Opinion on the notification for prior checking received from the Data Protection Officer of the European Court of Auditors concerning the ECA's Panel for Financial Irregularities

Brussels, 17 March 2014 (Case 2013-0846)

1. Proceedings

On 10 July 2013, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer ("DPO") of the European Court of Auditors ("ECA") a notification for ex-post prior checking concerning the ECA's Panel for Financial Irregularities ("PFI").

On 12 November 2013 and 7 January 2014, the EDPS sent requests for additional information to the DPO, who responded on 6 as well as 10 and 18 January 2014 respectively. The draft Opinion was sent to the DPO for comments on 27 February 2014 and these were received on 13 March 2014.

2. Facts

The PFI, which is operationally independent of the ECA, was established by Decision of the Court of Auditors No 43-2007 of 17 July 2007 ("the Decision")[1]. It consists of four members, who determine a President amongst them and meet at least once a year.

Purpose. According to Article 2 of the Decision, the PFI is competent to examine any infringement by an official or other member of the ECA's staff (the "person concerned") of a provision of the Financial Regulation (FR)[2] or of any rule relating to financial management or the audit of transactions, whether by commission or omission. The PFI thus examines whether a financial irregularity happened based on the facts brought to the attention of the PFI.

Description of the processing. Under Article 5(1) of the Decision, the PFI has established its own Rules of Procedure ("*Règlement intérieur de l'Instance spécialisée en matière d'irrégularités financières*" of 25 June 2012), which are available on the ECA's intranet. Under Title III (Articles 11 to 14) of these Rules of Procedure, once a case has been submitted to the PFI's scrutiny (Article 11(1)), the PFI invites comments by the person concerned (Article 12(1)) and further information where required (Article 13). Where required, a written procedure is launched (Article 14), which involves the consultation of all PFI members by the President on a draft

[1] Decision of the Court of Auditors No 43-2007 concerning the Court's specialised financial irregularities panel of 17 July 2007 ("the Decision") as amended by Decision of the Court of Auditors No 75-2010, in turn amended by Decision of the Court of Auditors No 20-2012.
[2] Financial Regulation (Regulation (EU, EURATOM) No 966/2012 of the European Parliament and the Council of 25 October 2012.

opinion (with the possibility of tacit approval within ten working days). Each non-approving PFI member can ask for the written procedure to end and for the matter to be put on the agenda of the next PFI meeting.

Legal basis: The PFI is based on Articles 66(8), 72(2) and 73(6) FR, Articles 29, 74 to 76 of the Rules of Application of the Financial Regulation[3] and the Decision.

Data subjects are:

- officials or other ECA staff members allegedly having committed an infringement of a provision of the FR or any rule relating to financial management or the audit of transactions, whether by commission or omission (the "persons concerned");
- witnesses contributing to the PFI investigation;
- PFI members.

According to the notification, the following **personal data** are collected and processed:

- For "persons concerned": (a) administrative data (name, first name, address, telephone number, grade, administrative position) and (b) facts about the alleged irregularity and (c) an evaluation of these facts by the PFI;
- For witnesses: administrative data (name, first name, address, telephone number, grade, administrative position);
- For PFI members: name, which under Article 16 of the Rules of Procedure will be made public each time the composition of the panel is modified and will be mentioned in the meeting minutes of the panel and in its reports.

The **recipients** of the data are:

- AIPN if the PFI judges it necessary;
- Internal auditor (mandatory following the FR);
- OLAF, administrative and/or disciplinary investigators for investigations;
- EDPS and the ECA DPO in case of data protection complaints;
- Ombudsman in case of administrative complaints;
- National authorities upon presentation of an official mandate.

Regarding the **right to be informed**, according to the notification, at the opening of an evaluation by the PFI, the person concerned is informed by the PFI of the objective of the evaluation procedure, why the PFI examines the facts, to whom the final report will be transmitted, her/his rights to access, possibly to rectify the data concerning her/him, the legal basis, the time period the data will be retained and stored and the right to contact the ECA's DPO and the EDPS at any time.

As concerns the **rights of data subjects with respect to their personal data:**

- The persons concerned can have access to the PFI file concerning her/him, at any time, except as concerns evaluations about other persons and the protection of identity of third person(s).

[3] Rules of Application of the Financial Regulation (Commission Delegated Regulation of 29.10.2012).

- According to the notification, the person concerned has the possibility to comment on the facts mentioned in the file as well as the draft final report. In addition, the person concerned can request, based on justifications and legitimate grounds, to block, erase and correct information about her/him.

