Opinion on a notification for Prior Checking received from the Data Protection Officer of EACI regarding the "*Analysis and transfer of information related to fraud to OLAF*".

Brussels, 14 March 2013 (Case 2012-0652)

1. Proceedings

On 30 July 2012, the European Data Protection Supervisor ("the EDPS") received a notification for prior checking within the meaning of Article 27(3) of Regulation 45/2001 ("the Regulation") concerning the "Analysis and transfer of information related to fraud to OLAF" from the Data Protection Officer ("the DPO") of the Executive Agency for Competitiveness & Innovation (EACI).

On 8 October 2012, the EDPS requested further information on the basis of the notification. The replies were provided on 11 and 22 November 2012. On 15 January 2013, EACI sent the EDPS additional information.

The draft Opinion was sent to the DPO for comments on 4 March 2013. The EDPS received a reply on 8 March 2013.

2. Facts

Purpose

EACI's operational departments are responsible for analysing and transferring information to OLAF and to the parent DGs by EACI's designated staff members. Such information relates to possible cases of financial irregularities and fraud concerning the management of E.U. funds on the basis of Article 12(2) of the Act of Delegation of 2 July 2007[1].

Data subjects

With regard to **internal cases**: temporary and contractual staff of the agency, staff not subject to the Staff Regulations (i.e interims) and members of the Steering Committee.

As to the **external cases**: beneficiaries of grant agreements or contractors under public procurement concluded with the EACI.

In both cases, they are allegedly connected with a suspicion of fraud, financial irregularity or conflict of interest.

[1] "*The Agency shall without delay pass on to the Commission and more particularly OLAF, in accordance with the specific rules applicable, information on any possible cases of fraud or corruption or any other illegal activity which comes to its attention and of any situation which may give rise to such cases*".

Legal basis

The legal basis of the processing consists of:

- Article 3(2) of the Decision of 15 July 2005 of the Steering Committee of the EACI "laying down internal rules to prevent fraud, corruption and any illegal activity detrimental to the Communities' interest", with regard to internal cases;
- Article 12 of the Act of Delegation of 2 July 2007, with regard to internal cases;
- Articles 11(3) and 6(2)(c) of the Council Regulation No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes; and
- Article II.20.5 of the Council Regulation (Euratom, EC) N° 2185/96 and Regulation (EC) N° 1073/1999 of the European Parliament and the Council, with regard to external cases, notably grant agreements.

Procedure and data processed

In the framework of the management of grants and contracts, the EACI may encounter cases of possible financial irregularities. The Director, on his own initiative and on the basis of the Act of Delegation, may inform the Director General of OLAF of these cases. The latter decides whether or not to open an investigation on the basis of the information transmitted. It is ultimately the decision of the EACI's Director whether or not to transfer the data to OLAF.

Some examples of data processed in the context of **internal cases**, on a case by case analysis, are the following:

- name, address, e-mail, phone numbers, fax,
- CV,
- information on the conduct of the person giving rise to possible irregularities,
- appraisal reports and probationary reports. According to the information provided, such reports might contain relevant information for OLAF on the suspected conduct of the data subject. For instance, in case an accountant is suspected of misappropriating funds from the EACI, such reports may evidence that the staff member had dealt with the funds in question or had been put on probation for similar activity in the past.

Some examples of data processed in the context of **external cases** are the following:

- name, address, e-mail, phone numbers, fax,
- position within the entity,
- personal data contained in progress reports, interim and final reports in case of beneficiaries of grant agreements. For instance, if a beneficiary is suspected of double-financing by claiming staff costs for a staff member on an EACI project and at the same time claiming staff costs for the same hours that had been worked by that person on another EU project, it might be necessary to transfer information on the staff costs claimed in the reports,
- information on the conduct of the person giving rise to possible irregularities. In the above case of double-financing, the information to be transferred could be the position of the staff member held in the beneficiary companies, what the staff member did for those companies, where the person was geographically situated at the time that staff costs were claimed under both projects etc.,
- personal data concerning payments, such as pre-financing and recovery orders, in order to evidence payments made to beneficiaries who are suspected of fraudulent or illegal activity.

Recipients
According to the procedure, the legal officers of the EACI are in charge of analysing each case and drawing up the file which contains the data to be transferred to OLAF.

The file is then transferred to the hierarchy in the EACI (Head of HR/Unit/Director) for approval and then transferred to the legal officers of OLAF and to their hierarchy (Director General).

Other recipients could be the EACI's Steering Committee and internal auditors, if their role is deemed necessary in order to interject in the work of the EACI and parent DGs.

The Steering Committee is made up of representatives of each parent DG of the Commission and is informed by way of report, by the Director of the follow up of cases notified to OLAF[2]. The report is anonymous and the data disclosed are the following: the programme to which the notification to OLAF refers to, information on dates, such as the date of communication to OLAF, as well as a short summary of the main facts of the case in question. EACI pointed out that the purpose of the information is not to include data that could help identify possible data subjects involved in the case.

Rights of access and rectification and right of information
According to the notification, data subjects may exercise their rights according to the OLAF procedures in place and they are directly informed by OLAF in accordance with its privacy statement.

EACI does not provide data subjects with a privacy statement.

Furthermore, the notification states that in both internal and external cases, "pursuant to Article 20(1) (a), (b) and (e) of the Regulation, the data subjects should not, in principle, be informed by the agency about the processing operations".

Retention policy
The notification states that data are kept for 5 years after the closure of the case by OLAF. This means in case OLAF decided:

- not to pursue any investigation,
- to dismiss the case after investigation and
- to close the case after pursuing investigation and taking action.

Security measures
Data are stored on computer's drives with no possibility of access to unauthorised persons. Files are kept in locked cupboards.

3. Legal aspects

3.1 Prior checking

Applicability of Regulation 45/2001 ("the Regulation"): The processing of data under analysis constitutes a processing of personal data ("*any information relating to an identified*

[2] According to Article 6(2)(c) of Council Regulation No 58/2003 of 19 December 2002 executive agencies may gather, analyse and transmit to the Commission all the information needed to guide the implementation of a Community programme.

or identifiable natural person" (Article 2 (a) of the Regulation). The data processing is performed by an agency of the European Union, EACI, in the exercise of activities which fall within the scope of EU law[3]. The processing of the data is both manual and automatic, since data are kept in physical files and on the computer's drives.

Grounds for prior checking: Article 27 (1) of the Regulation subjects to prior checking all "*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*" by the EDPS. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

According to Article 27(2)(a) of the Regulation "*the processing of data relating to suspected offences, offences, criminal convictions or security measures* " is subject to prior checking by the EDPS; it is the case here as the data processed by EACI and eventually transferred to OLAF and to the parent DGs, concern alleged information on fraud and financial irregularities which may, in principle, lead to offences and criminal convictions, hence within the scope of Article 27(2)(a) of the Regulation.

Furthermore, the EDPS notes that EACI, in the context of its reports on alleged frauds and financial irregularities, processes and evaluates various personal aspects related to the data subjects, namely with a view to assessing whether their conduct might constitute fraud. The notification therefore falls also under Article 27.2(b) of the Regulation which concerns processing operations *"intended to evaluate personal aspects relating to the data subject, including his or her (...) conduct*".

The notification also indicates Article 27(2)(d) of the Regulation, since in case OLAF concludes the existence of fraud by a staff member of the EACI, this might exclude the extension of his/her contract. The EDPS considers that the purpose of the processing is to evaluate the conduct of a staff member in order to avoid financial irregularities and to ensure sound management of the agency. The purpose is not to exclude the suspected data subject, who is subject to such evaluation, from a right, benefit or contract and hence the processing does not fall within the scope of Article 27(2)(d) of the Regulation. The EDPS therefore recommends that EACI erases this provision from the notification under analysis.

Ex-post prior checking: 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, the EDPS regrets that the processing operation has already been established prior his prior-checking Opinion. However, the EDPS underlines that all his recommendations given in the present Opinion should be duly implemented in all future processing operations carried out by EACI.

Notification and due date for the EDPS Opinion: The notification of the DPO was received on 30 July 2012. According to Article 27 (4) of the Regulation, the EDPS Opinion must be delivered within a period of two months. The procedure was suspended for a total of 99 days for further information from the controller and four days for comments. Consequently, the present Opinion must be delivered no later than on 14 March 2013.

[3] The concepts of "Community institutions and bodies" and "Community law" can not be any longer used after the entry into force of the Lisbon Treaty on 1st December 2009. Article 3 of Regulation 45/2001 must therefore be read in light of the Lisbon Treaty.

3.2 Lawfulness of the processing

According to Article 5 of the Regulation, data may be processed only on one of the grounds specified.

Of the five grounds listed in Article 5, the processing under analysis satisfies the conditions set out in Article 5(a) of the Regulation, to the effect that data may be processed if '*processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities* (…)'. Furthermore, paragraph 27 of the preamble to the Regulation, states that "*Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies*".

In the present case, **the legal basis** for the processing is found in the provisions of the legal instruments indicated in the facts.

The processing of personal data under analysis is considered by EACI as **necessary** in order to inform OLAF and the parent DGs about alleged fraud and financial irregularities and hence ensure the sound financial management of the EU funding managed by the EACI.

3.3 Processing of special categories of data

Considering that EACI may process information related to offences, criminal convictions and security measures, the EDPS recalls the application of Article 10(5) of the Regulation which establishes that *"[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor."* In the present case, the processing of these data is authorised by the legal instruments mentioned in the facts.

3.4 Data Quality

Adequacy, relevance and proportionality: According to Article 4(1)(c) of Regulation 45/2001, personal data must be "*adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed*". It should therefore be verified that the data collected are relevant in relation to the purpose for which they are being processed.

Although certain standard administrative data, such as name and contact details, are always present in a file of a suspected data subject, the EDPS acknowledges that there is no systematic rule regarding the nature of data which can be included in the report to be prepared for OLAF and generally in the file; the precise content of a file will vary according to the purpose of the particular case.

However, concrete guarantees should be established in practice in order to respect the principle of data quality. The EDPS highlights that EACI should include in the file of a suspected data subject, only information which is relevant and proportionate having regard to the purpose pursued. The EDPS therefore recommends that EACI instructs the persons in charge of drafting reports and setting up the files that they should only collect and further process necessary and proportionate data to the purpose of the processing under analysis.

Accuracy: Article (4)(1)(d) of the Regulation provides that data must be *"accurate and, where necessary, kept up to date*". According to this Article, "*every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified*".

In the present case, the rights of access and rectification are not available to the data subjects by the EACI, but only by OLAF after it receives the report. This means that data subjects are not given the possibility to ensure that their file is accurate and complete in the framework of the processing under analysis, before the transfer to OLAF. It follows that EACI should take every reasonable steps in order to ensure that the data subjects' data are accurate and updated in conformity with Article 4(1)(d) of the Regulation, for instance by granting them their rights of access and rectification (see also section 3.7 on "the right of access and rectification").

Fairness and Lawfulness: Article (4)(1)(a) of the Regulation provides that personal data must be *'processed fairly and lawfully'*. The lawfulness of the processing has already been discussed in section 3.2 of this Opinion. As to fairness, this is linked to the information that must be provided to the data subject (see section 3.8 on "the right to information").

3.5 Conservation of data

Article 4 (1)(e) of Regulation 45/2001 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 EDPS notes that EACI keeps all data processed for 5 years after the closure of the case by OLAF, in all three possible scenarios, namely when OLAF decided:

- not to pursue any investigation,
- to dismiss the case after investigation and
- to close the case after pursuing investigation and taking action.

The EDPS notes the 5-year-retention period in all three scenarios is considered as as reasonable in light of the Financial Regulation's obligations and hence Article 4(1)(e) of the Regulation.

Nevertheless, the EDPS invites EACI to set up a necessary and proportionate retention period for the data related to cases which are analysed within EACI and they are not in the end transferred to OLAF on the basis of the Director's final decision.

3.6 Transfer of data

Articles 7, 8 and 9 of the Regulation set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made (i) to or within E.U. institutions or bodies (based on Article 7), (ii) to recipients subject to Directive 95/46 (based on Article 8), or (iii) to other types of recipients (based on Article 9).

Internal transfers

In accordance with Article 7(1), EACI is required to verify both that all the recipients possess the appropriate competences and that the transfer of the personal data is necessary to the performance of the related tasks.

In the present case, there is a data transfer within the EACI, namely to the Head of HR, Head of Unit and internal auditors. Each recipient has its own specific competence and the data transferred to each one appear to be necessary to the lawful performance of their tasks.

Furthermore, there is a transfer from EACI and the representatives of each parent DG of the Commission, which compose the Steering Committee. EACI is bound by Article 6(2)(c) of Council Regulation No 58/2003 of 19 December 2002 for such transfer. The EDPS notes that the data transferred, as indicated in the facts, could impliedly lead to the identification of suspected data subjects, in particular through the description of the summary of facts. Consequently, the EDPS recommends that EACI verifies on a case by case basis that only the strictly necessary data are transferred to the representatives of the Steering Committee in accordance with the performance of their tasks.

As to the transfer from the EACI to OLAF, the above requirements on internal transfer under Article 7(1) are fully applicable and the EACI should apply them after careful assessment, on a case by case basis.

In order to ensure the full compliance with Article 7 of the Regulation, the controller should remind all recipients of their obligation not to use the data received for other purposes than the one for which they were transmitted, as it is explicitly stated in Article 7(3) of the Regulation. The EDPS therefore recommends that EACI prepares confidentiality declarations to be signed by all the above recipients before a specific transfer of data takes place in conformity with Article 7(3).

3.7 Rights of access and rectification

Article 13 of the Regulation provides for the principle of the right of access to the data – and the procedures thereof – at the request of the data subject. Article 14 of the Regulation provides for the data subject's right of rectification.

According to the notification, data subjects may exercise their rights of access and rectification according to the OLAF procedures.

The EDPS recalls that the EACI is the controller of the data processed in the present case until the transfer to OLAF takes place, if the EACI's Director decides so. Hence the obligation to grant data subjects their rights of access and rectification in relation to the data processed in the present case is incumbent on EACI in the first place and the latter should put in place the appropriate procedures. EACI should also take into consideration that apart from the data subjects described in the facts, there might be other categories of data subjects, who could request to exercise their rights of access and rectification, namely whistleblowers, informants or witnesses. These other potential data subjects should also be included in the notification.

It might however be the case that EACI decides to restrict the application of Articles 13 and 14, where such restrictions constitute a necessary measure under Article 20(1)(a-e) of the Regulation. The EDPS underlines that any exceptions to the rights of access or/and rectification of data subjects should be strictly applied in light of the necessity of such a restriction and they should be balanced in relation to the right of defence.

In light of the above, the EDPS recommends that the EACI guarantees all data subjects including whistleblowers, informants and witnesses their rights of access and rectification. EACI should therefore adopt procedures, which specify that,
data subjects' right of access,

- may be restricted within the limits of the possible exemptions set out in Article 20 of the Regulation. EACI should ensure that these exceptions are strictly applied in light of necessity and are balanced in relation to the right of defence; and data subjects' right of rectification,
- if it is not restricted under Article 20, it may be guaranteed by, for example, having the possibility to add their comments in view of keeping their file accurate and updated.

3.8 Information to the data subject

Articles 11 and 12 of the Regulation relate to the information to be given to data subjects in order to ensure transparency in the processing of personal data. These articles list a series of compulsory and optional items of information. In the present case, some of the data are collected directly from the data subject and other data from other sources.

EACI stated in the notification that it does not provide data subjects with a privacy statement. Furthermore, the notification states that in both internal and external cases, "pursuant to Article 20(1) (a), (b) and (e) of the Regulation, the data subjects should not, in principle, be informed by the agency about the processing operations".

The obligation to inform all data subjects is incumbent on EACI, since it is the controller of the data processed in the context of the present notification, before they are transferred to OLAF, if the agency's Director decides so. It follows that EACI should communicate to all data subjects a privacy statement which should provide all relevant information in compliance with Articles 11 and 12 of the Regulation.

As it might be the case that the rights of access and rectification are restricted (see point 3.7), it might be also necessary to restrict the data subjects' right to be informed under Article 20(1)(a-e) of the Regulation. Any restriction under Article 20(1)(a) should not however be absolute, as it should be based on justified reasons. Article 20(3) of the Regulation provides that if a restriction is imposed, "the data subject shall be informed [...] of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the EDPS".

In some specific circumstances, however, it might be necessary to defer from Article 20 (3), so that the process of the inquiry will not be harmed, as Article 20 (5) provides. The EDPS underlines that any decision for such deferral should be strictly taken on a case by case basis. The decision to defer the information to data subjects in specific cases should be adequately justified and documented in the light of Article 20 of the Regulation.

3.9 Security Measures

According to Article 22 of the Regulation concerning the security of processing, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected"*. These security measures should in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

After review of the security measures described in the notification, there is no reason to believe that the measures implemented by EACI do not comply with Article 22 of the Regulation.

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation, provided that the following considerations are taken into account. In particular, EACI should:

- instruct the persons in charge of drafting reports and setting up the files that they should only collect and further process necessary and proportionate data to the purpose of the processing under analysis;

- put in place a procedure in order to ensure that the data subjects' data are accurate and updated in conformity with Article 4(1)(d) of the Regulation;

- set up a necessary and proportionate retention period for the data related to cases which are analysed within EACI and they are not in the end transferred to OLAF on the basis of the Director's final decision;

- verify on a case by case basis that only the strictly necessary need-to-know data are transferred to the representatives of the Steering Committee in accordance with the performance of their tasks;

- apply the requirements on internal transfer under Article 7(1) before any transfer to OLAF, after thorough assessment, on a case by case basis;

- prepare confidentiality declarations to be signed by all potential recipients before a specific transfer of data takes place in conformity with Article 7(3);

- include in the notification other potential data subjects, such as whistleblowers, informants or witnesses;

- put in place procedures in order to guarantee the rights of access and rectification of all potential data subjects, specifying the restrictions under Article 20 of the Regulation, as it is analysed in point 3.7;

- communicate to all data subjects a privacy statement which should provide all relevant information in compliance with Articles 11 and 12 of the Regulation;

- inform data subjects that their right to information may be restricted in certain cases in light of Article 20 (1) (a-e) of the Regulation. However, the controller should inform the data subject of the principal reasons on which the application of the restriction is based as well as of his/her right to have recourse to the EDPS under Article 20 (3). Any decision for any deferral to this provision should be taken strictly on a case by case basis.

Done at Brussels, 14 March 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor