of the Investigations Division, subject to availability of resources and respecting the EIB Group's rules and procedures.

Article 9. Retention period applicable to digital forensic evidence and work files

- 9.1 At the end of the case file's administrative retention period, the digital forensic evidence file and work files are treated in accordance with the same document management principles as the other parts of the case file.

INVESTIGATION PROCEDURES



European
Investment Bank | Group