Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office on Monitoring Cases

Brussels, 11 July 2007 (Case 2006-548)

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") a prior check Notification regarding the data processing operations that take place when OLAF opens a Monitoring Case.

This Notification was received together with four other prior check Notifications related to OLAF cases in follow-up. On 20 December 2006, the EDPS made a request for further information regarding the Monitoring cases as well as the other four prior check notifications on cases in follow-up to which he received the responses on 10 January 2007[1]. On 1 February 2007, OLAF's Data Protection Officer ("DPO") communicated to the EDPS her decision to withdraw the Notification on Monitoring cases. The OLAF DPO explained that the content of the Notification was too focussed on the follow-up activities which follow from the Monitoring cases rather than on the Monitoring cases *per se*. Further, it was explained that the data controller for Monitoring cases was different to the controller for the cases in follow-up.

On 23 March 2007, OLAF's DPO submitted a new prior check Notification on Monitoring cases (hereinafter "the Notification" or "Monitoring cases notification") which is the object of this Opinion. The EDPS observes that whereas some variations exist between the data processing operations carried out in the context of cases in follow-up and those that take place in Monitoring cases, the differences are minor. Accordingly, the legal analysis in this Opinion basically follows the same lines and reaches similar conclusions as those adopted in the EDPS Opinion on cases in follow-up.

The case was suspended pending comments on the draft opinion from the DPO as well as some additional factual information requested on 7 May 2007. The comments plus the additional information were received on 27 June 2007.

[1] On 26 March 2007 the EDPS issued an Opinion which concerned the four "follow-up" prior check Notifications: Opinion of 26 March 2007 on Follow-up data processing operations (disciplinary, administrative, judicial, financial) (Cases 2006-543, 2006-544, 2006-545, 2006-546, 2006-547).

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. Examination of the matter

2.1. The facts

Background information. Within this section, it is relevant to first provide an overview of the different phases of OLAF's cases and the types of cases. This is necessary in order to see how the Monitoring cases fit within the different procedural phases and the typology. This is followed by a description of the main features of the Monitoring cases.

Regarding the procedures or phases, the EDPS notes that an OLAF case[2] 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 Executive Board recommends whether a case should be opened or not. If the Director accepts the recommendation to open a case, the *second phase* starts with the formal decision to open a case and continues with the necessary operational activities. Investigations can be internal and external[3]. Other cases include coordination, monitoring and criminal assistance cases[4]. OLAF may decide that a case should be closed with or without follow-up actions. If the case is closed with follow-up, the *third phase* starts during which OLAF's follow-up team carries out various activities designed to ensure that the competent Community and/or national authorities have executed the measures recommended by OLAF. If after the assessment phase, OLAF decides not to open a case, the matter at stake may be classified as a non-case or prima facie non-case[5].

Regarding the concept and main features of the Monitoring cases, according to the OLAF Manual[6], these are cases where OLAF would be competent to conduct an external investigation, but where a Member State or other authority is in a better position to do so (and is usually already doing it). Information relevant to a Monitoring case is passed directly to the authority judged competent to handle it. As outlined above, if a case is deemed to be a Monitoring case, no OLAF Investigation *per se* takes place. Instead, after the assessment phase, because the interests of the EU are at stake, OLAF opens a Monitoring case and an appropriate follow-up path (financial or administrative). The case is handled by the appropriate follow-up unit. OLAF's main activity in the context of the Monitoring case at stake consists of requesting reports from the Member State or other authority on developments at regular intervals. Updates are normally requested at least once every six months. At the conclusion of the Monitoring case, the OLAF Board recommends closure of the case and the follow-up path. The final decision is taken by the Director General or by a Director whom he has delegated to take this decision.

---

[2] The term "case" is used within OLAF as a general term which includes all types of investigations and cases.

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

[4] *Coordination cases:* These are cases that could be the subject of an external investigation, but where OLAF'S role is to contribute to investigations being carried out by other national or Community Services, by, inter alia, facilitating the gathering and exchange of information. There is no OLAF investigation *strictu sensu* within OLAF.
Criminal Assistance: These are cases within the legal competence of OLAF in which competent authorities of a Member State carry out a criminal investigation and request OLAF'S assistance. There is no OLAF investigation *strictu sensu* within OLAF.

[5] *Non-Cases:* These are the result of considering that EU interests appear not to be at risk from irregular activity or other factors indicate that no case should be opened, such as where a Member State is already dealing with a matter in a satisfactory manner.
Prima Facie-Non-Cases: Information clearly and unequivocally does not fall within the competence of OLAF.

[6] Page. 98

Obviously, there are many similarities between the procedures of Monitoring cases and cases in follow-up. One of the main differences is that cases in follow-up are preceded by an investigatory phase that takes place within OLAF whereas such a phase does not take place in Monitoring cases, at least not within OLAF. Furthermore, for cases in follow-up, OLAF works towards ensuring that national authorities implement OLAF's recommendations adopted in the investigatory phase whereas for Monitoring cases, OLAF's involvement consists mostly of overseeing and monitoring what the national authorities do regarding a case, without relating it to a given set of recommendations reached by OLAF.

From a data protection perspective, the procedural differences vis-à-vis cases in follow-up do not entail major differences in the data processing operations. Indeed, the main features of the data processing that takes place within the cases in follow-up coincide with those of the Monitoring cases.

Purpose of the data processing operations. The purpose of the data processing is to monitor the activities of the national authorities or EU institutions that are responsible for a case in order to ensure that the appropriate judicial or administrative actions are taken to protect the Community's financial interests.

Responsibility for the data processing. The responsibility for conducting assessments lies within Directorates A and B. The responsibility for the active phase of Monitoring cases lies within Unit C1 (Judicial and Legal advice), C2 (Fraud Prevention and Intelligence) or C3 (Mutual Assistance and Intelligence). Accordingly, the data controller for data processing operations that take place with the purpose of carrying out monitoring cases is the Director General. The units of Directorate C are also co-data controllers for cases in follow-up. Accordingly, the OLAF agents responsible for Monitoring case are referred to as "Follow-up agents". In this Opinion we will refer to them as Follow-up agents or simply agents.

Description of the automated data processing operations. The data processing operations carried out in the context of the Monitoring cases are both manual and automated. The automated operations use mainly the Case Management System which is a central database which permits the management of 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 is attached to the case, through its different phases. This applies to Monitoring cases and to all other types of cases. All significant events concerning a case which take place during the various stages are recorded in the CMS[7].

Once a case has been deemed to be a Monitoring case, a follow-up agent/s is appointed as responsible for the case at stake. 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 principle". (iii) In line with the above principles, follow up agent/s competent for a given case are given read/write access to all the documents contained in the CMS. (iv) Each follow-up agent is

[7] 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.

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.

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

When the Monitoring case is closed, the follow-up agent hands over all case-related documents to the Greffe. The Greffe staff 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 assessment phase.

Data subjects involved. According to the notification form, the types of data subjects whose data are processed in the context of the data processing operations consist of the following:

(i) personnel of the EU institutions, bodies, offices and agencies who are *the subject* of a monitoring case, including officials, temporary agents, national experts; *(ii)* persons outside of the EU institutions, authorities, bodies, offices and agencies who are *the subject* of a monitoring case; *(iii)* persons inside and outside of the EU institutions, bodies, offices or agencies who may be involved in the case, either as whistleblowers, informants or witnesses; *(iv)* persons *inside and* outside of the EU institutions who may be involved in the case not covered by the categories listed above.

Categories of personal data. According to the Notification, the type of personal data processed 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 monitoring.

The Notification specifies 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.

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 notification, data may be transferred to the following entities: *(i)* concerned Community institutions, bodies, offices or agencies in order to allow them to take appropriate measures to protect the financial interests of the EU; *(ii)* competent Member State authorities, judicial and administrative in order to allow them to take appropriate measures to protect the financial interests of the EU; *(iii)* competent third country authorities and international organisations in order to ensure the protection of the financial interests of the EU.

[8] Commission Decision 2002/47/EC, ECSC, Euratom, OJ L 21, 24.1.2002, p. 23.
[9] Special categories of data are those referred to in Article 10.1 of Regulation (EC) No 45/2001.

Data subjects' rights to information, access and rectification. As far as the right to information is concerned, and in particular *the channels* through which information is provided, we note that on the one hand OLAF has created a privacy statement which is on the OLAF website. A copy of the privacy statement is attached to the Notification. On the other hand, OLAF has not put in place information notices addressed directly to individuals who are the subject of investigations. OLAF has explained that given that its role in Monitoring cases is limited to requesting reports from the Member State or other authority on developments at regular intervals, OLAF could interfere with the national proceedings by doing so. For this reason, in order to provide information to data subjects, OLAF proposes in the near future to enter into agreements with Member States asking them to include in their privacy statement addressed to the data subjects a paragraph informing them of the possibility for their personal data to be transferred to OLAF for monitoring purposes.

