Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Fund on procedures related to fraud investigations

Brussels, 29 June 2016 (Case 2014-1163)

1. Proceedings

On 17 December 2014, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Investment Fund (EIF) a notification for prior checking regarding the data processing operations that take place in the context of procedures related to fraud investigations.
The EDPS request further clarifications on 6 January 2015, which were provided on 21 January 2015 and 30 April 2015. A meeting with the EIF DPO took place on 28 January 2015.
On 22 May 2015, the EDPS sent the draft Opinion to the EIF for comments. The EIF did not reply to a final reminder sent on 7 June 2016, which announced the adoption of the Opinion as of 15 June 2016.

2. The facts

Purpose. Under section II.9 of the EIF's Anti-Fraud Policy adopted in March 2015 ("2015 Policy"), EIF Staff and EIF's business partners are required to maintain the highest level of integrity and efficiency in relation to all EIF activities and operations and the EIF "will not tolerate Prohibited Conduct in its activities". "Prohibited Conduct" is defined in sections I.1 and IV.13 of the 2015 Policy as covering corruption, fraud, collusion, coercion, obstruction, money laundering and terrorist financing.
Under a 2009 service level agreement with the EIF[1], the Inspector General and the Fraud Investigation Division of the European Investment Bank ("IG/IN") shall provide fraud investigation services to the EIF in accordance with the terms and conditions set out in the 2015 Policy.
The 2015 Policy in turn determines (section VII.C.53) that these investigations will be undertaken in conformity with the "**Procedures for the Conduct of Investigations by the Inspectorate General of the EIB**". These have been examined in the **EDPS Opinion in case 2009-0459** (closed) and will not be re-examined in the context of this Opinion. This Opinion will only refer to the EIF specific terms and conditions set out in the 2015 Policy in so far as they give raise to recommendations in the light of the facts as notified.

Procedure. ***Launching an investigation.*** Under section VI.C.45 of the 2015 Policy, all allegations by EIF staff members[2], EIF business partners, other counterparts and partners, or members of the public (including civil society) of suspected prohibited conduct should be

[1] Framework Agreement between the European Investment Bank and the European Investment Fund of 17 December 2009, there Annex 1 - Protocol of Understanding, section 3
[2] Under the Whistleblowing Policy and the Staff Code of Conduct, EIF staff members are required to report any suspected incidents of prohibited conduct immediately after becoming aware of the matter, see section VI.A.43 of the 2015 Policy.

reported to the IG/IN[3], which will acknowledge receipt of the allegation. A report can be made by letter, email, through the on-line form available on the website of the EIB, by telephone or by fax.
Under section VI.D.47 and 48 of the 2015 Policy, all allegations of prohibited conduct will be treated by the EIF as strictly confidential and may be made anonymously. As regards reports made by an EIF staff member, the Staff Code of Conduct and the EIF Whistleblowing Policy provide that the EIF will ensure confidential treatment for members of staff who make *bona fide* reports of suspected misconduct, and that such members of staff will enjoy the assistance and protection of the EIF.
Under section VII.A.49 of the 2015 Policy, the IG/IN, acting on behalf of EIF and working in close collaboration and full transparency with OLAF, shall be responsible for:

- receiving reports of alleged or suspected Prohibited Conduct involving the EIF's activities or EIF members of governing bodies and staff;
- investigating such matters and cooperating directly with OLAF in order to facilitate the latter's investigations; and
- reporting its findings to the Chief Executive, OLAF and the EIF Audit Board which has an oversight function, as well as any other staff member on a need-to-know basis.

