Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on "follow-up" data processing operations (disciplinary, administrative, judicial, financial)

Brussels, 26 March 2007 (Cases 2006-544, 2006-545, 2006-546, 2006-547)

1. Proceedings

On 1 December 2006, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the European Anti-Fraud Office ("OLAF") five notifications for prior checking (hereinafter "notifications"). The five notifications refer to the following data processing operations: *(i)* Follow-up master, *(ii)* Judicial follow-up, *(iii)* Disciplinary follow- up, *(iv)* Administrative follow-up, *(v)* Financial follow-up.

The decision to submit this set of data processing operations for prior checking all at once was previously discussed and agreed upon by the EDPS and OLAF's Data Protection Officer (hereinafter "DPO") in the light of their similarities. It was considered that if the EDPS had simultaneous access to the information regarding the five data processing operations, it would facilitate his analysis of each individual prior checking notification.

Further to the receipt of the five notifications, the EDPS considered that the notification submitted for prior checking entitled "Follow-up master"[1] was not in itself a data processing operation but rather a summary of common aspects present in the other notifications. Accordingly, on 12 December 2006 the EDPS communicated to OLAF'S DPO that this notification was not subject to prior checking.

The EDPS decided to analyze four individual follow-up notifications jointly, in a single prior check opinion (Judicial follow-up, Disciplinary follow- up, Administrative follow-up, Financial follow-up). This was feasible because the four data processing notifications all refer to follow-up courses of action, which normally take place subsequent to the closure an investigation, and also because of their similarities in terms of the type of processing operation and nature of the personal data involved.

On 20 December 2006, the EDPS made a request for further information to which he received the responses on 10 January 2007. The procedure was suspended during this period. The procedure was suspended again on 9 February until 5 March to allow comments from OLAF's DPO. The procedure was suspended a third time on 7 March until March 15 to request clarification about certain factual information.

[1] Case 2006/0543.

2. Examination of the matter

2.1 The facts

Background information

An investigation carried out by OLAF may have various phases or stages. Within the *first stage*, OLAF assessors evaluate the initial information received. At the end of this stage, the OLAF Board recommend whether a case should be opened or not. If the answer is positive and is agreed upon by OLAF, then, the *second phase* starts with the formal decision to open an investigation and continues with the investigation itself[2]. At the end of the investigation, OLAF adopts a report with the findings of the investigation, namely whether the case should be closed with or without follow-up actions. In the latter case, the report includes recommendations for follow-up actions and the steps to be taken in the follow-up stage. Within the *third phase*, OLAF's follow-up team carries out various activities designed to ensure that the competent Community and/or national authorities have executed the measurers recommended by OLAF. The types of follow-up actions may include administrative, disciplinary, financial, or judicial. At the end of this stage, a closure of follow-up stage report is drafted setting forth the results obtained within this third stage[3].

The four data processing operations submitted to the EDPS for prior checking are carried out within the third stage of OLAF investigations, the so called "follow-up phase". In particular, each notification describes data processing operations carried out in specific domains where follow-up actions may take place, including administrative, disciplinary, financial, and judicial.

Purpose of the data processing operations

Generally speaking, it can be said that the overall purpose of the data processing operations carried out in the four domains is to ensure the proper execution of OLAF recommendations reached in the investigation phase. More specifically, the purpose of the processing operations carried out in each domain is as follows:

Data processed to carry out Judicial-follow-up: The purpose of the processing is to ensure that national judicial authorities are aware of the perpetration of a possible criminal act and to ensure that the case is investigated and possibly prosecuted.

Data processed to carry out Administrative follow-up: The purpose of the processing is to ensure that national administrative authorities or Community organs execute Community policies and law, including (i) specific measures to remedy fraud, irregularities or other illegal activity in specific cases and, (ii) more general measures such as ensuring that all the appropriate notifications have been made by the national authorities to the Commission services.

Data processed to carry out Disciplinary follow-up: The purpose of the processing is to ensure that the case is referred to the appropriate EU authorities, particularly DG ADMINISTRATION and the disciplinary services of the other Community organs for

[2] On 23 June 2006, the EDPS issued a prior check opinion on OLAF internal investigations (Case 2005-418).The Opinion assesses the respect to Regulation 45/2001 as far as the data processing operations that take place in the assessment and investigation phases of internal investigations.

[3] Occasionally, at an early stage of the investigation, OLAF may have findings of serious irregularities/serious administrative errors, which requires taking safeguarding measures. In such cases, OLAF opens a "follow-up path" while the investigation is still ongoing, which allows the follow up agents, together with the investigator where appropriate to assist the Authorising Officer to take the relevant measures.

appropriate disciplinary action. Often, the purpose will also include ensuring that proceedings are initiated under Article 22 of the Staff Regulations for the recovery of funds from the officials/other servants guilty of deliberate misconduct or gross negligence.

Data processed to carry out Financial follow-up: The main purpose of the processing is to ensure that national authorities and Commission services carry out the necessary steps to recover the sums due.

Responsibility for the data processing carried out within the scope of the four notifications for prior checking

Once an investigation is closed with a recommendation for follow-up action, responsibility for the follow-up stage moves from the investigation team to the various follow-up teams which exist within OLAF. The actual team responsible will depend on the type of follow-up action recommended (judicial, administrative, disciplinary or financial). For example, the follow up teams of Unit C1 are responsible for judicial and disciplinary follow-up actions; the follow up teams for financial and administrative follow-up are the teams of Units C2 and C3.

Accordingly, the data controller for data processing operations that take place with the purpose to carry out judicial and disciplinary follow-up is Unit C1 and the data controller for the data processing operations that take place with the purpose to carry out financial and administrative follow-up is Directorate C.

Description of the automated data processing operations carried out in the context of the four types of data processing operations

The data processing operations carried out in the context of the follow-up actions are both manual and automated. The automated operations use mainly the Case Management System and the Administration and Registration System, which are further described below.

Use of the Case Management System and Basic Content. OLAF uses a central database referred to as the Case Management System (hereinafter "CMS") to manage all OLAF's operational cases.

From the first moment when information about an alleged wrongdoing is discovered or passed on to OLAF for initial assessment, it is assigned a number referred to as Operational File. This number will be attached to the case, through its different phases, assessment, investigation and follow-up. All significant events concerning a case which take place during the various stages are recorded in the CMS[4].

Once an investigation is closed with a recommendation for follow-up action, a follow-up agent/s is appointed as responsible for a given case. The access rights to CMS are determined according to the following rules: (i) Access rights to the CMS are assigned to the appointed follow-up agent/s. (ii) As a matter of rule, access rights are assigned on an individual basis according to the responsibility and function of the agent concerned, based on the "need to know

[4] In particular, information stored in CMS may include the following: (a) Significant events, administrative information and intelligence. The supporting research and analyses may be stored in a secure "ibase environment" or on the OLAF secure server linked by reference to the CMS file. (b) All registered documents relating to a case are scanned and added to the CMS case file by means of the electronic document management system. (c) Where relevant case information is held in unstructured formats (e.g. hard drives which have been seized from a computer during an OLAF investigation), a reference to its existence will be noted in the CMS and the data from such files are made available to the investigator or person associated with the case. When OLAF receives information which clearly falls outside the competence of OLAF (prima facie non-cases), then the case appears in the CMS as closed.

principle". (iii) In line with the above principles, follow up agent/s competent for a given case are given read/write access to all follow-up stage documents contained in the CMS. This includes case reports (final case report and dissemination sheet[5]), evidence and closure reports[6] as well as the follow-up recommendations report and the lessons learnt sheet[7]. Access will also be granted to correspondence exchanged with or sent to the national authorities, Commission service and other institutions. The agent/s will only have read access to investigation details. (iv) Each follow-up agent is responsible for updating the system in a timely manner and monitoring the completeness of details and documentation for the case for which he/she is responsible.

During this phase, the team responsible for the investigation during the preceding phase is given an observer status by virtue of which they can read the documents related to the case. In certain cases, during the investigation phase, the follow-up team is already given access rights to the information contained in CMS in order to allow this team to assist the investigators.

The *Administration and Registration System ("ARS") and Basic Content*. The Administration and Registration System contributes to the overall purpose pursued by the follow-up phase. It is an MS Access database for OLAF cases which are transferred from the operational/investigation Units to the follow-up units. ARS is managed by the follow-up units, for their own internal use. Analyses, statistics and reports for the follow-up units can be produced automatically from it.

ARS contains case-related information (CMS official number, case type, officer in charge, unit, sector, title, etc.) for internal registration purposes.

Description of the manual data processing operations carried out in the context of the four types of data processing operation

Follow-up agents may keep their own working files for the cases assigned to them, containing only copies of documents, while the follow-up is ongoing. The OLAF Greffe Registry maintains the official cases in paper form in a uniform manner, in compliance with the Commission Decision on Document Management.[8]

When the follow-up phase is closed, the follow-up agent hands over all case-related documents to the Greffe. The Greffe staff will compare the two sets of files (i.e., the original and the copies) in order to ensure that the Greffe file is complete and mirrors the information recorded in the CMS.

Where necessary, the follow-up team can have direct access to the original documents of a given file, created during the investigatory phase.

[5] The final report presents the findings and conclusions of the investigation; the dissemination sheet specifies the competent Member State/Community authorities to whom the final case report should be disseminated.
[6] The closure note signifies that the case is closed, either with or without follow-up.
[7] The Follow-up recommendation report specifies the type of follow-up action, the steps to be taken in the follow-up phase of the case, and any information useful to the follow-up team. It may contain details of the exact amount to be recovered and from whom. The Lessons learnt sheet summarises the lessons that can be drawn from the experiences during the case and recommends actions to be taken based on these experiences.
[8] Commission Decision 2002/47/EC, ECSC, Euratom, OJ L 21, 24.1.2002, p. 23.

Data subjects involved in the context of the four types of processing operations

According to the notification forms, the types of data subjects whose data are processed in the context of the four types of data processing operations are very similar and consist of the following:

(i) personnel of the EU institutions, bodies, offices and agencies who are *the subject* of the follow-up actions that follow an investigation, including officials, temporary agents, national experts.

(ii) persons outside of the EU institutions, authorities, bodies, offices and agencies who are *the subject* of follow-up actions that follow investigations.

(iii) persons inside and outside of the EU institutions, bodies, offices or agencies who may be involved in the matters under investigation, either as whistleblowers, informants or witnesses.

(iv) persons *inside and* outside of the EU institutions who may be involved in the matters underlying follow-up activities not covered by the categories listed above, such as Community and national civil servants, subcontractors, managers, employees and citizens.

Categories of personal data

According to the notification forms, the type of personal data processed in the context of the four types of data processing operations is very similar and consists of the following:

(i) Typically identification data such as surname, forename, nickname, date and place of birth, address, telephone number and private e-mail address.

(ii) Professional data, including the profession, organisation where the data subjects carries out his/her profession, function, telephone number, fax number, professional e-mail address.

(*iii)* Information concerning activities related to matters which are the subject of follow-up activities. This includes statements made by the person regarding events investigated and which are the subject of follow-up actions, statements made about the person regarding events investigated and which are the subject of follow-up actions, evidence mentioning the person and notes regarding the relation of the person to the events which are the subject of follow-up. In this regard, the following reports must be completed in the context of the follow-up stage and included in CMS: (i) "Follow-up developments", which is completed whenever there are significant developments in the follow-up phase; (ii) "Proposal for a new follow-up path", whenever new information gathered during the follow-up phase gives rise to actions other than or in addition to those recommended in the final case report/follow-up recommendations report; and (iii) "Closure of follow-up stage", which sets out the conclusions of the follow-up stage and the results obtained.

The notification forms submitted to the EDPS specify that special categories of data[9] are not processed in the context of OLAF follow-up actions. The EDPS has been informed that only very exceptionally there may be *ad hoc* circumstances where, due to the subject matter under investigation, such data may be processed.

[9] Special categories of data are those referred to in Article 10.1 of Regulation (EC) No 45/2001.

Conservation of data

OLAF may keep both electronic and paper files relating to follow-up actions for up to 20 years after the date on which the follow-up has been completed.

Transfers of data

According to the four notifications, data may be transferred to the following entities:

(i) To concerned Community institutions, bodies, offices or agencies in order to allow them to take appropriate measures to protect the financial interests of the Community.

(ii) To competent Member State authorities, judicial and administrative in order to allow them to take appropriate follow-up measures.

(iii) To competent third country authorities and international organisations in order to ensure an appropriate follow-up and to maximise the protection of the financial interests of the EU.

Types of information that may be transferred include:

The information transferred to Member States may vary slightly, depending on the type of follow-up action.

Regarding judicial and disciplinary follow-up, at the end of the investigation phase with follow-up actions, a "Final Case Report" is sent to Judicial/disciplinary authorities. The transfer of this report entails the disclosure of the most important elements of a given file. Afterwards, in the context of the follow-up stage, additional complementary information may be sent to the same authorities. For example, OLAF may provide judicial/disciplinary authorities with additional documents or information contained in the OLAF file or received from other concerned services of the Commission or the EU institutions. This would normally be done in response to a request from the judicial authority for further documentation related to its investigation/prosecution. Thus, a broad variety of types of documents could be involved.

Information regarding administrative and financial follow-up is not usually requested by or given to national judicial authorities. However, OLAF can provide other competent national authorities and/or competent Commission services, as appropriate, with additional documents or information contained in the OLAF file which had not been forwarded to such an authority or service with the "Final Case Report". Examples of such documents include audit and mission reports, details about the identified debtors, explanation of the amount to be recovered, calculation of interest etc. This can be done either in response to a request by the authority or service concerned, or spontaneously by OLAF when the follow-up team believes the provision of such information or documentation could be of assistance.

Data subjects' rights to information, access and rectification

As far as the right to information is concerned, OLAF has created standard information notices to be provided to individuals from whom personal data are collected, including, individuals who are the subject of follow-up activities. The information notice is provided to individuals when personal data related to them are recorded or no later than when such data are first disclosed to third parties, unless one of the exceptions specified in Article 20 is applicable. Similar procedures exist regarding informants, whistleblowers and witnesses. OLAF is still assessing how to comply with this obligation as far as individuals who do not fall within the above categories (i.e., persons who are not the subject of the investigation, informants,

whistleblowers and witnesses) and whose personal data may be included in investigation and follow-up investigations.

In order to make sure that OLAF investigators provide the relevant information notices to data subjects, the Director General of OLAF has provided guidance to investigators regarding the procedure to follow to inform individuals (document entitled "Instructions to staff conducting investigations following an opinion of the EDPS", hereinafter "OLAF Instructions to Investigators"). The OLAF DPO has provided a copy of this document and the information notices addressed to data subjects to the EDPS for comments.

The Instructions to Investigators foresee the possibility for OLAF to withhold information if it would be harmful to the investigation. OLAF Instructions foresee that such restrictions can only be applied when necessary, on a case-by-case basis. On each occasion that a restriction on the right of information is imposed a note to the file will be drafted specifying the reasons for imposing the restriction. A standard form has been drafted towards this end. Furthermore, the data subject will be subsequently informed of the reasons for the imposition of the restrictions and of his right to have recourse to the EDPS, unless it would be harmful to the investigation to provide this information.

Regarding the right of access and rectification, OLAF has informed the EDPS that it has put a procedure in place to react to access requests from data subjects. To this end, OLAF has created a form to be used by OLAF investigators and follow up agents in response to access requests received from data subjects. The Director General of OLAF has sent instructions to OLAF staff conducting investigations about such procedures (note referred above entitled " OLAF Instructions to Investigators").

OLAF Instructions to Investigators foresee the possibility for OLAF to deny access if (a) it would be harmful to the investigation and (b) if it would be harmful to the right and freedoms of others. In this case, OLAF has informed the EDPS that it will grant access to the extent possible without revealing information of other individuals. OLAF Instructions to Investigators foresee that such restrictions can only be applied when necessary, on a case-by-case basis. On each occasion that a restriction to the right of access is imposed a note to the file will be drafted specifying the reasons for imposing the restriction. Also, the data subject will be subsequently informed of the reasons for the imposition of the restrictions and of his right to have recourse to the EDPS, unless it would be harmful to the investigation to provide this information.

The EDPS understands that whereas OLAF Instructions to Investigators were provided to Investigators following the EDPS prior checking Opinion on OLAF internal investigations, the procedures set forth in the Instructions are relevant for the processing of personal data carried out by other staff, including follow up agents. The OLAF DPO has confirmed the application of OLAF Instructions to all staff, including follow up agents.

2.2 Legal aspects

2.2.1 Prior checking

Presence of the elements that trigger the application of Regulation (EC) No 45/2001

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001") applies to the *"processing of personal data wholly*

or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system", and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law*".

For the reasons described below, the EDPS considers that all the elements that trigger the application of the Regulation exist in the four data processing operations notified for prior checking.

First, the EDPS notes that the four notifications for prior checking relate to the processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, the four notifications indicate that data of individuals such as first and last name, private and professional contact details as well as information concerning the potential involvement of individuals in wrongdoing activities are collected and further processed.

Secondly, the four notifications clearly point out that the data collected undergo "processing" operations, as defined under Article 2 (b) of the Regulation (EC) No 45/2001 which include the collection, recording, storage, consultation and use of personal data. Some of the operations are automatic, for example, those carried out through the use of the Case Management System. Others are carried out through a non electronic filing system as defined under Article 2 (c) of the Regulation (EC) No 45/2001, such as for example, the maintenance by the follow-up units of chronological files, containing paper copies of all the documents produced by follow-up units.

Finally, the EDPS confirms that the processing is carried out by a Community institution, in this case by OLAF, the European Anti-Fraud Office, which is part of the European Commission, in the framework of Community law (Article 3.1 of the Regulation (EC) No 45/2001). Therefore, clearly all the elements that trigger the application of the Regulation exist in the four cases.

Assessment of whether the data processing operations fall under Article 27 of the Regulation

Article 27.1 of the Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject 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.

The EDPS considers that the four notifications submitted to the EDPS for prior checking clearly fall under Article 27.2. of Regulation (EC) No 45/2001.

In the first place, in the EDPS' opinion, such data processing operations fall under Article 27.2(a) of Regulation (EC) No 45/2001, which establishes that processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" shall be subject to prior checking by the EDPS. In the four cases in point, OLAF will process information about suspected offences and offences insofar as the scope of the processing may entail follow up investigations of alleged offences.

The EDPS considers that in some instances the four notifications may also fall under Article 27.2(b) of the Regulation (EC) No 45/2001 which stipulates that data operations which *"evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall be subject to prior checking by the EDPS. Whereas most of the evaluation of individuals will take place during the investigation phase, there may be instances where follow-up agents may

also be required to engage in analysis of information in order to evaluate whether the actions of individuals constitute illegal or unlawful behaviour, thus, triggering the application of Article 27.2(b).

Since prior checking is designed to address situations that are likely to present specific risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have already been established. This is not a serious problem as far as any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 1 December 2006. Complementary information was requested on 20 December, 2006. The answers were received on 10 January 2007. Pursuant to Article 27.4 of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended during such interval. The procedure was suspended again on 9 February until 5 March to allow comments from the DPO. The procedure was suspended a third time on 7 March until 15 March to request further clarification on certain factual information. The Opinion will therefore be adopted no later than 27 March 2007 (deadline was 2 February plus 53 days of suspension).

2.2.2 Lawfulness of the processing

Personal data may only be processed if grounds can be found in article 5 of Regulation (EC) No 45/2001.

As pointed out by the four notifications for prior checking, of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operations notified for prior checking fall under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001 three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out by OLAF, second, whether the processing operations are performed in the public interests and, third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

Relevant legal grounds in the Treaty or other legal instruments

In ascertaining the legal grounds in the Treaty or other legal instruments that legitimise the four follow-up processing operations notified for prior checking, the EDPS takes note of the following:

First, the four notifications refer to activities carried out following the closure of an investigation with recommendations for follow-up. The processing operations aim to implement OLAF recommendations reached at the end of the investigation. In this regard, the EDPS understands that the overall purpose of the processing actions carried out within the follow-up phase is the same as the purpose of the processing carried out within the earlier phase, the investigation phase. For this reason, it would appear that the legal instruments that legitimise the data processing carried out within the investigation phase also legitimise the processing carried out within the follow up phase. If the Treaties or other legal instruments establish OLAF's powers to engage in an investigation, logically such powers encompass the various phases of an investigation, from the initial assessment to the last phase or follow-up.

The EDPS has reviewed the legal grounds to legitimise internal investigations[10] and considers that such legal grounds may legitimise the data processing that takes place during the follow-up phase insofar as such processing pursues the same goals as those pursued by the investigation. For example, the processing of data in the context of administrative, judicial, disciplinary and financial follow-up actions related to *internal administrative investigations* is based on (i) Article 4 of Regulation (EC) No 1073/1999[11] and (ii) Article 2 of Commission Decision 1999/352 which sets forth the tasks of OLAF[12]. These instruments enable OLAF to carry out several actions towards combating fraud, corruption and other illegal activity adversely affecting the Community's financial interests. They also allow OLAF to investigate serious facts linked to the performance of professional activities which may constitute a breach of obligations by members, officials and servants of the Communities likely to lead to disciplinary and/or criminal proceedings.

In addition, applicable legislation expressly refers to actions that entail the processing of personal data which are likely to be taken within the scope of the follow up stage. Most of these actions consist of transfers of personal information from OLAF to relevant authorities. This is consistent with the general purpose of the follow-up stage which, as defined above, mainly intends to ensure that relevant national and Community authorities execute OLAF findings in order to prosecute and remedy fraud, irregularities or other illegal activities. Others foresee the recovery of sums due.

Disciplinary follow-up actions are foreseen in various legal instruments: Article 86 of the Staff Regulations[13] provides that any official who fails to comply with his obligations under the Staff Regulations shall be liable to disciplinary action, together with Annex IX, which specifies the procedures to be followed in disciplinary proceedings. Furthermore, Article 22 of the Staff Regulations provides for the recovery of funds from the officials/other servants guilty of deliberate misconduct (full reparation) or gross negligence (partial reparation), which concerns disciplinary but also financial follow-up investigations. The Memorandum of Understanding concerning a code of conduct is also relevant in order to ensure a timely exchange of information between OLAF and the Commission with respect to OLAF internal investigations in the Commission[14]. Particularly relevant is paragraph 7.1 which specifies that OLAF will promptly forward all final case reports concerning internal investigations to the Commission, and upon receipt, the Commission will take all appropriate actions and the Secretary General will report to OLAF's Director General on all such actions taken[15].

Some judicial follow-up actions are expressly referred to in Regulation 1073/1999. For example, Article 10 (2) of Regulation 1073/1999 establishes that OLAF must forward the information obtained by OLAF during internal investigations into matters liable to result in criminal proceedings to judicial authorities of the Member State concerned.

---

[10] See prior check Opinion of 23 June 2006 on OLAF internal investigations (Case 2005-418).

[11] Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), Official Journal L 136, 31/05/1999.

[12] Commission Decision of 28 April 1999 establishing the European Anti-fraud (OLAF) Office, Official Journal L 136, 31/05/1999.

[13] Council Regulation (EC, Euratom) No 723/2004 of 22 March 2004 amending the Staff Regulations of officials of the European Communities and the Conditions of Employment of other servants of the European *Communities,* OJ L 124, 27/4/2004.

[14] SEC (2003) 871.

[15] In this regard, the EDPS has prior checked the data processing operations relating to internal administrative inquires and disciplinary procedures within the European Commission, (Opinion adopted on 20 April 2005, Case 2004-187) and the operations of the Financial Irregularities Panel (FIP) (Opinion adopted on 15 March 2006, Case 2005-407).

The processing of data in the context of administrative, judicial, disciplinary and financial follow-up actions related to *external administrative investigations* is based on a variety of legal instruments. According to Article 3 of Regulation (EC) No 1073/1999, these instruments can be horizontal or sectoral. Examples of horizontal legal instruments providing legal bases for external investigations include Article 2 of Regulation 2185/96[16], in conjunction with Article 3 of Regulation (EC) No 1073/1999. Also, Article 2 (1) of the Commission Decision 1999/352 establishing OLAF provides that OLAF exercises the Commission's powers to carry out external administrative investigations for the purpose of strengthening the fight against fraud, corruption and any other illegal activity adversely affecting the Community financial interests as well as any other act or activity by operations in breach of Community provisions.

Furthermore, actions carried out in the context of external administrative investigations are also expressly referred to in Regulation (EC) No 1073/1999. For example, Article 9 which sets forth the requirements for preparation of a final case report and for forwarding the report to the relevant authorities, and Article 10, which sets forth the requirements for forwarding of information by OLAF to the relevant authorities.

Processing operations are carried out in the legitimate exercise of official authority

The EDPS notes that OLAF carries out the processing activities in the legitimate exercise of its official authority. Indeed, Articles 9 and 10 combined with Article 4 and 5 of Regulation (EC) No 1073/1999 confer upon OLAF the competence and the obligation to engage in investigations and ensure the effective implementation of their findings in cooperation with relevant national and Community authorities.

Necessity test

According to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above.

As far as follow-up actions are concerned, generally speaking, the EDPS presupposes that such necessity exists whenever OLAF has reached a decision to close a case with follow-up actions, in line with the standard procedures that apply to OLAF.

However, the EDPS notes that the real "necessity" of the data processing has to be analysed *in concreto*, for each particular follow-up case. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the follow-up actions has to be proportional to the general purpose of processing (combat fraud, corruption, etc) and to the particular purpose of processing in the context of the case under analysis. Thus, the proportionality has to be evaluated on a case-by-case basis.

2.2.3 Processing of special categories of data

The EDPS considers that it may happen that OLAF processes data related to offences, criminal convictions or security measures. In this regard, the EDPS recalls the application of Article 10.5 of Regulation (EC) No 45/2001 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

[16] Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15/11/1996.

case, processing of the mentioned data is authorised by the legal instruments mentioned in point 2.1.2 above.

As far as special categories of data are concerned, Article 10.1 of Regulation 45/2001 establishes that "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited*"

The four notifications for prior checking state that no data falling under the categories of data referred to in Article 10.1 are processed in the context of the four data processing operations notified for prior checking. Taking into account the overall purpose pursued by OLAF when it engages in data processing operations, the EDPS understands that the collection of special categories of data is not OLAF's intention.

However, the EDPS considers that in the context of OLAF follow-up investigations, OLAF may become, perhaps involuntarily, in possession of special categories of data, which will often be of no interest/relevance to the investigation. In this regard, the EDPS recalls the application of the data quality principle, according to which data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed (Article 4.1.c). Pursuant to this principle, if special categories of data that are not useful for the purposes sought by the follow-up actions are somehow "captured" in the follow-up files, they should be deleted or never collected in the first place. If they are captured in the context of other information that is relevant, the EDPS suggests that OLAF deletes this information from the file (or somehow makes it unreadable).

Nonetheless, if special categories of data are processed insofar as they are necessary for the purpose of the follow-up actions, such processing may be permissible under Article 10.2 (d) of Regulation 45/2001 according to which the processing of such data will not be prohibited if it is necessary for the "*establishment, exercise or defence of legal claims*".

2.2.4 Data Quality

As outlined above, pursuant to Article 4.1.c of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This is referred to as the data quality principle.

The EDPS notes the types of data that OLAF processes as stated in sections 17 and 18 of the four notifications for prior check. It is not possible for the EDPS to determine whether such data are appropriate in *all* cases. Whether such data are appropriate or not will depend on the particular follow-up case at stake. In order to ensure that follow-up agents process data in accordance with the data quality principle, the EDPS suggests considering the following:

First, certain types of data mentioned in the notification for prior checking, such as identification data, are certainly adequate for the purpose of the follow-up phase. As a general rule, this information will be relevant for all cases.

Second, from the factual information provided in the notifications for prior checking and in the OLAF manual it appears that a great deal of the data processed within the various types of follow-up stages originates from the investigation phase. In fact, once an investigation is closed with a recommendation for follow-up action, a follow-up team is given access to all follow-up stage documents contained in the CMS. The follow-up team uses this information for the purpose of ensuring that the recommendations are properly followed. In this context,

the EDPS appreciates the practice consisting of granting "read only" access to follow-up agents regarding investigation details as it appears that the scope of their functions does not require them to have more privileges.

Third, as far as the data collected directly by the follow-up team are concerned, the EDPS would like to recall the recommendations made in the context of the Opinion on a notification for prior checking on OLAF internal investigations, mainly the fact that only data that are necessary for the purpose of the follow up investigation must be collected or further processed.

Fourth, the EDPS welcomes OLAF's practice described above consisting of appointing a follow-up agent responsible for updating the system in a timely manner and monitoring the completeness of details and documentation for his case since this practice contributes to the correct application of the principle under analysis.

2.2.5 Conservation of data/ Data retention

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.*

According to the OLAF's Manual, once all appropriate measures have been taken and the follow-up of the case has been completed, a report entitled "Closure of Follow-up Stage" is created. The report sets forth the results obtained during the follow-up stage such as amounts recovered, administrative sanctions applied, fines, penalties and prison sentences imposed.

According to OLAF's notification, OLAF may keep both paper and electronic files relating to follow-up activities for up to 20 years after the date on which the follow-up has been completed, in other words, since the adoption of the Closure of Follow-up Stage.

The EDPS is concerned by the recording of investigation related information for such long period of time. Indeed if one takes into account that after the follow-up stage has been closed, all the possible measures have been carried out, amounts recovered and sanctions applied, the information is still kept for 20 years, it is difficult to comprehend the purposes for which the data are going to be used during such long period of time

The EDPS considers that the suggestion made in the context of OLAF internal investigations is relevant here as well. There, the EDPS suggested that when OLAF had been in existence for 10 years it should carry out a preliminary evaluation of the necessity of the 20 year period vis-à-vis the purpose of such a conservation frame, and that a second evaluation should be carried out when OLAF has been in existence for 20 years. Accordingly, the EDPS calls upon OLAF to perform the first assessment after 10 years of existence and inform the EDPS of its findings.

Furthermore, the EDPS recalls that if there is a need to keep the data for statistical, historical, scientific purposes, under Article 4(1)d of Regulation, OLAF is authorised to do so if it anonymises the data or if the data are encrypted.

2.2.6 Transfer of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 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 *ex* Article 7 to Community institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46 or to other types of recipients *ex* Article 9.

According to the notifications for prior checking, OLAF transfers personal information to three types of third parties, thus, triggering the application of Article 7, 8 and 9 of Regulation (EC) No 45/2001. This section will analyse data transfers covered by Article 7 and 8 of Regulation (EC) No 45/2001. It will not analyse data transfers covered by Article 9 of Regulation (EC) No 45/2001 (i.e., transfers of personal data to recipients other than Community institutions, and bodies, which are not subject to Directive 95/46/EC). This is because this issue is being dealt with in the context of case 2005-0154 and case 2006-0493, in the framework of which the EDPS analyses the conformity of OLAF international transfers taken as a whole with Regulation (EC) No 45/2001.

Transfers to Community institutions and bodies ex Article 7 of Regulation (EC) No 45/2001

The OLAF Manual as well as complementary information provided by the OLAF DPO refers to various provisions in legislation that foresee the transfer of personal information related to cases under the investigation and follow-up phases to Community institutions, bodies, offices or agencies, in order to allow them to take appropriate measures to protect the financial interests of the Community. For example, within the follow-up phase, the responsible follow-up agent contacts, among others, the authorising Directorate General, Directorate General Budget and the Commission's Legal Service to establish the status of implementation of the recommendations contained in the Final Case Report, to encourage them to take the necessary measures and if necessary, to assist them with the implementation of the recommendations.

The EDPS recalls that in addition to having legal grounds enabling OLAF to transfer the information, Article 7 of Regulation (EC) No 45/2001 requires that personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, OLAF must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. In other words, even if the transfer of information is foreseen in relevant legislation, such transfer is only lawful if it meets these two additional requirements.

Whether a given transfer meets such requirements will have to be assessed on a case by case basis. Accordingly, OLAF follow-up agents should apply this rule for each particular data transfer. Doing so will avoid unnecessary transfers of information as well as transfers of information to parties that do not have the appropriate competences. To ensure compliance with this rule, the EDPS suggests that OLAF puts in place a procedure whereby a note to the file is drafted establishing the necessity of the data transfers that have taken place or will take place in the context of a given case. The use of a single record, based on a form such as that developed by OLAF following the recommendations of the EDPS in the context of the consultation concerning OLAF's transfers of personal data to third parties, would also be appropriate for transfers under Articles 7 and 8. This will help follow-up agents to apply the rule and provide accountability. The EDPS suggests that OLAF provides guidance to follow-up agents on the application of this rule.

In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.

Transfers to competent Member State authorities subject to Directive 95/46/EC ex Article 8 of Regulation (EC) No 45/2001

Article 8 of Regulation (EC) No 45/2001 offers several legal grounds authorising the transfer of personal information. Given the circumstances of OLAF data processing, OLAF may avail itself of Article 8 (a) according to which personal data can be transferred if the data will be used to perform a task subject to public authority or if the data transfer is made in the data subject's legitimate interest. Whereas under Article 8 (a) of Regulation (EC) No 45/2001 it is up to the recipient to establish the interest, the EDPS understands this provision to mean that if the sending of the information is not carried out at the request of the recipient, is up to the sender to accredit such a need.

In accordance with the above, when the information is not sent at the request of the recipient, OLAF must accredit the necessity of the data transfer. In order to implement this rule, as suggested above regarding data transfers to Community institutions and bodies, the EDPS recommends that OLAF follow-up investigators use the same approach as under Article 7 of Regulation (EC) No 45/2001 and list in a reasoned opinion all the data transfers that will be carried out or have been carried out in the context of a case and describe their necessity.

These procedures should be communicated to OLAF staff.

2.2.7 Right of access and rectification

The EDPS considers OLAF's practice as set forth in OLAF's Instructions to Investigators regarding the right of access and rectification to be in line with Article 13 of the Regulation (EC) 45/2001. Generally speaking, the EDPS also considers that the restrictions foreseen by OLAF's Instructions to Investigators are in line with Article 20 of Regulation (EC) No 45/2001, which foresees various hypotheses where the right of access can be limited.

However, OLAF must be aware that the application of Article 20.1 (a) which enables OLAF to suspend access for the prevention/detection/prosecution of a criminal offence may not always apply in the context of follow-up phase, particularly when the matter at stake is neither criminal nor disciplinary. Furthermore, it would not be possible either to apply Article 20.1. (a) after the criminal investigation is closed and the individual has been charged with a criminal offence. It may be possible to apply it when the follow up phase has started before the investigation is closed[17]. The contrary would be against Article 6.3. (a) of the European Convention of Human Rights which recognises the right to be informed of the nature and causes of criminal accusations, although, this right may be temporarily suspended during the filing of interlocutory injunctions.

However, OLAF may rely on other sections of Article 20 of Regulation (EC) No 45/2001 to suspend access/rectification. For example, if OLAF considers that the suspension of access/rectification is necessary in order to safeguard an economic or financial interest of the Community or of the Member States, OLAF may be able to avail itself of the exception foreseen in Article 20.1.(c) according to which access can be denied where such restriction constitutes a necessary measure to safeguard "an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters". This exception will apply independently of the type of offence (criminal or other).

If OLAF uses an exception to suspend access, it should take into account that the restrictions to a fundamental right can not be applied systematically. OLAF must assess in each case whether

[17] See footnote number 3.

the conditions for the application of one of the exceptions, for example, Article 20.1.a, or 20.1 c or others may apply. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. For example, if OLAF wishes to rely on the exception of Article 20.1. (c) it must assess whether it is necessary to suspend access in order to safeguard an important economic interest. In making such assessment, OLAF must take into account that not because there is an economic interest at stake, there will invariably be a need to suspend access. In other words, there must be a clear link between the need to suspend access and the safeguard of an economic interest. Furthermore, OLAF should also recall that the exceptions to the data protection rights only apply temporarily "for as long as such information would deprive the restriction imposed by paragraph 1 of its effect" *ex* Article 20.5. of Regulation (EC) 45/2001. Finally, if OLAF uses an exception, it must comply with Article 20.3 according to which "the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor"

In addition to the above, the EDPS observes that OLAF's practice regarding access as set forth in OLAF's Instructions to Investigators is not reflected in the OLAF Manual. In fact, the Manual contains a statement that directly contradicts the Instructions: *"the interested party has no right of full access to the OLAF investigation file"*. The EDPS urges OLAF to revise the OLAF Manual as a far as this issue is concerned and bring it in line with OLAF's Instructions to Investigators mentioned above.

Furthermore, the issue of access to the personal data included in an investigation file is being considered in the context of the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No. 1073/1999 concerning investigations conducted by (OLAF). On 27 October 2006 the EDPS issued an Opinion on the Proposal for a Regulation amending Regulation (EC) No. 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF)[18]. The EDPS urges OLAF to take into account the considerations expressed in this Opinion as far as the right of access and rectification are concerned. The EDPS considers it important for the right of access and rectification to be expressly recognised by Regulation (EC) No. 1073/1999 in line with 13 of the Regulation (EC) 45/2001.

2.2.8 Information to the data subject

Pursuant to Article 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The EDPS considers that the information that OLAF foresees to provide to individuals as described in the Instructions to Investigators and related documentation is in line with Article 11 and 12 of Regulation (EC) 45/2001.

The OLAF Instructions to Investigators foresee the possibility for OLAF to withhold information if it would be harmful to the investigation. OLAF Instructions foresee that such restrictions can only be applied when necessary, on a case-by-case basis. As stated before regarding the right of access, during the follow-up stage, the EDPS considers that the

[18] Opinion of 27 October 2006 on the Proposal for a Regulation amending Regulation (EC) No. 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF).

possibility to deny access on the basis of "harm to the investigation" may be limited, although other exceptions such as Article 20.1.(c) may apply, subject to the safeguards described above under section 2.1.7.

Regarding the moment in time when the information will be provided, the EDPS recalls that individuals should be informed at the opening of the follow-up phase of, *inter alia*, the transfer of their personal information to national/other authorities, the purposes of the processing and the name of the responsible follow-up agent.

The fact that OLAF may have given information to data subjects at earlier stages of the investigation does not in itself fulfil the obligation to inform them of this new processing. In other words, information given at earliest stages of the investigation does not cover the data processing that will take place during the follow-up phase. Thus, a notification specific to the follow-up stage is necessary.

The EDPS understands that OLAF has foreseen the possibility to provide information about the processing that takes place during the follow-up stage at the end of the investigation phase, with the notification of the case closure. The EDPS considers this practice to be appropriate. If this information was not provided at the end of the investigation phase, it should be given to individuals at the earliest possible time.

In addition to the above, the EDPS recommends that OLAF puts forward proposals to inform individuals that are not covered by the OLAF Instructions to Investigators and related documents.

2.2.9 Security measures

The EDPS notes that the security measures set forth in the context of OLAF follow-up investigations are the same as those used in other data processing operations that have been notified to the EDPS for prior checking or will be notified. In order to ensure a consistent approach to OLAF security measures, the EDPS has decided to analyse the security measures in a horizontal way, rather than doing it in the context of each particular prior checking notification. Accordingly, this Opinion will not deal with security measures and the analysis will be carried out in a different Opinion which will address security issues only.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations in this Opinion are fully taken into account. In particular, OLAF must:

- Evaluate on a case-by-case basis the data collected in order to ensure that only data that are necessary for the purpose of the particular follow-up procedure are included in the CMS or otherwise used. Ensure that follow-up agents are made aware of this rule so that they apply it systematically.
- If special categories of data not useful /necessary are somehow "captured" in the follow up CMS/paper files, they should be deleted or never collected in the first place. OLAF follow-up agents should be made aware of this rule.
- Conduct a preliminary evaluation of the necessity of the 20 years conservation period *vis-à-vis* the purpose of such conservation when OLAF has been in existence for 10 years. A second evaluation should be conducted when OLAF has been in existence for 20 years.

- Ensure that data transfers under Article 7 take place only "if necessary" so that unnecessary transfers will not occur. Make sure that OLAF follow-up agents apply this rule on a case by case basis. Towards this end, put in place a procedure whereby a note to the file is drafted establishing the necessity of the data transfers that have taken place or will take place in the context of a given follow-up case.
- Ensure that a notice is given to the recipient of information in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.
- Accredit the "necessity" to carry out data transfers under Article 8 when they take place following a request from the recipient. To this end, list in a reasoned opinion all the data transfers that will be carried out or have been carried out in the context of a follow-up case and describe the "necessity" *ex* Article 8.
- Ensure that individuals are informed of the data processing that takes place under the follow up stage *ex* Article 11 and 12 either at the end of the investigation phase or as early as possible during the follow-up phase.
- Put forward proposals to the EDPS in order to inform individuals *ex* Article 11 and 12 which are not covered by the current OLAF notification procedures (so-called "fifth category").
- Take into account the recommendations made in this Opinion as well as in OLAF Instructions to Investigators when updating OLAF Manual.

Done at Brussels, 26 March 2007

Peter HUSTINX
European Data Protection Supervisor