Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on the Fraud Notification Service

Brussels, 18 December 2007 (Case 2007-481)

1. Proceedings

On 23 July 2007, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the European Anti-Fraud Office ("OLAF") a notification for prior checking regarding the setting up of a Fraud Notification Service ("the Notification").

The EDPS requested complementary information about the Fraud Notification Service ("FNS") on 31 July 2007. The answers were received on 19 October 2007. On 26 November 2007 the EDPS sent the Draft Opinion to OLAF for comments which were received on 11 December 2007.

2. Examination of the matter

The Fraud Notification Service is a web based information system that OLAF has put at the public's disposal in order to facilitate the collection of information to use in the fight against fraud, corruption and other illegal activities affecting the financial interests of the Community. The functions of this system are basically the same as the OLAF Free Phone Service which the EDPS prior checked in June 2007[1]. Taking into account the similarity of purposes and of data processing features of both systems, the legal reasoning used in this prior check is basically the same as that used in the prior check Opinion regarding the OLAF Free Phone Service.

The data processing under examination is a component of OLAF overall investigative activities and procedures in the fight against fraud, corruption and other illegal activities affecting the financial interests of the Community. In particular, the collection of the information through the FNS is the first step of a procedure that may continue with the opening of a full investigation, if this is considered necessary and appropriate. However, the legal analysis in this Opinion will only address those aspects that are exclusively related to the data processing that takes place as a result of the operation of the FNS; it will not analyse data processing operations that take place in other phases of OLAF investigation procedures, which may have been examined in the context of other prior checks[2].

1 EDPS Opinion of 6 June 2007 on a notification for prior checking on a free phone service (Case 2007-74).
2 See footnote 3 and 7.

Below is a summary of OLAF investigatory procedures, in order to show how the FNS fits within the overall OLAF investigation process. It is followed by a description of the data processing features of the FNS.

2.1 The Facts

The lifespan of an OLAF investigation can be summarised as follows: Within the *first stage*, OLAF case handlers evaluate the initial sources of information which may have been collected directly by OLAF or provided to OLAF by third parties (witnesses, whistleblowers, informants, etc). This phase is called the "assessment phase". If the initial information does not relate to a matter within OLAF competence, it is classified as a prima facie non-case[3] or as a non-case[4]. If OLAF decides that the matter is relevant, the *second phase* takes place during which the investigatory activities *per se* will be carried out. There are two categories of investigations - internal and external - and several other categories of cases - monitoring, coordination and criminal assistance[5]. If an investigation has been opened, at the end of the investigation, OLAF decides whether it should be closed with or without follow-up actions. In the first hypothesis, the *third phase* starts, during which OLAF follow-up team carries out various activities designed to ensure that the competent Community and national authorities have executed the measures recommended by OLAF[6]. If a case has been opened (instead of an investigation), it is not followed by a third phase.

The processing operations that take place in the management of the Fraud Notification Service generally occur *before* the start of the first phase. As further described below, the processing operations that take place in the context of the FNS constitute a sort of "pre-assessment phase". In particular, in the management of the FNS, OLAF investigators and managers review the information left through the FNS and engage in a preliminary analysis of their relevance in order for OLAF to decide whether an assessment phase should be opened. The further processing that may occur once an assessment phase has been opened will not be analysed in the context of the present opinion, which as outlined above, will be limited to the analysis that takes place exclusively in the context of the operation and management of the FNS[7].

---

3 *Prima Facie-Non-Cases*: Information clearly and unequivocally does not fall within the competence of OLAF.

4 *Non-Cases:* These are the result of considering that EU interests appear not to be at risk from irregular activity or where a Member State is already dealing with a matter in a satisfactory manner.

5 *Monitoring cases:* These are cases where OLAF would be competent to open an external investigation but in which a Member State or other authority is in a better position to investigate. In these cases, there is no OLAF investigation; however, OLAF follows up with the appropriate follow-up team.
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.

6 Some variations in these three phases may occur.

7 The EDPS has issued an opinion of the processing operations that take place during the assessment and investigation phase related to internal investigations, where further processing of messages left in the FPS may take place. See EDPS Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418). It should also be noted that the EDPS has assessed prior checking notifications related to OLAF processing of personal data in the context of, among others, external investigations, prima facie non cases, non cases and monitoring cases.

The Fraud Notification Service is made available to the public as a web-based information system that may be used by the public to submit information to OLAF about suspected fraud or corruption affecting Community interests.

The ***purpose of the processing*** is to obtain information from the public which may reveal the existence of fraud and corruption affecting the financial interests of the Community.

The ***primary responsibility for the data processing*** lies with OLAF adviser on anticorruption. However, as further described below, the investigators from the Investigations and Operations Units (various Units in Directorates A and B) carry out some of the data processing operations that take place in the context of the operation of the FNS. In addition, the Information Services Unit (D8) is responsible for several aspects related to the management and technical maintenance of the FNS.

As further described below, the ***automated and manual data*** processing operations are closely interrelated and can be described altogether as follows:

Stage one: Members of the public can provide the information in two different ways. First, they can complete a questionnaire which includes a free text field, to which they may also attach a file. Second, they can register to have two-way communications with OLAF, which take the form of electronic messages transmitted within the FNS. In such cases, a username is generated and supplied to the user who is asked to choose a password. The system allows the user to provide the information anonymously and permits a secure communication channel. Such communications normally take the form of questions by the responsible OLAF investigator and answers by the user. Incoming messages are automatically stored on the stand-alone server, which is managed by Unit D.8.

Stage two: The initial review of the messages within the system is carried out as follows:

1) Automatic review of questionnaires by the system:

1. If they are totally devoid of any content (i.e. no free text, no attachment and no other fields have been selected), then the system will automatically generate a message to the user that the questionnaire has not been submitted.
2. If they contain no free text and no attachment, but one of the other fields has been selected, then the system places them in the "blank folder". The Review officer (an investigator from Directorate A or B assigned by his/her Head of Unit to perform the task of reviewing FNS messages, based on experience and linguistic knowledge) can either (i) mark it for deletion, in which case it will be passed to the System Administrator[8] (who can either definitively delete it from the system or deem it relevant and assign it to the Head of Unit responsible for the sector concerned), or (ii) deem it to be relevant, and assign it to the Head of Unit responsible for the sector concerned.
3. If the system deems them to be irrelevant, based on statistics accumulated from previously classified messages, then it places them in the "irrelevant folder". The messages in this folder are handled in the same manner as messages in the “blank folder,” described in the previous paragraph.

[8] The System Administrator is responsible for managing the investigators’ access, reviewing and deleting messages marked for deletion by review officers; accessing system-generated statistics, and verifying the backup and audit logs. During the first 12 months of operation, the System Administrator will be Mr.S.Knolle, who works under the authority of the data controller of the system.

2) Human review

Review officers will review all messages that have not been deleted in the first phase described above. The System recognizes the language of the incoming questionnaire and allocates it automatically to the Review officer who is assigned to this language. He gets an automatically generated e-mail notification that a new message is in the system. The System Administrator will provide each Review officer with a username and a password. The Review Officer decides whether this information is relevant or irrelevant. The questionnaire/message is sent by the Review officer via the system to the Head of Unit responsible for the sector concerned (who gets an email notification that a new message is in the system).

Stage three: The further review of the message by the unit responsible for the sector concerned by the message is as follows.

Upon receipt, the Head of Unit will delete irrelevant messages and forward relevant messages to an investigator in his/her unit. The investigator will first determine whether a communication channel has been selected by the user. If so, the investigator may activate the communication channel with the user, and thereby correspond with the user through the system via the anonymous mailbox. Once he has received any further information through such communications, the investigator will handle the information as any incoming information, in accordance with procedures described in the OLAF Manual. Ultimately, the Head of Unit will decide whether the matter merits initiation of the assessment stage, or should be classified as a prima facie non-case. If an assessment is initiated, then the matter will be assigned a CMS number and the investigator will place all information received through the system in the CMS file.

As with any other incoming information, the responsible Head of Unit may deem the information to be relevant for a Member State authority in its work in the fight against fraud and corruption affecting the financial interests of the EU. If so, he will forward the information to the OLAF operational intelligence unit, which will forward the message to the concerned Member State authority.

All information in the system is encrypted and accessible by only one member of OLAF staff at any one time. Information received is stored in the FNS stand alone server only during the three stages described above. Irrelevant messages will be definitively deleted from the system by the system administrator. Messages leading to an assessment will be deleted by the responsible investigator once a CMS file is created. Altogether the information will not be stored for a period superior to one year.

The data processing involves the following ***types of data subjects***: *(i)* Individuals who choose to use the system and leave their contact details and *(ii)* Any person named by a user of the system.

Regarding the categories of personal data, the personal data collected from users of the system include, date and time when they left the message, the country of origin and the content of the message which may include additional personal information from them. The personal data collected may also include the identity of persons named by the users of the system and other variable information, depending on each message.

Regarding ***conservation periods,*** if the information is deemed not relevant it is deleted. This may happen automatically, via the automatic classification mechanism described above or it may happen upon review by the Review officer, the System administrator and the Head of Unit responsible for the case.

If the data becomes part of an investigation file, the information is kept for a period of 20 years, 10 years if it is exchanged with a Member State under Mutual Assistance, 3 years if it is exchanged with a Member State under irregularities and 5 years if it is classified as a non-case.

Regarding ***data transfers,*** the EDPS notes that the messages are not transferred outside of OLAF. They may be transferred to investigators within the investigative units and operational intelligence unit in case they are deemed relevant for Member States or if they become part of a case or if an investigation is opened. The data transfers that may occur within these two contexts are beyond the processing that occurs within FNS. Some of these data processing operations have been prior checked by the EDPS in the context of the notification of the data processing operations that take place in the context of investigations (external or internal) or cases.

Regarding the ***Data Subjects' Rights to Information***, the prior check notification refers to a privacy statement, intended to provide information to individuals who use the FNS.

The privacy statement contains information on the purposes of the processing, the recipients of the data, the existence of a right of access and the right to rectify, including the name of the contact person to exercise such rights. It also contains the time limits for storing the data and the right to have recourse to the European Data Protection Supervisor.

Regarding how information is provided to the different data subjects, it is stated in the Notification that a link to the privacy statement will be placed on the home page of the FNS, within the OLAF Europa site. Thus, the users of the system will have access to the privacy statement when they access the site in order to use the system.

The persons named by the users of the system will be informed as follows: If the information is eventually used in an OLAF investigation or a case, it will become part of the case file. Thus, the named person will be informed in the context of the case, as established in the prior checks of the various types of OLAF cases. The provision of information may be deferred if one of the exceptions set forth in Article 20 of Regulation (EC) No 45/2001 applies. If the information is deemed as irrelevant, and does not become part of an investigation or case file, then personal information will not be provided.

As far as the FNS callers' ***right of access and rectification*** are concerned, the privacy statement declares that individuals have such rights regarding the information that OLAF holds about them. It gives the name and e-mail of the data controller as the contact person to exercise such rights as well as to answer any further questions regarding the processing of their personal information. The privacy statement does not distinguish between the different types of data subjects (persons named in the messages v persons who left the messages).

The EDPS notes that OLAF has implemented ***security measures***.

2.2. Legal aspects

2.2.1. Prior checking

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"[9].

For the reasons described below, all the elements that trigger the application of the Regulation exist in the operation of the FNS:

Firstly, the operation of the FNS entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, as described in the Notification, personal data of individuals who use the FNS to leave messages are kept such as the time of the voice message, country of origin and content of message. Furthermore, the FNS may also entail the processing of the identity and other information related to the persons named by the users of the system.

Secondly, as described in the Notification, the personal data collected undergo "automatic processing" operations, as defined under Article 2 (b) of the Regulation (EC) No 45/2001. The mere storage of the electronic messages and their on-line transfer among OLAF investigators constitutes an automatic data processing operation.

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 with respect to the management of the FNS.

Assessment of Whether the Data Processing Operations Fall Under Article 27 of the Regulation

Article 27.1 of 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 a 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 FNS notification submitted to the EDPS for prior checking clearly falls under various hypotheses foreseen by 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, by setting up the FNS, various units within OLAF will process information which may relate to allegations of fraud and other irregularities which have an impact on the EU budget as well as allegations of corruption and other serious misconduct on the part of members or staff of European institutions. As a matter of fact, the FNS is a tool for OLAF to discover irregularities and misconduct, and thus will, in some instances, collect information related to offences.

In addition, the EDPS considers that the notification also falls under Article 27.2(b) of the Regulation (EC) No 45/2001 which stipulates that data operations *"intended to evaluate personal aspects relating to the data subject, including his or her (...) conduct*". In the case under analysis, various personal aspects relating to data subjects are evaluated as a matter of course, from the individual who uses the system to inform to the individual named by others, thus triggering the application of Article 27.2(b).

[9] *Ex* Article 3.2 of Regulation (EC) No 45/2001.

The notification from the OLAF Data ¨Protection Officer was received on 23 July 2007. Pursuant to Article 27.4 of Regulation (EC) No 45/2001 due to information requests and to allow comments from the DPO on the EDPS Draft Opinion the procedure was suspended for 65 days, plus the month of August. The Opinion will therefore be adopted no later than 3 January 2008 (28 December 2007 and the following days not being working days)

2.2.2. Lawfulness of the Processing

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

As pointed out in the Notification, 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 in Other Legal Instruments: In ascertaining the legal grounds in the Treaty or in other legal instruments that legitimise the processing operations that take place in the context of the management of the FNS, the EDPS takes note of the following:

First, in indicating the legal basis for the processing that takes place through the FNS, it is explained that the processing is part, often the first step, of the collection of information that may lead to the opening of an investigation. Thus, it is explained in the Notification that the legal grounds that justify the data processing that occurs during the investigation also justify the data processing that occurs prior to the investigation phase, i.e. particularly during the pre-assessment phase, in this case the processing that occurs through the FNS. As far as internal investigations are concerned, as pointed out in the EDPS Opinion on OLAF internal investigations[10], the legal grounds are mainly Article 4 of Regulation 1073/1999 concerning investigations conducted by OLAF[11]. Also relevant is Article 2 of Commission Decision 1999/352 establishing OLAF[12]. As far as external investigations are concerned, there are a

---

10 Prior check Opinion of 23 June 2006 on OLAF internal investigations (Case 2005-418).

11 The relevant part of Article 4 of Regulation 1073/1999 stipulates the following: "1. In the areas referred to in Article 1, the Office shall carry out administrative investigations within the institutions, bodies, offices and agencies (hereinafter "internal investigations"). (...) 2. Provided that the provisions referred to in paragraph 1 are complied with: (...),- the Office may request oral information from members of the institutions and bodies, from managers of offices and agencies and from the staff of the institutions, bodies, offices and agencies. 3. (...) The Office may, moreover, ask any person concerned to supply such information as it may consider pertinent to its investigations.

12 This Article establishes the following: "(...) The Office shall be responsible for carrying out internal administrative investigations intended: (a) to combat fraud, corruption and any other illegal activity adversely affecting the Community's financial interests, (b) to investigate serious facts linked to the performance of professional activities which may constitute a breach of obligations by officials and servants of the Communities likely to lead to disciplinary and, in appropriate cases, criminal proceedings or an analogous breach of obligations by Members of the institutions and bodies not subject to the Staff Regulations of

variety of legal sources. For example, the processing that takes place when OLAF engages in horizontal anti-fraud investigations covering Community expenditure, both direct and indirect and income collected directly on behalf of the Communities (traditional own resources) is based on Article 2 of Council Regulation No 2185/96[13] in conjunction with Article 3 of Regulation No 1073/99 concerning investigations conducted by OLAF[14]. In addition, there are a number of sectoral legal instruments that legitimise the data processing in specific sectors, which are referred to by Article 9(2) of Council Regulation 2988/95 on the protection of the European Communities financial interests enabling the Commission to "*carry out checks and inspections on the spot under the conditions laid down in the sectoral rules"*. Other legal grounds apply regarding other types of cases.

Second, the EDPS notes the existence of the above legislation enabling OLAF to engage in investigations (of different categories), of alleged fraud, corruption and other irregularities affecting the Community. The EDPS concurs with OLAF that these legal instruments also constitute an appropriate legal basis *ex* Article 5 a) to legitimise the collection and further processing of personal data through the FNS. As pointed out in the Notification, the processing that takes place through the FNS *"is part of the initial information gathering which may lead to the opening of an investigation"*. Taking into account that OLAF is under an obligation to investigate serious irregularities, it seems appropriate for it to employ tools such as the FNS, which facilitates the disclosure of information to OLAF by informants or witnesses, and thus may ultimately assist OLAF in the overall purpose of fighting fraud, corruption and other irregularities.

Processing Operations are Carried out in the Public Interest: 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 Articles 4 and 5 of Regulation (EC) No 1073/1999 and Commission Decision 1999/352 establishing OLAF 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. It is therefore relevant to assess whether the data processing that occurs in the context of the FNS is pertinent for the performance of a task.

In doing so, in the first place, one must assess whether the setting up of the FNS *as such* can be deemed as necessary to perform a task. To answer this question, it is helpful to recall that OLAF core competence or task consists of carrying out investigations to combat various types of wrongdoings that may affect the Community financial interests. The EDPS understands

---

Officials of the European Communities and the Conditions of Employment of Other Servants of the Communities. (...)".

13 Council Regulation (Euratom, EC) No 2185/96 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, p. 2. Article 2 states: "The Commission may carry out on-the-spot checks and inspections pursuant to this Regulation:- for the detection of serious or transnational irregularities or irregularities that may involve economic operators acting in several Member States, or- where, for the detection of irregularities, the situation in a Member States requires on-the-spot checks and inspections to be strengthened in a particular case in order to improve the effectiveness of the protection of financial interests and so to ensure an equivalent level of protection within the Community, or- at the request of the Member States concerned."

14 "The Office shall exercise the powers conferred on the Commission by Regulation (Euratom, EC) No 2185/96 to carry out on- the- spot inspections and checks in the Member States and, in accordance with the cooperation agreements in force, in third countries".

that OLAF effectiveness to perform its task relies, among others, on its ability to gather and receive information that may reveal the existence of wrongdoings. The EDPS also understands that this applies throughout the life of a possible investigation, i.e. from the pre-assessment phase to the follow-up phase. Hence, the EDPS views the FNS in itself as a necessary instrument that helps OLAF in the initial information gathering phase. The FNS can be considered to be equivalent to other tools that also serve to report suspected frauds, and to this extent, it is as necessary as the other tools, which are described in OLAF website, including the possibility for the public in general to send e-mails and correspondence to inform OLAF about the existence of a potential wrongdoing or to use the OLAF Free Phone Service.

After having examined the necessity for the FNS as such, it is important to stress that the "necessity" of the data processing also has to be analysed *in concreto*, for each particular case, here, for each specific use of the FNS. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the processing of the information received from the FNS 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. For example, information that obviously falls outside the competence of OLAF and which would not help OLAF to pursue its goals should not be retained.

2.2.3. Processing of Special Categories of Data

Taking into account that the purpose of the Fraud Notification Service is to facilitate the receipt of information about alleged wrongdoings affecting the Community financial interests, it is expected that in a number of cases this information will be 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 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*". Taking into account the overall purpose pursued by OLAF when it engages in data processing operations, the EDPS understands that OLAF does not intend to collect such types of personal data.

2.2.4. Data Quality

Pursuant to Article 4.1.c of Regulation (EC) No 45/2001, personal data must be *"adequate, relevant and not 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 that it is up to individuals who use the FNS to decide which information they want to provide to OLAF. They may provide adequate and relevant information but they may also provide information that is completely irrelevant for the purposes sought by the FNS and overall OLAF competences. On the other hand, OLAF has the means to avoid or minimise this outcome in different ways. For example, OLAF may indicate the type of information that

is relevant and which falls within the scope of its competences. This could be done in the section of the OLAF website that deals with the FNS, in a manner similar to that used for OLAF Free Phone Service. Furthermore, in corresponding with OLAF via electronic messages, OLAF investigators should avoid asking questions that would lead informants to disclose information that is irrelevant for the purposes of detecting fraud and corruption affecting the financial interests of the Community. The personal data processed within the scheme should be limited to the data which is strictly and objectively necessary to verify the allegations made. OLAF investigators should be made aware of this rule.

If individuals leave messages with information that is pointless for the purposes at stake, such information should not be retained. In this regard, the EDPS welcomes OLAF practice consisting of deleting messages as soon as they have been deemed irrelevant and in any event establishing a maximum period of a year for their conservation.

In addition to the above, it is important to recall the application of Article 4.1(d) of Regulation (EC) No 45/2001 requiring that personal data must be *"accurate and where necessary kept up to date"*, and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."* This principle is very much connected to the exercise of the right of access, rectification, blocking and erasure (see point 2.2.7 below). Obviously, if efforts have been made to ensure the accuracy and the update of personal data, there are likely to be fewer requests for rectification.

Guarantees for whistleblowers and informants: Community legislation does not set forth a legal framework for informants, which in principle do not enjoy the same guarantee as EU Officials and other EU Staff if they come forward to OLAF with information. In this context, OLAF has adopted a policy consisting of making an effort to guarantee the confidentiality of the informants until the information is passed to national judicial authorities where no guarantee for confidentiality is given. As to the right to confidentiality that applies to EU Officials and Staff, the EDPS observes that the EU legal framework is not crystal clear: the right to confidentiality is addressed in a Commission Communication which provides for specific measures to ensure a maximum of protection for staff making proper use of the whistleblowing procedures, one of them being that *"[i]information relating to the identity of the whistleblower will be treated in confidence"*[15]. However, such a right has not been enshrined in binding legislation. As was stated in the EDPS Opinion on internal investigations[16], the EDPS considers that the confidentiality of whistleblowers and informants should be guaranteed throughout the lifespan of a case, from the pre-assessment to the assessment and investigations phases in as much as this would not contravene national rules regulating judicial procedures. Towards this end, in its Opinion on the Proposal for a Regulation amending Regulation (EC) No. 1073/1999 concerning investigations conducted by OLAF[17], the EDPS recommended that the Proposal should include a new paragraph guaranteeing the confidentiality of whistleblowers.

2.2.5. Conservation of Data/ Data Retention

15 (SEC/2004/151/2) of 6 February 2004 from Vice-President Kinnock.

16 Opinion on a notification for prior checking received form the Data Protection Officer of the European Anti-Fraud Office (OLAF) on internal investigations, 23-June 2006 (Case 2005-418).

17 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).

Pursuant to Article 4 (1) e) of Regulation (EC) No 45/2001, personal data may be kept in a form which permits the identification of data subjects for *"no longer than is necessary for the purposes for which the data were collected and/or further processed"*.

The conservation policy related to the FNS has two different rules: one for irrelevant messages and one for relevant messages. If the information is deemed not relevant it is deleted soon after this assessment is made. This may happen at various stages: by the System administrator (following the suggestion of the Review officer) or after verification by the Investigative Unit. Altogether an irrelevant message may be kept up to a year.

The EDPS considers that OLAF intention to delete irrelevant messages as soon as this assessment is made is positive. The EDPS further encourages OLAF to keep the maximum period of conservation of this type of data as short as possible and in any event for no longer than a year.

If the information is deemed relevant and thus becomes part of an investigation file, it is kept for a period of 20 years, 10 years if it is exchanged with a Member State under Mutual Assistance, 3 years if it is exchanged with a Member State under irregularities and 5 years if it is classified as a non-case. The present Opinion does not address the adequacy of such data retention/conservation periods because the EDPS has already analysed the data retention periods of the processing operations undertaken by the investigative Units in different Opinions related to each type of case or investigation. For example, the EDPS has issued opinions commenting on the data retention periods used for internal investigations as well as follow up cases[18].

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.

The facts described in the Notification reveal that the transfer of the information collected through the FNS is limited to other Units within OLAF, thus, Article 7 of the Regulation applies. In particular, the messages are transferred to OLAF Investigative Units in Directorates A and B for their further analysis. The role of these Units can be deemed as a role of data processor which performs certain tasks on behalf of the data controller. The messages are also transferred to OLAF Investigative Units and the Operational Intelligence Units which may onward transfer them to Member States when they are deemed relevant for other Community or national bodies.

***Transfers to OLAF Investigative Units*:** Article 7 of Regulation (EC) No 45/2001 requires personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". The transfers of information to the Investigative Units in Directorates A and B for their further analysis seem to comply with this provision insofar as *(i)* the recipient has the appropriate competences to perform the further analysis and *(ii)* the transfer is necessary in order to ascertain whether the information reveals the existence of a

[18] See EDPS Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418) and 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 2006/0543, 2006/0544, 2006/0545, 2006/0546, 2006/0547).

wrongdoing. The same applies to the transfers to OLAF Investigative Units and the Operational Intelligence Units.

Transfers to Member States' Authorities: In the context of the further processing of the information, OLAF Investigative Units and the Operational Intelligence Units will send the information to third parties, including recipients subject to Directive 95/46 or not subject to that Directive. The EDPS considers that such onward transfers must be considered as taking place outside the scope of the data processing that occurs within the FNS, hence, they do not fall within the scope of this Opinion. These onward transfers take place in the context of the data processing operations for which these other Units are responsible. Such data processing operations have been prior checked by the EDPS and will be taken into account in such contexts[19] or are being dealt with in the context of cases 2005-154 and 2006-493, where the EDPS analyses the conformity of OLAF international data transfers.

2.2.7. Right of Access and Rectification

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the data controller. According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source. The information can then be obtained directly by the data subject (this is the so-called "direct access") or, under certain circumstances, by a public authority (this is the so-called "indirect access", normally exercised by a Data Protection Authority, being the EDPS in the present context).

As pointed out above regarding the right of information, in assessing whether the data controller for the case in point grants these rights to individuals, one must distinguish between two different types of data subjects: First, the individuals who use the FNS and choose to leave their personal data, second, any person named by a user of the FNS.

As to the FNS callers' right of access and rectification, the privacy statement declares that individuals have such a right regarding the information that OLAF holds about them. It gives the name and e-mail of the data controller as the contact person to exercise such rights as well as if individuals have further questions regarding the processing of their personal information. The practice as described in the privacy statement is in line with Article 13 of Regulation (EC) No 45/2001.

The Notification is silent regarding the right of access/rectification of those who have been named by users of the FNS. The EDPS reminds that under Article 13 of Regulation (EC) No 45/2001, such persons have the right of access and rectification and can call upon OLAF to implement such rights. However, such rights may be deferred if one of the conditions of sections (a), (b) and (c) of Article 20 (EC) Regulation No 45/2001 are present. The Article 29 Working Party's Opinion on Whistleblowing stressed that these rights "*may be restricted in order to ensure the protection of the rights and freedoms of others involved in the scheme*", which is the hypothesis foreseen under subsection (c) of Regulation (EC) No 45/2001 (see point 2.2.8 below).

---

[19] For example, such transfers may occur in the context of internal investigations, which were the subject of an EDPS Opinion on internal investigations, 23 June 2006 (Case 2005-418). Others may occur in the framework of external investigations or monitoring cases, both currently under analysis by the EDPS following the submission by the OLAF DPO of their respective notifications for prior check.

In the context of exercising the right of access, the EDPS would like to stress the Article 29 Working Party's recommendations pursuant to which *"Under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed".*

In order to ensure compliance with the above, the EDPS recommends that when access is granted, personal information of third parties, such as informants or whistleblowers, be deleted. If providing access, even if the personal information is deleted, may reveal personal details of third parties such as whistleblowers and informants, access should be denied.

2.2.8. Information to the Data Subject

Pursuant to Articles 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 has checked the content of the information provided in the privacy statement and considers it to be in line with the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001. Indeed, it contains information on the purposes of the processing, the recipients of the data, the existence of a right of access and the right to rectify, including the name of the contact person to exercise such rights. It also contains the time limits for storing the data and the right to have recourse to the European Data Protection Supervisor.

In addition to assessing the content of the privacy policy, it is also necessary to examine how the information is given and whether it is given to *all* data subjects whose personal data are collected in the context of the FNS. In this context, one must again distinguish between two different types of data subjects: First, the individuals who use the FNS and choose to leave their personal data; second, any person named by a person who uses the system.

Information Provided to Individuals who Use the FNS and Choose to Leave their Personal Data. The Notification refers to a privacy statement, intended to provide information to individuals who use the FNS. A link to the privacy statement will be placed on the home page of the FNS, within the OLAF Europa site.

It is not entirely clear where the privacy statement will be made available. In order to ensure that individuals who use the FNS are effectively provided with the information, the link to the privacy policy should be directly accessible at the web page through which visitors who want to use the FNS must necessarily go through or alternatively in a very prominent way, immediately after or before the information on the FNS. In addition to including the privacy policy in the page that informs about the use of the FNS, a link to the privacy policy could also be included in the on-line questionnaire and/or email correspondence with the informants. Other techniques such as the use of pop up windows may also be considered, provided that the content of the pop-up window can be printed out and stored for later use.

Information Provided to any Person Named by the User of the Fraud Notification Service: As explained above, the processing that occurs through the FNS does not only include those who use the FNS but also those who are named by the users of the FNS. According to the Notification if the persons named by the informants are used in an OLAF investigation or other case, they will be informed in the context of the case. However, the Notification says

that "*If the information is deleted because it is deemed not relevant, and has not become part of a case file, then it is not necessary to provide the information to named person on an individual basis*".

The EDPS recalls that *ex* Article 12 of Regulation (EC) No 45/2001 individuals whose names are mentioned by callers who use the FNS have the right to receive information about the processing of their data. In this case, the information regarding individuals named by the users of the FNS which is eventually deemed irrelevant may undergo a true processing. Indeed, whereas certain information will be automatically deleted upon its arrival using an automatic classification mechanism, other messages/information will be forwarded first to Review officers and then to investigators of Directorates A and B for the final confirmation of their relevance. The information may be dealt with, viewed, read and analysed by a number of investigators of such Directorates. Furthermore, all in all, this process may take up to one year during which information about this person will be kept by OLAF. For these reasons, for information that is not deleted automatically upon arrival, unless an exception applies (see below), no legal grounds appear to exist to justify the lack of provision of information to data subjects.

The existence of a similar obligation under the Data Protection Directive was highlighted by the Article 29 Working Party in its Opinion on whistleblowing schemes[20]: "*The person accused in a whistleblower's report shall be informed by the person in charge of the scheme as soon as practicably possible after the data concerning them are recorded*". OLAF should implement such an obligation.

The same Opinion recognises that "*where there is substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather the necessary evidence, notification to the incriminated individual may be delayed as long as such risk exists. This exception to the rule provided by Article 11 is intended to preserve evidence by preventing its destruction or alteration by the incriminated person. It must be applied restrictively, on a case-by-case basis, and it should take account of the wider interests at stake"*. Similar types of exceptions, subject to similar conditions, exist under Article 20 of Regulation (EC) No 45/2001. In particular, this Article provides for certain restrictions to the right of information notably where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences; (b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others."*

In the case in point, the application of Article 20 of Regulation (EC) No 45/2001 enables OLAF to defer the provision of information to safeguard the interests mentioned in subsections (a), (b) and (c). In practical terms this means that both when the information is deemed to be relevant and irrelevant OLAF will have to assess whether the provision of information to the person named by the user of the FNS would jeopardise the values mentioned above under subsections (a), (b) and (c) of Article Regulation (EC) No 45/2001, in which case the provision of information may be deferred. Particularly if the matter is deemed relevant, in some cases, OLAF is likely to be able to rely on section (a) of Article 20 of

[20] Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, adopted on 1 February 2006. According to the Article 29 Working Party, the individual must be informed about "[1] the entity responsible for the whistle blowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification".

Regulation (EC) No 45/2001. When the information is deemed to be irrelevant, in most cases, the EDPS questions the use of the exception (a) and (b) of Article 20 of Regulation (EC) No 45/2001. Under these circumstances, in principle, there will be neither an investigation *per se* to protect nor a financial interest at stake. Yet, OLAF may rely on section (c) if it considers that deferring the information is necessary in order to safeguard *"the protection of the data subject or of the rights and freedoms of others"*, for example, if it considers that the disclosure of information may reveal the identify of the whistleblower or informant which may be the case in a number of instances. In deciding whether OLAF is under the obligation to provide information or whether an exception applies, OLAF must engage in a case-by-case assessment of the circumstances of the particular data processing at stake.

If OLAF uses an exception to defer the provision of information, 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. (c) 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. (b) it must assess whether it is necessary to suspend giving information in order to safeguard an important economic interest. In making such an assessment, OLAF must take into account that an economic interest at stake in itself does not justify a need to suspend giving information. In other words, there must be a clear link between the need to suspend giving information and the safeguard of an economic interest. 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*". However, OLAF may avail itself of Article 20.5 to defer the provision of this information as set forth in this Article: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."*

2.2.9. Security Measures

The EDPS notes that OLAF has implemented certain security measures to prevent unauthorised disclosure and access, destructions, loss and unlawful processing. 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, as the analysis has been carried out in a different Opinion which addresses security issues only, with positive conclusions.

3. Conclusion

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

- If individuals leave messages with information that is pointless for the purposes at stake, such information should not be retained. Investigators should be made aware of this rule.
- In corresponding with OLAF via electronic messages, OLAF investigators should avoid asking questions that would lead informants to disclose information that is irrelevant for the purposes of detecting fraud and corruption affecting the financial interests of the Community. OLAF investigators should be made aware of this rule.
- There should be a description on the website where the Fraud Notification Service is available of the type of information that is relevant for OLAF in order to minimise that individuals report irrelevant and pointless information.
- As far as possible, the confidentiality of informants should be guaranteed throughout the life span of a case in as much as this would not contravene national rules regulating judicial procedures.
- The conservation period of irrelevant information should be kept as short as possible and in any event for no longer than one year.
- A link should be inserted in the privacy policy at the webpage through which visitors who want to use the Fraud Notification Service must necessarily go through or alternatively in a very prominent way, immediately after or before the information on the Fraud Notification Service. Also, consider inserting a link to the privacy policy in the on-line questionnaire and/or email correspondence with informants.
- It should be ensured that those people who have been named by the users of the Fraud Notification Service benefit from the right to information, subject to the application of the exceptions of Article 20 of Regulation (EC) No 45/2001. OLAF must decide on a case-by-case basis whether the exceptions apply. This applies also to individuals who have been named in messages deemed not relevant.
- The EDPS calls upon OLAF to ensure the right of access and rectification to those people who have been named by the users of the Fraud Notification Service. The EDPS recalls that in some cases, the exceptions of Article 20 of Regulation (EC) No 45/2001 may apply.

Done at Brussels, 18 December 2007

Peter HUSTINX
European Data Protection Supervisor