As far as the right of access is concerned, the OLAF privacy statement available in OLAF website provides that individuals, on request, will be sent their personal data and be able to correct or complete them.

The Director General of OLAF has provided guidance to case handlers regarding, among other things, the procedures to follow in order to ensure that the data subjects' rights are respected (document entitled "Instructions to staff conducting investigations following an opinion of the EDPS", hereinafter "OLAF Instructions to staff"). OLAF Instructions to staff include a form to be used by OLAF staff, including follow-up agents in response to access requests received from data subjects. The standard form will facilitate the response to those who make access requests. In addition, if the access rights have been denied to an individual, the Instructions foresee that Follow-up agents must complete a note to the file, explaining the reasons for imposing such restriction.

OLAF Instructions to staff 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 staff 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.

2.2. Legal aspects

2.2.1. Prior checking

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 data processing operations notified for prior checking.

First, the EDPS notes that the notification for prior checking relates to the processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, the notification indicates 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 notification clearly points out that the data collected undergo "processing" operations, as defined under Article 2 (b) of the Regulation (EC) No 45/2001, which includes 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.

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.

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 subjects by virtue of their nature, their scope or their purposes".* Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks.

The EDPS considers that the notification on Monitoring cases submitted to the EDPS for prior checking clearly falls 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 case in point, OLAF will process information about suspected offences and offences insofar as the scope of the processing may entail monitoring cases and other actions related to alleged offences.

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 was received on 23 March 2007. Pursuant to Article 27.4 of Regulation (EC) No 45/2001, the procedure was suspended on 7 May 2007 until 27 June 2007 to allow comments from the DPO on the draft opinion and obtain confirmation regarding certain factual information. The Opinion will therefore be adopted no later than 14 July 2007 (deadline was 24 May 2007 plus 51 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 Notification 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 interest 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 processing operations notified for prior checking, the EDPS takes note of the following:

First, some of the legal grounds for the processing of data in the context of Monitoring cases are found in the EC Treaty itself. For example, Article 280 of the EC Treaty establishes a general duty upon the Community and Member States to counter fraud and any other activities affecting the financial interests of the Community. Article 280.3 particularly refers to the obligation that falls upon Member States and the Commission to coordinate their action "*aimed at protecting the financial interests of the Community against fraud. To this end they shall organise, together with the Commission, close and regular cooperation between the competent authorities*". The activities that take place in the context of Monitoring cases whereby OLAF and Member States will exchange information regarding a case derives and has its basis on Article 280.3 of the EC Treaty.

Second, the above statement in the EC Treaty must be read in conjunction with Article 1(2) of the 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. Article 1(2) establishes that OLAF "*shall provide the Member States with assistance from the Commission in organising close and regular cooperation between their competent authorities in order to coordinate their activities for the purpose of protecting the European Community's financial interests against fraud*". Article 1(2) is a consequence and a specification of Article 280.3 of the EC Treaty.

Third, also relevant is Article 9(1) of Council Regulation No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests according to which "*the Commission shall, on its responsibility, have checks carried out on: (a) the conformity of administrative practices with Community rules; (b) the existence of the necessary substantiating documents and their concordance with the Communities' revenue and expenditure as referred to in Article 1; and (c) the circumstances in which such financial transactions are carried out and checked".* Insofar as Article 9(1) entitles OLAF to request from Member States the performance of checks, it also provides a legal basis for the processing of personal data collected in the context of such activities.

Finally, specific provisions in the sectoral legislation foresee the request of information from Member States and the request to Member States to carry out national checks. Examples of the former include Articles 3, 4 and 5 of Council Regulation (EEC) No 595/91 of 4 March 1991 concerning irregularities and the recovery of sums wrongly paid in connection with the financing of the common agricultural policy and the organization of an information system in this field and repealing Regulation (EEC) No 283/72. Examples of the latter include Article 6 of the same Regulation. These articles constitute the legal basis for the performance of these activities and the related processing of personal data.

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 280.3 EC Treaty and 10 combined with Article 1 (2) Regulation (EC) No 1073/1999 confer upon OLAF the competence and the obligation to coordinate its actions with Member States in order to protect the financial interests of the Community against fraud. The specific legislation foresees for concrete cases how such coordination must be carried out, namely, by exchanging information, particularly obtaining information from Member States and asking Member States authorities to carry out national checks.

Necessity test. *A*ccording 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 Monitoring cases are concerned, generally speaking, the EDPS presupposes that such necessity exists whenever OLAF has reached a decision to open a Monitoring case. However, the EDPS notes that the real "necessity" of the data processing has to be analysed *in concreto,* for each particular Monitoring 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 monitoring 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 or criminal convictions. 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 case, processing of the mentioned data is authorised by the legal instruments mentioned in point 2.2.2 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 Notification states that no data falling under the categories of data referred to in Article 10.1 are processed in the context of the 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 Monitoring cases, OLAF may become, perhaps involuntarily, in possession of special categories of data, which will often be of no interest/relevance to the case. 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 relevant for the purposes sought by the Monitoring cases are somehow "captured" in the 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 Monitoring related 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 notification 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 Monitoring 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. As a general rule, this information will be relevant for all cases.

Second, as far as the data collected directly by the Monitoring case 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 Monitoring activities must be collected or further processed.

Third, 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 OLAF's Notification, OLAF may keep both paper and electronic files relating to Monitoring cases for up to 20 years after the date on which the follow-up actions that take place in the context of Monitoring cases have been completed.

The EDPS is concerned by the recording of case-related information for 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)e of the Regulation, OLAF is authorised to do so if it makes the data anonymous 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 within or between 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 Notification 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 within or between 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 not only under investigation but also cases in the follow-up phase or typically Monitoring cases. Such legislation foresees the transfer of data to Community institutions, bodies, offices or agencies, in order to allow them to take appropriate measures to protect the financial interests of the Community.

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 Monitoring 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 provide 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, it 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 agents 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 staff regarding the right of access and rectification to be in line with Article 13 of the Regulation (EC) 45/2001.

In addition to OLAF's Instructions to staff, for Monitoring cases, the procedures to exercise the right of access/rectification are partially described in the draft privacy statement attached to the Notification. In this regard, the statement says that "*In case of any difficulties, or for any questions related to the processing of your personal data, please contact Mr. Franz-Hermann Bruner*". This paragraph follows a sentence acknowledging that individuals may be sent their personal data in order to be corrected or completed. Thus, presumably the person with whom individuals exercise the right of access is Mr. Franz-Hermann Bruner, Director General of OLAF.

The EDPS notes that the nature of access requests and the necessary measures to provide such access implies in-depth, hands on knowledge of the handling of the personal data in a given data processing. For this reason, usually, access requests are handled by someone appointed by the data controller, somebody who follows the day-to-day data processing operations. Taking into account the responsibilities of the Director General of OLAF, the EDPS wonders whether it would not be more appropriate for the Director General to appoint a person close to the handling of the data in Monitoring cases as the person with whom individuals can exercise their access/rectification rights. In such cases, as stated below, the name and contact details of such a person should be provided in the privacy statement. Of course, this is without prejudice to the Director General of OLAF, as data controller, taking full responsibility for the final decision as to whether access has to be granted in each case.

As far as the use of the exceptions is concerned, the EDPS considers OLAF's practice as set forth in OLAF's Instructions to staff to be in line with Article 20 of the Regulation (EC) 45/2001. 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.(b) 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).

Within certain limits, OLAF may also be able to rely on the exception of Article 20.1 (a) which enables OLAF to suspend access for the prevention/detection/prosecution of a criminal offence. In particular, OLAF will be able to rely on this exception if the investigation at national level is still on-going. However, it would not be possible to apply Article 20.1. (a) after the national investigation is closed and the individual has been charged with a criminal offence as once the investigation is closed, no secrecy applies to the trial, judgement and possible appeal. The contrary would violate 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.

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 the conditions for the application of one of the exceptions, for example, Article 20.1 (a), or 20.1 (b) may apply, and if so, whether they continue to 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 (b), it must assess whether it is necessary to suspend access in order to safeguard an important economic interest. In making such an assessment, OLAF must take into account that simply because there is an economic interest at stake, does not imply that there will invariably be a need to suspend access. Rather, there must be a clear and continued link between the need to suspend access and the safeguarding of an economic interest. Furthermore, 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"*. The provision of this information may only be deferred *"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.

In addition to the above, the EDPS observes that OLAF's practice regarding access as set forth in OLAF's Instructions to staff is not reflected in the OLAF Manual. In fact, the Manual contains a statement that could be viewed as contradictory to 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 staff mentioned above.

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.

As to the *channel* through which information is provided to individuals, the EDPS considers that the provision of information through the OLAF Europa website as a positive step towards complying with Article 11 and 12 of Regulation (EC) No 45/2001 and a measure to enhance transparency regarding the data processing operations in which OLAF is engaged. However, the EDPS is concerned by the fact that many data subjects which are the object of investigations may not visit OLAF Europa website, and thus, may never have access to such information. In order to take care of this concern OLAF has proposed to the EDPS to implement the arrangement described under section 2.1. (paragraph dealing with *Data subjects' rights to information, access and rectification*) which would ensure the provision of direct information to individuals. Indeed, OLAF has suggested that Member States include in their privacy statement addressed to data subjects a paragraph informing them of the possibility for their personal data to be transferred to OLAF for monitoring purposes. Because individuals will have been informed of the transfer of their personal data to OLAF by Member States, it would not be necessary for OLAF to provide such information again. The EDPS notes that this is in line with Article 11 and 12 of Regulation (EC) No 45/2001 which requires the data controller to provide the information "*except where he or she already has it*". In order to ensure the effectiveness of this arrangement OLAF proposes entering into an agreement with Member States pursuant to which Member States would agree to inform data subjects that their data will be transferred to OLAF for monitoring purposes.

The EDPS understands that given the limited role that OLAF plays in Monitoring cases and the potential interference with Member State proceedings, it may not be appropriate for OLAF to provide information notices directly to individuals who are the object of a Monitoring case. The EDPS considers that the arrangement that OLAF has proposed may be an effective way of providing the information to data subjects as requested under Article 11 and 12 of Regulation (EC) No 45/2001 while avoiding interfering with the national proceedings. Accordingly, the EDPS calls upon OLAF to enter into such agreements with Member States.

As far as the *content* of the information is concerned, the EDPS considers that the information that OLAF foresees to provide to individuals as described in the privacy statement, which is published on the OLAF Europa website, is in line with Article 11 and 12 of Regulation (EC) 45/2001. However, regarding the right of access and rectification, the EDPS would find it more appropriate if the language used in the statement was replaced by a sentence plainly acknowledging that individuals have such rights ("You have a right to access the personal data we hold regarding you and to correct and complete it") as opposed to the current sentence "*On request, you may be sent your own personal data and correct or complete them"* which

may be read as somehow limiting the scope of the right of access. This should be followed by an indication of how such rights can be exercised including an address (e-mail/postal/telephone) where individuals can exercise such rights.

In addition to the above, as far as the right of access and rectification are concerned, as noted under 2.2.7, it may be more effective to provide the name and contact details of someone directly involved in the day to day data processing operations as the person appointed by the data controller to handle access requests. The contact details of such person should be provided clearly in the privacy statement.

2.2.9. Security measures

The EDPS notes that the security measures set forth in the context of Monitoring cases are the same as those used in other data processing operations that have been notified to the EDPS for prior checking. This may also be true for any future cases. 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 Monitoring case are included in the CMS or otherwise used, and ensure that agents are made aware of this rule so that they apply it systematically.
- Ensure that if special categories of data are unduly "captured" in the CMS/paper files of a given Monitoring case, they should be deleted or never collected in the first place. OLAF 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 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 Monitoring 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.
- Ascertain 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 Monitoring case and describe the "necessity" *ex* Article 8.

- Consider appointing a person directly involved in the day to day data processing operations as the person appointed by the data controller to handle access/ rectification requests.
- Ensure that individuals are informed of the data processing that takes place under the Monitoring cases *ex* Article 11 and 12 through publication of the privacy statement on the OLAF Europa website *and* agreements with Member States whereby they agree to inform data subjects that their data will be transferred to OLAF for monitoring purposes. In particular, as far as the privacy statement is concerned, (i) reformulate the paragraph regarding access rights and (ii) ensure that individuals are given sufficient information to contact the person competent for access requests.

Done at Brussels, 11 July 2007

Peter HUSTINX
European Data Protection Supervisor