Conducting the investigation. Section VII.B.51 of the 2015 Policy stipulates that "The Fraud Investigations Division shall enjoy complete independence in the exercise of its responsibilities. Without prejudice to the powers conferred on OLAF, the Head of the EIB Fraud Investigations Division shall have full authority to open, pursue, close and report on any investigation within its remit without prior notice to, the consent of, or interference from any other person or entity".
According to section VII.D.54 and 55 of the 2015 Policy, EIF members of governing bodies and staff are required to cooperate with the EIB Fraud Investigations Division and OLAF promptly, fully, efficiently and in the manner specified by the IG/IN, including by answering relevant questions and complying with requests for information and records. In order to conduct an investigation, the IG/IN and OLAF shall have full access to all relevant personnel, information, documents and data, including electronic data, within the EIF, in accordance with the applicable procedures.
Under sections VII.F.62 and 63 of the 2015 Policy, a member of governing bodies or staff who is the subject of an investigation shall be entitled to due process rights, in particular to be notified of that fact as early as possible, unless it is determined that to do so would be harmful to the investigation[4]. In any event, a member of governing bodies or staff who is the subject of an investigation shall be given notice of the allegations and evidence against him or her, and the opportunity to respond before any adverse action is taken.
According to section VIII.66 of the 2015 Policy, "any involved persons are entitled to access, rectify and (in certain circumstances) block data related to him/her by contacting the data processing controller or the EIF DPO. They may also at any time contact the EDPS to check that the rights conferred by the relevant provisions have been respected". Footnote 21 of the 2015 Policy notes in this context that "The data processing controller may be contacted at the following address: investigations@eib.org".

Outcome of an investigation. The IG/IN provides its findings to EIF senior management who have specific responsibility for the project and reports at the same time to the OLAF and the Audit Board of the EIF. A summary of all cases is, in addition, also sent to the EIF's external auditors every quarter. The EIF Chief Executive is informed by the EIB Inspector General on

[3] Under section II.10 of the 2015 Policy, any prohibited conduct is to be reported promptly to the IG/IN.
[4] Sections VII.F.64 of the 2015 Policy further stipulates that the provisions of the 2015 Policy, the Investigation Procedures and the appropriate Code of Conduct provide the framework for the rights of members of governing bodies and staff during an investigation.

the follow-up measures to be taken by the operational services, including contractual consequences.
In line with sections X.A.70 and 72 of the 2015 Policy, the IG/IN may refer suspected prohibited conduct to national authorities within and/or outside the EU for further investigation and/or criminal prosecution and provide further assistance as may be requested. Under sections X.B.73 and 74 of the 2015 Policy, the IG/IN may provide assistance to and share its findings and/or relevant information with other investigation functions of International Financial Institutions (IFI) and the IG/IN provides assistance to other international organisations and agencies in respect of suspected prohibited conduct.

The **legal basis** to conduct investigations in EIF operations and activities stems from:

- Article 325 of the Treaty on the Functioning of the European Union (TFEU);
- Council Regulation (EC, Euratom) No 966/2012[5] and the "Procedures for the Conduct of Investigations by the Inspectorate General of the EIB Group" adopted on 8 April 2008 as well as internal guidance developed on that basis ("Data Protection Guidance for IG/IN");
- A service level agreement (Chapter I of Annex 1 of the "Framework Agreement" of 17 December 2009) between the EIF and the EIB outsourcing investigation services to the IG/IN;
- Article 2 of the EIF Statute and the EIF Anti-Fraud Policy adopted on 9 March 2015[6].

Data subjects. In the course of the investigations, IG/IN may process data of staff members, EIF counterparts, suppliers and consultants, who are relevant for the investigation as subject, whistleblower and/or informant/witnesses.

Data quality. By standard practice, the IG/IN may access personal files of EIF staff members, including their electronically stored personal data, only with the prior written approval of the Head of HR and the EIF DPO.

Information given to data subjects. A privacy statement[7] is included in all of the IG/IN's outgoing correspondence in order to inform data subjects of the processing of their personal data, their rights as well as the possibility to contact directly the EDPS.
Under section VIII.66 of the 2015 Policy, all data subjects are entitled to access, rectify and (in certain circumstances) block data related to them "by contacting the data processing controller" or the EIF DPO. Regarding the former, footnote 21 reads as follows: "The data processing controller may be contacted at the following address: investigations@eib.org".
Concerning EIF staff members, in accordance with section VII.F.62 of the 2015 Policy, a staff member who is the subject of an investigation shall be entitled to due process rights, in particular, to be notified of that fact as early as possible, unless it is determined that to do so would be harmful to the investigation.
Furthermore, in accordance with section VII.F.63 of the 2015 Policy, a staff member who is subject of an investigation shall be given notice of the allegations and evidence against him or her, and the opportunity to respond before any adverse action is taken. According to the

[5] Regulation (EC, Euratom) No 966/2012 of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (Financial Regulation), see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:298:0001:0096:EN:PDF, in particular recital 56, stipulating that "*This Regulation should lay down the principles and conditions for financial instruments and rules on the limitation of the financial liability of the Union, the fight against fraud and money laundering, the winding down of financial instruments and reporting.*"
[6] The procedures established at the EIF to combat fraud are based on principles agreed by the IFIs Anti-Corruption Task Force and laid out in the Uniform Framework agreement, signed in Singapore in September 2006, see http://www.eib.org/attachments/general/uniform_framework_en.pdf.
[7] Annex 2 of the Data Protection Guidance for IG/IN covered by case 2009-0459.

notification, the information may be deferred if this constitutes a necessary measure to safeguard the investigation. This restriction is applied only when necessary and subject to a "necessity test" to be conducted on a case-by-case basis. The IG/IN shall review from time to time whether the restriction still applies. If the information to a data subject has been postponed, the information will be provided to the data subject as soon as this no longer negatively impacts on the ongoing investigation.

Recipients. The IG/IN provides its findings to EIF senior management who have specific responsibility for the project and reports at the same time to the OLAF and the Audit Board of the EIF. A summary of all cases is, in addition, also sent to the external auditors of the EIF every quarter.
The EIF Chief Executive is informed by the IG/IN about the follow-up measures to be taken by the operational services, including contractual consequences.
With the assistance of the OLAF, the IG/IN may refer a matter to the appropriate national authorities within and outside the European Union for further investigation and/or criminal prosecution. Under sections X.B.73 and 74 of the 2015 Policy, the IG/IN may provide assistance to and share its findings and/or relevant information with other investigation functions of International Financial Institutions (IFI) and the IG/IN provides assistance to other international organisations and agencies in respect of suspected prohibited conduct.

Transfers. The IG/IN may refer suspected prohibited conduct to national authorities outside the EU for further investigation or criminal prosecution and provide further assistance as may be requested. The IG/IN may also share its findings with other IFIs' investigation functions. Where such referrals to third countries and international organisations include the transfer of personal data, the following procedure applies:

- Where the recipient provides an adequate level of protection under the list of countries established by the European Commission, the appropriate transfer clause is used.
- Where the recipient does not ensure an adequate level of protection, but has a Memorandum of Understanding (MoU) with the IG/IN including appropriate data protection clauses, the relevant transfer clause is used.
- Where the recipient has neither an adequate level of protection nor a MoU with the IG/IN, it is possible to rely for occasional transfers on the derogation in Article 9(6)(d) of the Regulation which states that the "transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims.". Use of this derogation is determined on a case-by-case basis for every transfer. In such situations, a standard transfer clause is included[8].

Rights of data subjects. Any request from data subjects for an access, rectification, blocking and erasure is forwarded the Head of IG/IN. If the request is made orally to the IG/IN, the concerned investigator shall ask the data subject to submit his/her request in writing to the Head of the IG/IN. As part of the rights of data subjects, access is granted to any documents containing personal data processed during an investigation to the relevant data subject. In the case of an interview, this includes the written record of interview of which a copy is given to the interviewee for review and signature.
When information has been provided by a whistleblower or external informant, the data subject requesting access must be given access to his/her personal data, but will not be provided with the name or any other element of information which would allow for the identification of the whistleblower or external informant.

[8] See Annex 3 of the Data Protection Guidance for IG/IN covered by case 2009-0459.

Retention periods. Personal data shall be retained for at least five years and up to ten years maximum from the date of closure of the case.

- 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, data shall be retained for up to five years maximum from the decision not to open a case or from the closure of the case.
- According to the notification, however, paper files will be destroyed ten years after the case has been closed.

Security. (...)

3. Legal Aspects

3.1. Prior checking

Fraud investigations entail the collection and further processing of personal data as defined under Article 2(a) of Regulation (EC) No 45/2001 (the "Regulation") by an EU entity, here the EIF, in the framework of its activities (Article 3(1) of the Regulation). In the case at hand, these personal data undergo "automatic processing" operations, as defined under Article 2(b) of the Regulation as well as manual data processing operations. The Regulation thus applies to the processing operation at issue.

Article 27(1) of the Regulation subjects to prior checking by the EDPS "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (b), the processing operations intended to evaluate personal aspects related to the data subject, including his or her ability, efficiency and conduct. Fraud investigations intend to evaluate the conduct or reliability of persons. Furthermore, Article 27(2)(a) stipulates that processing operations relating to "suspected offences, offences, criminal convictions or security measures" shall be subject to prior checking. In the case at hand, the processing operation can encompass such type of data. The processing operation at hand is thus prior-checkable.

The notification was received on 17 December 2014. The period within which the EDPS must deliver an Opinion was suspended for a total of 511 days. Following the lifting of the suspension on the occasion of the consultation of the EIF, this Opinion must now be adopted no later than 12 July 2016.

3.2. Controller / processor

Investigation services are outsourced under a service level agreement to the IG/IN. According to section VII.B.51 of the 2015 Policy, "The Fraud Investigations Division shall enjoy *complete independence in the exercise of its responsibilities*. Without prejudice to the powers conferred on OLAF, the Head of the EIB Fraud Investigations Division shall have full authority to open, pursue, close and report on any investigation within its remit without prior notice to, the consent of, or interference from any other person or entity." (emphasis added).
However, as explicitly stipulated in the service level agreement with the EIF, the Fraud Investigation Division of the EIB shall provide fraud investigation services to the EIF *in accordance with the terms and conditions set out in the EIF Anti-Fraud Policy*. It is thus the EIF that remains the EU entity determining the purposes and means of the processing at issue and therefore 'controller' in the sense of Article 2(d) of the Regulation. The EIF's Compliance and Operational Risk Division (EIF COR) is responsible on behalf of the EIF as controller of the processing operation.

This should be reflected in the provisions regarding the following two topics:

- Under section VIII.66 of the 2015 Policy, all data subjects are entitled to access, rectify and (in certain circumstances) block data related to them "*by contacting the data processing controller*"; the respective footnote 21 refers to investigations@eib.org. Although this is a functionally correct contact information, in the light of the above, it would seem preferable to not allude to the EIB as controller by reference to an EIB functional mailbox. The EDPS consequently invites the EIF to clarify the wording of footnote 21 of the 2015 Policy on the occasion of the next review of the policy document to read "*The EIF as controller may be contacted at the following address:* investigations@eib.org".

- As mentioned in the notification, by standard practice, the IG/IN may access personal files of EIF staff members, including their electronically stored personal data, only with the prior written approval of the Head of HR and the EIF DPO. The EDPS invites the EIF to justify the involvement of the Head of HR in this by its nature sensitive procedure. The EDPS further suggests formalizing this standard practice (e.g. by introducing an explicit reference to it in Chapter I of Annex 1 of the "Framework Agreement" of 17 December 2009 upon the occasion of its next revision) and Section VII.B.51. of the 2015 Policy, which currently reads "*...the Head of the Fraud Investigations Division shall have full authority to... pursue...any investigation... without prior notice to, the consent of, or interference from any other person or entity*", should then be amended accordingly.

3.3. Data Quality

Article 4(1)(a) of the Regulation requires inter alia that data must be processed fairly. In this context, the EDPS notes that allegations submitted by anonymous or confidential sources raise a specific problem in this with regard. The EDPS considers that schemes aimed at collecting personal data in the context of fraud allegations should be built in such a way that they do not encourage anonymous reporting as the standard way to raise concerns[9]. Whilst section VI.D.47 of the 2015 Policy allows for allegations to be made anonymously, this should not be encouraged as standard practice. This principle should be reflected in the EIF whistleblowing policy and the EDPS reminds the EIF that data quality should be carefully ensured in such processing operation.

3.4. Conservation of Data

Pursuant to Article 4(1)(e) of the Regulation, personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

As it is not obvious how the medium of storage (electronic files vs paper files) could make a difference to retention needs, the EDPS underlines the need to harmonize the conservation periods. In addition, the EIF should re-assess the need to keep data relating to fraud investigations for up to ten years when the Head of IG/IN decides not to open a case or if, after an investigation, the IG/IN determines that a complaint or allegation has not been substantiated and decides to close the case.

[9] See also Article 29 Working Party Opinion 1/2006 on the application of the EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

3.5. Transfers of Data

According to the notification, if the Head of IG/IN decides not to open a case, he shall make information regarding the allegation and its evaluation available upon request to the President and the Vice President responsible for investigations, the Secretary General, the Audit Committee, the OLAF and the external auditors. The EDPS underlines that such requests must be examined in the light of Articles 7(2) or 8 of the Regulation, which notably implies the verification of the competence of the recipient of the necessity of the transfer. Moreover, Article 7(3) of the Regulation states that "The recipient shall process the personal data only for the purposes for which they are transmitted". The EDPS underlines that at all stages of the procedure, the recipients to whom the data are transferred must be reminded that they can only process the data for the purposes of fraud investigations.

All other transfers by the IG/IN occurring in the context of the processing operation at hand have already been examined in the EDPS Opinion in case 2009-0459. There, with a particular view to IG/IN transferring personal data to IFIs located in third countries, the EDPS recommended that the EIB ensure compliance with Article 9 of the Regulation. The EDPS invites the EIF to do so *mutatis mutandis* and in keeping with respective guidance given in the 2014 EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies[10].

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation provided that the EIF as 'controller' in the sense of Article 2(d) of the Regulation takes all recommendations contained in this Opinion into account.

In particular, the EIF must:

- Harmonize the conservation periods for different storage media;
- Re-assess the necessity to keep data relating to fraud investigations for up to 10 years generally and in particular for cases in which the Head of IG/IN decides not to open a case or if, after an investigation, the IG/IN determines that a complaint or allegation has not been substantiated and decides to close the case;
- Where information regarding the allegation and its evaluation is requested after the Head of IG/IN decided not to open a case, the EIF must ensure that the necessity of such transfer is verified and remind the recipients that they can only process the data for the purposes of fraud investigations.

In addition, the EIF should:

- Clarify the wording of footnote 21 of the 2015 Policy on the occasion of the next review of the policy document to read "The EIF as controller may be contacted at the following address: investigations@eib.org";
- Ensure data quality in the context of allegations made anonymously in the context of the EIF's whistleblower scheme;

[10] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf

- Formalize the standard practice requiring the prior written approval of access by IG/IN to personal files of EIF staff members (e.g. by introducing an explicit reference to it in Chapter I of Annex 1 of the "Framework Agreement" of 17 December 2009 upon the occasion of its next revision) and amend section VII.B.51 of the 2015 Policy accordingly.

Done at Brussels, 29 June 2016

(signed)

Wojciech Rafał WIEWIÓROWSKI
Assistant Supervisor