Retention period. Depending on the outcome of the procedure, different retention periods apply:

- where no evaluation is judged necessary, three years after the decision not to evaluate;
- where the evaluation is made and the evaluation report is sent to the AIPN, who decides not to launch an administrative investigation or a disciplinary procedure, three years;
- where the evaluation is made and the evaluation report is sent to the AIPN, who decides to launch an administrative investigation or a disciplinary procedure and where there is no sanction or a minor sanction, three years after the decision on the sanction;
- where the evaluation is made and the evaluation report is sent to the AIPN, who decides to launch an Administrative investigation/Disciplinary procedure and where there is a major sanction, six years after the decision on the sanction.

Security measures. (...)

3. Legal aspects

3.1. Prior checking

Applicability of Regulation (EC) No 45/2001 ("the Regulation"). The processing by the ECA of data relating to persons concerned, witnesses and panel members in the context of PFI investigations constitutes a processing of personal data ("*any information relating to an identified or identifiable natural person*", Article 2 (a) of the Regulation). The PFI, which is operationally independent of the ECA, performs the processing of data, but operates under the Decision as an entity, which is an integral part of the ECA environment. In examining potential infringements of the Financial Regulation or of any rule relating to financial management or the audit of transactions, the ECA acts within the scope of EU law (Article 3(1) of the Regulation in the light of the Lisbon Treaty). According to the notification, the processing is done entirely manually and only the final report is in writing and transmitted in a paper format. However, the final report (and in case of the written procedure under Article 14 of the Rules of Procedure also the draft opinion) forms part of a filing system. Therefore, the Regulation is applicable.

Grounds for prior checking. According to Article 27(1) of the Regulation, "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purpose shall be subject to prior checking by the European Data Protection Supervisor*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

- This list includes "*processing of data relating to...suspected offences, offences, criminal convictions or security measures"* (Article 27 (2)(a) of the

Regulation). Under Article 2 of the Decision, the PFI's purpose is to examine any infringement by an official or other member of the Court's staff (the "person concerned") of a provision of the Financial Regulation or of any rule relating to financial management or the audit of transactions, whether by commission or omission.

- The list further includes "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*" (Article 27 (2)(b) of the Regulation). The PFI evaluates the conduct of persons concerned and a PFI investigation might also lead to the evaluation of personal aspects in the context of assessing the credibility of witnesses.

The processing operation at hand is thus prior-checkable.

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case however, the EDPS notes with great regret that the processing operation has already been established (the Decision dates of 2007 and the Rules of Procedure of 2012). In any case, any recommendations made by the EDPS should be adopted accordingly.

Deadlines. The notification of the DPO was received on 10 July 2013. As this is an ex-post case, the deadline of two months for the EDPS to issue his Opinion under Article 27(4) of the Regulation does not apply; this case has been dealt with on a best-effort basis.

3.2. Lawfulness of the processing

Article 5 of the Regulation provides criteria for making the processing of personal data lawful. According to Article 5(a), the processing is lawful if it is "*necessary for the performance of a task carried out in the public interest on the basis of the Treaties...or other legal instruments adopted on the basis thereof*".

a) The processing operation is performed in the context of a **task carried out in the public interest** in the context of the ECA's obligations under the Financial Regulation to examine financial irregularities.

b) **Existence of a legal basis.** The PFI is based on Articles 66(8), 72(2) and 73(6) of the Financial Regulation, Articles 29, 74 to 76 of the Rules of Application of the Financial Regulation and the Decision.

c) As to the **necessity of the processing**, it appears that the processing of personal data is necessary, in frame of PFI investigations of potential infringements by ECA staff members of a provision of the Financial Regulation or of any rule relating to financial management or the audit of transactions are necessary for ensuring the effective functioning of the ECA.

3.3. Data Quality

Adequacy, relevance and proportionality. According to Article 4 (1)(c) of the Regulation, personal data must be *"adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed"*.

Adequacy: The data processed in the context of a PFI investigation seem adequate, relevant and non excessive for the purpose for which they are collected.

Accuracy. Article 4 (1) (d) of the Regulation provides that personal data must be "*accurate and, where necessary, kept up to date*" and that "*every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified*".

The EDPS notes that according to the notification, at the opening of an evaluation by the PFI, the person concerned is informed of the objective of the evaluation procedure, why the PFI examines the facts, to whom the final report will be transmitted, her/his rights to access and eventually to rectify the data concerning her/him. The EDPS further notes that under Article 12(1) of the Rules of Procedure, the PFI invites the person concerned to submit comments within 15 days. Where the PFI during its investigation receives additional information on the person concerned, the person concerned is again invited to comment (Article 13(2) of the Rules of Procedure).

The contradictory nature of the PFI procedure in itself guarantees data quality as regards the personal data processed as well as all pieces of information on which the PFI bases its report[4]. For reasons of completeness, the EDPS considers that the procedure has to ensure that all the elements validly presented are included. Consequently, all processed information should be contained in the PFI file. To ensure the highest degree of completeness, it is advisable to guarantee also the rights of access and rectification of the concerned person. They represent the second possibility of ensuring data quality (concerning these two rights of access and rectification, see also below Section 3.6).

Fairness and lawfulness. Article 4 (1) (a) of the Regulation also provides that personal data must be *"processed fairly and lawfully"*. Lawfulness has already been discussed (see above Section 3.2) and fairness will be dealt with in relation to information provided to data subjects (see below Section 3.7).

3.4. Data retention

Article 4 (1)(e) of the Regulation states that personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"*. The different retention periods outlined above as such are no reason for concern to the EDPS[5]. However, the EDPS notes that the ECA network drives containing the PFI opinions are backed up daily and kept for seven years. Such opinions occur in the following two situations:

- where an evaluation is made and the evaluation report is sent to the AIPN, who decides to launch an administrative investigation or a disciplinary procedure as well as in cases where there is no sanction or a minor sanction;

[4] See e.g. EDPS Opinions in cases 2012-0533 and 2007-0433 of 26 September 2012 and 17 October 2007 respectively.
[5] See for similar retention periods EDPS Opinion of 17 October 2007 in case 2007-0433.

- where the evaluation is made and the evaluation report is sent to the AIPN, who decides to launch an Administrative investigation/Disciplinary procedure and where there is a major sanction.

The retention periods set out in the notification under such circumstances are three years after the decision on the sanction and six years after the decision on the sanction respectively.

The ECA noted in this respect that the backups consist of taking snapshots of the entire network drive or full backups on tape and that the ECA has an obligation to keep its financial and audit files for seven years. The equally concerned PFI files (on average less than five Word files a year) are marginal and, due to a technical restriction, it is impossible to delete some files from a disk snapshot or from a backup tape. Installing a dedicated back-up/snapshot procedure only for PFI files would be disproportionate under these circumstances.

Given that the retention periods set out in the notification in practice will not differ very much from seven years and that, according to the ECA, restoring PFI files would require the precise path name and/or file name, the EDPS does not see any reason for concern under Article 4 (1)(e) of the Regulation. The EDPS would, however, want to remind the ECA that the personal data cannot be used for further purposes after the end of the retention period.

3.5. Transfer of data

In line with Article 7 of the Regulation, personal data can be transferred within or to other institutions or bodies *"if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient"* (paragraph 1). The recipient shall process the data "*only for the purposes for which they were transmitted"* (paragraph 3). Under Article 8(a) of the Regulation, personal data can be transferred to recipients subject to national law implementing Directive 95/46/EC, if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority.

The EDPS considers that the transfer of data to the PFI is covered by Article 7(1) of the Regulation as a transfer internal to the ECA structure. The EDPS further considers that the transfers to the other recipients listed in point 2 above, with the exception of transfers to national authorities, are transfers to other EU institutions or bodies complying with Article 7(1) of the Regulation. The EDPS recommends that in accordance with Article 7(3) of the Regulation, each of the recipients is explicitly reminded that they should process the personal data they receive only for the purpose for which they were transmitted. Given that national authorities will receive personal data upon presentation of an official mandate, the requirements of Article 8(a) of the Regulation are met.
The transfers foreseen in the context of the processing operation therefore do not give rise to concern under Articles 7 or 8 of the Regulation.

3.6. Rights of the data subjects to access and to rectify

Articles 13 and 14 of the Regulation establish the right for data subjects to access their data upon request and the right to rectify their personal data.

a) The person concerned

The person concerned can have access to the PFI file concerning her/him, at any time, except for the evaluations about other persons and the protection of identity of third persons. According to the notification, the person concerned has the possibility to comment on the facts mentioned in the file as well as the draft final report. In addition, the person concerned can request, based on justifications, to block, erase and correct information about her/him.

The EDPS has previously noted that in the context of a "conduct evaluation" it is difficult to determine whether personal data are *"inaccurate"* or not[6] and that, consequently, the right of rectification only applies to objective and factual data in such context. As regards the right of the person concerned to comment on the facts mentioned in the draft final report, the EDPS notes that the Rules of Procedure do not explicitly refer to this right; he consequently recommends including such a reference in the Rules of Procedure.

b) Other data subjects (witnesses, PFI members)

As regards the other data subjects (witnesses, PFI members), no rules exist to safeguard their rights under Articles 13 and 14 of the Regulation. The EDPS therefore recommends that the ECA establish such rules in the Rules of Procedure.

c) Exception based on Article 20 of the Regulation

As regards the exception applicable to the evaluations about other persons and the protection of identity of third persons, the EDPS recalls that the PFI acts as an advisory body and not as an investigative body[7]. Pursuant to Article 20 of the Regulation, it is therefore necessary to distinguish two situations in the context of the PFI's activities:

- The two rights at issue (access and rectification) cannot be restricted under Article 20(1)(a) of the Regulation, which provides in particular that such restriction constitutes a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences[8]. Article 20(1)(a) of the Regulation therefore does not apply to the PFI where the opinion of the PFI is given outside the context of an investigation by OLAF. However, in such situations, another restriction based on Article 20 of the Regulation might apply, for example when considering the protection of the rights and freedoms of others (Article 20(1)(c) of the Regulation). In such cases, the PFI needs to conduct a case-by-case analysis.

- Where the PFI considers that a case falls within the competence of OLAF, as referred to in Article 76(1) of the Rules of Application of the Financial Regulation and Article 6 of Decision No 43-2007, it must transmit the case-file and immediately inform OLAF. This means that exceptions to the rights of access and rectification must be based on the possible impact on future *OLAF* investigations. This interpretation is consistent with the restriction provided for in Article 20(1)(a) of the Regulation, given that it is not the PFI that

[6] Guidelines concerning the processing of personal data in administrative inquiries and disciplinary proceedings by European institutions and bodies, p. 4.
[7] See similar considerations in EDPS Opinion of 26 September 2012 in case 2012-0533.
[8] The interpretation of the EDPS also concerns administrative investigations and disciplinary cases.

investigates, but OLAF and, under such circumstances, it is for OLAF to determine whether or not to maintain such restriction.

3.7. Information given to data subjects

Articles 11 and 12 of the Regulation provide for information to be given to data subjects to ensure the transparency of the processing of personal data. When the data has not been obtained from the data subject, the information must be given when the data is first recorded or disclosed, unless the data subject already has it (Article 12 of the Regulation).

The EDPS notes that the Decision as well as the Rules of Procedure themselves contains some of the pieces of information required under Articles 11 and 12 of the Regulation.

- The EDPS further notes that, according to the notification, at the opening of an evaluation by the PFI, the PFI informs the **person concerned** of the objective of the evaluation procedure, why the PFI examines the facts, to whom the final report will be transmitted, her/his rights to access, eventually to rectify the data concerning her/him, the legal basis, the time period the data will be retained and stored and the right to contact the ECA's DPO and the EDPS at any time. However, Article 12(1) of the Rules of Procedure only stipulates that the PFI invites the person concerned to submit comments within 15 days; it does not contain any reference to the additional pieces of information listed above.
- The notification also does not refer to any information given to **other data subjects, i.e. witnesses and PFI members**.

The EDPS consequently recommends drafting a privacy statement containing all pieces of information required under Articles 11 and 12 of the Regulation and complementing Article 12 of the Rules of Procedure with a reference to it so as to ensure that every data subject receives it when the data is first recorded or disclosed.

3.8. Security measures

(...)

4. Conclusions

The EDPS considers that there is no reason to believe that the procedure is in violation of Regulation (EC) No 45/2001, provided the ECA fully takes into consideration the above considerations. In particular, the ECA should:

- include a reference to the right of the person concerned to comment on the facts mentioned in the draft final report in the Rules of Procedure;
- establish rules to safeguard the rights of other data subjects under Articles 13 and 14 of the Regulation by stipulating them in the Rules of Procedure;
- remind each of the recipients that they should process the personal data they receive only for the purpose for which they were transmitted in accordance with Article 7(3) of the Regulation;

- draft a privacy statement containing all pieces of information required under Articles 11 and 12 of the Regulation and adding a respective reference in Article 12 of the Rules of Procedure so as to ensure that every data subject receives the privacy statement when his/her personal data is first recorded or disclosed.

Done at Brussels, 17 March 2014

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor