Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations

Brussels, 23 June 2006 (Case 2005-418)

1. Proceedings

On 3 January 2006, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) a notification for prior checking relating to OLAF internal investigations. A document with the title *Memorandum in Support of Notification for Prior Checking with the European Data Protection Supervisor Pursuant to Article 27 of Regulation 45/2001 Concerning OLAF's Processing of Personal data in the Context of Internal Investigations* ("the Memorandum") was also enclosed.

The EDPS requested OLAF to provide some complementary information on 14 February, 10 March and 11 April 2006. The answers were received on 2 March, 23 March and 17 May, respectively. On 23 March the period to deliver the Opinion was extended for 2 months, based on Article 27.4 of Regulation (EC) no. 45/2001.

On 7 April 2006 a meeting among the Assistant EDPS, EDPS staff members and OLAF staff members took place. On that occasion, relevant information for the present case was gathered. Another source of information considered for the elaboration of this Opinion is the OLAF Manual, version 2005.

2. Examination of the matter

2.1. The facts

2.1.1. Scope of internal investigations

- Purpose of data processing activities

Internal administrative investigations[1] are conducted to determine whether fraud, corruption or any other illegal activity affecting the financial interests of the European Community have occurred, or whether serious matters relating to the discharge of professional duties such as to constitute a dereliction of the obligations of officials and other servants of the Communities

[1]Internal investigations are one type of the investigations conducted by OLAF. The other ones are described in point 3.3.3.1 of the OLAF Manual as follows: External investigations; Coordination cases; Criminal assistance cases; Monitoring cases; Non-cases; and Prima facie non-cases.

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

liable to result in disciplinary or criminal proceedings have occurred, and if so, to refer the results of OLAF's investigation to the appropriate national or Community authorities for judicial, disciplinary, administrative, legislative or financial follow-up. In the areas mentioned above (Article 1 of Regulation (EC) No. 1073/1999), OLAF shall carry out administrative investigations within the institutions, bodies, offices and agencies (this is referred to as "internal investigations" in Article 4 of Regulation (EC) No. 1073/1999).

- The competence of OLAF and the Appointing Authorities of EU institutions and bodies *vis-à-vis* administrative investigations

Article 86 of the Staff Regulations empowers both OLAF and the Appointing Authority to conduct administrative investigations to determine whether disciplinary violations have occurred.

Concretely, in the case of the European Commission, the competence of IDOC[2] is specified in Article 2, paragraph 1 of the Commission Decision on General implementing provisions on the conduct of administrative inquiries and disciplinary procedures (No 86-2004 of 30.06.2004), which establishes IDOC. The Decision indicates that IDOC is responsible primarily to carry out "administrative inquiries", defined as all actions taken by the authorized official to establish the facts and, where necessary, determine whether there has been a failure to comply with the obligations incumbent on Commission officials, and to carry out disciplinary procedures.

In contrast, the competence of OLAF is specified in Articles 1 – 4 of Regulation (EC) No. 1073/99. Regarding discharge of professional duties' matters, OLAF is responsible to investigate serious facts linked to the performance of professional activities which may constitute a breach of obligations by members, officials and servants of the Communities likely to lead to disciplinary and/or criminal proceedings. OLAF has no competence to conduct disciplinary procedures. Rather, it prepares a final case report recommending disciplinary action, in cases where this is appropriate. The disciplinary procedures are then conducted by IDOC and other Appointing Authorities of EU institutions and bodies.

Indeed, Article 1, paragraph 3, second indent of Regulation (EC) No. 1073/99 states in part that within the institutions, bodies, offices and agencies, OLAF shall conduct administrative investigations of *"serious matters relating to the discharge of professional duties such as to constitute a dereliction of the obligations of officials and other servants of the Communities liable to result in disciplinary or, as the case may be, criminal proceedings, or an equivalent failure to discharge obligations on the part of members of institutions and bodies, heads of offices and agencies or members of the staff of institutions, bodies, offices or agencies not subject to the Staff Regulations of officials and the Conditions of employment of other servants of the European Communities."* However, the regulation does not define what is meant by the words "serious matters".

As a practical matter, the OLAF Investigations and Operations Executive Board considers, on a case-by-case basis, whether the initial information received by OLAF constitutes a "serious matter", with guidance from the criteria listed in its operational priorities, in Section 3.2 of the OLAF Manual. Regarding internal investigations, the following criteria are listed under Section 3.2.1.1:

[2] The internal administrative inquiries and disciplinary procedures conducted by IDOC (Investigatory and Disciplinary Office within the European Commission) have been submitted to prior check (case 2004-187). The Opinion of the EDPS has been issued on 20 April 2005.

* Whether serious criminal or disciplinary offences are potentially involved;
* The likely financial impact;
* Whether it involves a conspiracy or a single actor;
* Whether senior officials are involved;
* Whether it involves an abuse of power;
* Whether the matter could have a negative impact on the reputation/credibility of European institutions and bodies;
* Whether an investigation has been requested by a service or institution.

However, there is a substantial area of overlap in the competences of OLAF and IDOC (and other internal investigatory bodies of the EU institutions and bodies). For this reason, the Commission Decision establishing IDOC specifies that before opening an inquiry, IDOC must consult OLAF to ascertain whether it is undertaking or intends to undertake an investigation on the same matter. If this is the case, IDOC cannot open an investigation. If OLAF has finalized its inquiry, then the Appointing Authority (through IDOC) is free to conduct an inquiry on its own, the reason being that the Appointing Authority is not bound or limited by OLAF's findings and assessments.

In practice, OLAF concentrates primarily on those cases that correspond to its core business – financial irregularities.

- Role of OLAF concerning investigations of its staff

As indicated above, Article 86 paragraph 2 of the Staff Regulation specifies that where the Appointing Authority (AIPN) or OLAF becomes aware of evidence of failure of an official or former official to comply with his obligations under that Regulation, they may launch administrative investigations to verify whether such failure has occurred. Thus, an administrative investigation (pre-disciplinary) against an OLAF staff member may be conducted either by OLAF or by IDOC, which acts on behalf of the Commission's AIPN on disciplinary matters. If the investigation is conducted by IDOC, the procedures foresee that OLAF will not intervene other than to respond to IDOC's requests for information or interviews.

The disciplinary procedures specified in Annex IX of the Staff Regulation are applied with respect to OLAF officials and other servants, as for any other Commission officials or other servants. Those procedures indicate the role of AIPN at various stages. The AIPN for OLAF is the Director General of OLAF. However, for purposes of conducting disciplinary proceedings, the role played by the Director General for OLAF, and the role played by the Director General for Personnel and Administration (who is the AIPN for the Commission) is spelled out in detail in Annex III of Commission Decision C(2004)2286/3 (Administrative Notice No. 99-2004, 19.7.2004), pp. 47-49.

2.1.2. Data processing in internal investigations

- Categories of data subjects

The categories of data subjects involved in this processing activity are the following: personnel of the EU institutions, bodies, offices and agencies who are the subject of the investigation or otherwise involved in the matters under investigation, either as whistleblower or witness; persons outside of the EU institutions, bodies, offices or agencies who may be involved in the matters under investigation, either as informants or witnesses.

- Categories of data

The categories of data processed are: name, address, telephone number, e-mail address, date of birth, nationality, employer, marital status, children, professional position, statements made regarding events under investigation by the person or about the person, evidence mentioning the person and notes regarding the relation of the person to the events under investigation.

The notification form specifies that special categories of data (those referred to in Article 10.1 of the Regulation) are not processed in the context of OLAF internal investigations. The EDPS has been informed that only very exceptionally, there may be ad hoc circumstances where, due to the subject matter under investigation (e.g. access to reimbursement of expenditures from health insurance systems), such data may be processed.

The personnel number of an official under investigation is normally included in the final case report in order to be absolutely certain that the person under investigation is identified without ambiguity.

- Collection of personal data

Once the decision is taken to open the investigation, OLAF is empowered to have immediate and unannounced access to any information and to the premises of the Community organ concerned; to inspect accounts; to take a copy of and obtain extracts from any documents or the contents of any data medium and to assume custody of such documents or data; to request oral information from members and staff; to carry out on-the-spot inspections at the premises of economic operators according to Regulation 2185/96; and to ask any person for information. The evidence added to the file is of charge and discharge.

- Forensic examination of computers

The OLAF Manual defines it in point 3.4.4.2 as "[i]mmediate and unannounced access to the contents of a computer belonging to a Community organ which has been made available to an official exclusively for the performance of his duties. It includes the right to take the computer or a copy of the contents of the computer's storage devices."

An *Investigation Authority* form must be completed and signed by Director B of OLAF before the computer search is executed. In addition, a *Note to the Secretary General* of the Community organ concerned should be presented.

A technical expert from Unit C.3 of OLAF, in conjunction with the investigator in charge of the investigation, should conduct the search. The *Appointment of case team* form should include the names of any technical experts that will carry out such activities. The computer storage devices should be "disk imaged". The OLAF Manual further points out that it is important that a technical expert does this, as the evidence collected may otherwise be inadmissible. The official concerned need not be present during a search of his computer.

OLAF's DPO has informed that, in general, several basic principles are observed[3]:

[3] It has to be noted that those principles are neither contained in any official OLAF document, nor further developed in a "Standard Operating Procedures" Protocol.

Principle 1
No action taken by Law Enforcement agencies or their agents should change data held on a computer or storage media, which may be relied upon in court.
Principle 2
In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person MUST be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3
An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4
The person in charge of the investigation (the case handler) has overall responsibility for ensuring that the law and these principles are adhered to.

The EDPS has also been informed that each member of the OLAF Technical Assistance Team - the personnel who conduct forensic examination of computers - has more than 10 years' experience in computer technology prior to specialising in computer forensics. The DPO has expressed that, as certified forensic computer examiners, they continuously upgrade their knowledge and skills by attending courses provided by computer forensic, equipment and software companies and by the International Association of Computer Investigative Specialists, an independent organisation.

- The handling of files

-Electronic files

A central database, the Case Management System (CMS), is used to manage all OLAF's operational cases. All cases within the CMS are identified by a specific Operational File (OF) number. Whenever a new case is opened, an OF number is assigned. If the matter is within OLAF's competence, an assessment is initiated.

The CMS is the electronic means by which all significant events concerning a case are recorded. In particular:

*Significant events, administrative information, or intelligence relating to the case are recorded in a series of fields within the CMS. 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.

*All registered documents relating to a case are scanned and added to the CMS case file by means of the electronic document management system.

*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.

Each case handler is responsible for updating the system in a timely manner and monitoring the completeness of details and documentation for his cases. Case handlers are required to document each investigative step and significant event to ensure a thorough documentation of the investigation.

-Paper files

The OLAF Greffe maintains the official file in paper form for all cases in a uniform manner, in compliance with the Commission Decision on Document Management.[4] Accordingly, only one official file is maintained for each case and all documents in the file, including all working papers that contain important information which is not short-lived, must be originals and must be registered. Every investigation file must be paginated in continuous order.

Investigators may keep their own working files for the cases assigned to them, containing only copies of documents, while the investigation is ongoing. When the investigation is closed, the investigators must hand over their files to the Greffe, which will compare the two sets of files and destroy duplicate documents. Similarly, when the follow-up phase is closed, the follow-up agent should hand over to the Greffe all case-related documents, which the Greffe will treat in a similar manner.

- Conservation of data

OLAF may keep both electronic and paper files relating to internal investigations for up to 20 years after the date on which the investigation was closed.

In order to allow for the comparison of precedents and the compilation of statistics, final case reports of internal investigations may be kept in anonymised form for 50 years.

OLAF has informed the EDPS that national judicial proceedings may take a number of years to reach a conclusion, and that OLAF must retain the integrity of its investigation files until such proceedings, including all possible appeals, are concluded. OLAF has also expressed that the OLAF investigation file may be relevant to disciplinary proceedings of the person concerned during the full duration of his employment and pension rights.

- Transfers of data

-Transfers of data may be made:

*To concerned Community institutions, bodies, offices or agencies, in order to allow them to take appropriate measures to protect the financial interests of the Community, in accordance with paragraphs 9(4) and 10(3) of Regulation 1073/99[5] (and as spelled out in section 3.5.3 of the OLAF Manual);

*To competent Member State judicial authorities, in order to allow them to take appropriate judicial follow-up measures, in accordance with paragraph 10(2) of Regulation 1073/99 (and as spelled out in section 3.5.5 of the OLAF Manual);

*To competent third country authorities and international organisations (as spelled out in section 3.5.6 of the OLAF Manual).

-Content of the final case report to be transmitted either to judicial or disciplinary authorities

[4] Commission Decision 2002/47/EC, ECSC, Euratom, OJ L 21, 24.1.2002, p. 23.
[5] Regulation (EC) No. 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), O.J. L 136, 31.5.1999, p. 1-7.

At the conclusion of an investigation, the investigator in charge must prepare a Final Case Report, presenting the findings and conclusions of the investigation. After an internal investigation, this report will be sent to the judicial and/or disciplinary authority concerned. OLAF points out that, usually, there is no difference in the information sent to disciplinary and judicial authorities. If an investigation leads to both disciplinary and judicial follow-up, the same report is sent to both authorities. In some cases the versions of the reports vary slightly in order to focus on the information needed by each authority. The documents attached to the report are those which would constitute evidence of the findings of the report. As stated above, the evidence included is of charge and discharge.

Disciplinary and judicial authorities, as well as the lawyer of the defendant, can possibly ask for further information if relevant. In any case, documents of pure internal nature are not included in the final case report.

The elements of the report are the following:

i. Case history: Specifies the date on which the investigation was opened, the EU institution and official involved (for internal cases) or natural or legal persons involved (for external cases), the area concerned, the initial source of information.

ii. Executive summary: Provides a brief explanation of the fraud or irregularity alleged, the scope of the investigation and the main results of the investigation. It should state whether the facts confirm the allegation.

iii. Recommendation for follow-up: Makes a proposal as to which OLAF units or external bodies should execute the follow-up activities.

iv. Result of the investigation: This is the centrepiece of the final case report, describing the steps taken and the facts gathered during the investigation. It should state whether the facts confirm the allegations.

v. Legal evaluation of the facts: Specifies the legal provisions infringed by the subject of the investigation. All requirements of the legal provision should be specified and applied to the facts gathered during the investigation to demonstrate the violation.

vi. Conclusions and recommendations: Outlines the appropriate follow-up to the investigation, such as referring the case to the competent national authorities, the Commission's disciplinary authority, and/or the competent service to launch a recovery procedure.

- Information given to the data subjects and further guarantees

-Person concerned

Article 4 of the Model Decision annexed to the Inter-institutional Agreement concerning internal investigations by OLAF[6] provides:

[6] Inter-institutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Ant-fraud Office (OLAF), O.J. L 136, 31.5.1999, p. 15. The 'Model Decision' concerns the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any illegal activity detrimental to the Communities' interests.

"Where the possible implication of a member, manager, official or servant emerges, the interested party shall be informed rapidly as long as this would not be harmful to the investigation. In any event, conclusions referring by name to a member, manager, official or servant of (the institution, body, office or agency) may not be drawn once the investigation has been completed without the interested party's having been enabled to express his views on all the facts which concern him.
In cases necessitating the maintenance of absolute secrecy for the purposes of the investigation and requiring the use of investigative procedures falling within the remit of a national judicial authority, compliance with the obligation to invite the member, manager, official or servant of (the institution, body, office or agency) to give his views may be deferred in agreement with the President or the Secretary General respectively."

OLAF will notify the person concerned ("interested party" in the terminology used by OLAF documents to refer to the person under investigation) at various stages of an internal investigation: at the initial phase, to arrange an interview, and at the close of the case.

*Initial information:

Article 4 of the Model Decision attached to the Inter-institutional Agreement (and consequently the internal decisions of the Community institutions, bodies, offices and agencies) and Article 1 of Annex IX of the Staff Regulations establish that the interested party has the right to be informed of his/her possible implication in an investigation under certain specified circumstances. An official who may be implicated must be informed "rapidly" if it would not be harmful to the investigation to do so. In practical terms, a letter is sent from OLAF to the person concerned, emphasising that, in accordance with Article 4 paragraph 6(a) and (b) of Regulations 1073/99 and Article 1 of the Model Decision, he has a duty to cooperate with and supply information to the Office, unless this infringes his/her right not to incriminate himself; providing a summary of the allegations; indicating the possibility to produce documents or provide oral evidence; and indicating he/she will, in due course, receive an invitation for an interview providing him an opportunity to express his/her views on all the facts which concern him. This initial information is sent to the interested party as soon as OLAF opens an investigation, unless it would be detrimental to the investigation to do so (as discussed below). It may also be sent when it becomes apparent, within the framework of an existing investigation, that a Member, official or servant of an EU institution is involved. OLAF may defer providing this initial information to the interested party in cases where doing so would be detrimental to the investigation. In practice, the OLAF Head of Unit in charge of the case, having consulted with Director of Investigations and Operations, will justify in writing the reasons for deferral of this notice in a Note to the file. This document will be added to the case file.

*Notice of interview:

Article 4(1) of the Model Decision and Article 1 of Annex IX of the Staff Regulations provide that conclusions may not be drawn referring by name to a member, official or servant of a Community organ once the investigation has been completed, without first giving the interested party the opportunity to express his views on all the facts which concern him. Thus, the interested party is normally invited for an interview before conclusions are drawn which refer to him by name in a final case report. The letter of invitation informs the person that the interview may lead to one or more of the following outcomes: no further action; financial recovery; referral of the matter to the disciplinary authorities of the Community organ concerned; and/or referral of the file to the judicial authorities.

The letter must advise the interested party that an attorney or other person of his/her choice may represent him during the interview; he is not obliged to make self-incriminating statements; he may request, in advance that the interview be carried out in any official Community language; an official written record of the interview will be made; his statement, together with the official record of the interview, may be used as evidence in a disciplinary or court procedure; he/she may request that the documents he has produced be annexed to the interview record and sent with the case papers to the judicial authorities or to IDOC.

At the interview, the following statement is read: "The interview is being conducted by [names of the investigators] at [location] on [date] at [time]. The interviewee is [name]; the other persons present are [names]. The purpose of this interview is to gather information as to [subject]. You have the right to speak in any of the official Community languages; the right to have a legal or other representative present; and the right not to incriminate yourself. You may request that any documents you produce be appended to the official record of this interview. You will be provided with a copy of the record of this interview, including all annexes. It may be used as evidence in any administrative, disciplinary, legal or penal procedures."

However, in accordance with Article 4(2) of the Model Decision (and the analogous provisions of all of the internal decisions), in cases necessitating the maintenance of absolute secrecy and requiring means of investigation falling within the competence of national judicial authorities, OLAF may, with the agreement of the Community organ concerned, decide to defer inviting the interested party to express his/her views. Whenever the Director General of OLAF (or Director B, acting on his behalf) decides to defer inviting the interested party for an interview, there is no legal obligation to inform the person concerned of this decision.

*Information at closure of internal investigation: two scenarios are possible:

First, the case may be closed without follow-up. In this case, in accordance with Article 5 of the Model Decision and Article 1(3) of Annex IX of the Staff Regulations, the interested party will be informed by a letter from the Director General of OLAF (or the Director B, acting on his behalf), stating that the case has been closed without follow-up action. Article 1(3) of Annex IX of the Staff Regulations also requires that the official's institution be notified in writing that the case has been closed with no follow-up. In practical terms, a copy of the letter sent to the official should also be sent to the Secretary General of his institution. This Article also provides that the official may request that the decision be inserted in his/her personal file.

Second, the case may be closed with follow-up. In this case, a letter from the Director General (or the Director B, acting on his behalf) will normally be sent to the interested party, informing him/her that the case has been passed on, unless this would be detrimental to the follow-up action.

-Whistleblowers

Whistleblowers are EU officials and other EU Staff (temporary staff, auxiliary staff, local staff, contract staff and special advisers) of the Community organs who come forward to OLAF with information they have discovered in the course of or in connection with their duties concerning matters which may be within OLAF's competence.

Their rights and obligations are described in the Staff Regulations:

Article 22.a): *"1. Any official who, in the course of or in connection with the performance of his duties, becomes aware of facts which gives rise to a presumption of the existence of possible illegal activity, including fraud or corruption, detrimental to the interests of the Communities, or of conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the obligations of officials of the Communities shall without delay inform either his immediate superior or his Director-General or, if he considers it useful, the Secretary-General, or the persons in equivalent positions, or the European Anti-Fraud Office (OLAF) direct.*

Information mentioned in the first subparagraph shall be given in writing.

This paragraph shall also apply in the event of serious failure to comply with a similar obligation on the part of a Member of an institution or any other person in the service of or carrying out work for an institution.

2. Any official receiving the information referred to in paragraph 1 shall without delay transmit to OLAF any evidence of which he is aware from which the existence of the irregularities referred to in paragraph 1 may be presumed.

3. An official shall not suffer any prejudicial effects on the part of the institution as a result of having communicated the information referred to in paragraphs 1 and 2, provided that he acted reasonably and honestly.

4. Paragraphs 1 to 3 shall not apply to documents, deeds, reports, notes or information in any form whatsoever held for the purposes of, or created or disclosed to the official in the course of, proceedings in legal cases, whether pending or closed."[7]

A Commission Communication (SEC/2004/151/2) of 6 February 2004 from Vice-President Kinnock, 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]nformation relating to the identity of the whistleblower will be treated in confidence".

As specified in section 3.3.2.2 of the OLAF Manual, upon receipt of information from a whistleblower, he/she will be advised in writing of his rights and obligations pursuant to the provisions of the Staff Regulations related to whistleblowers, and of the period of time within which OLAF will take appropriate action. This must occur within 60 days from the date on which the official reported the concern.

If interviewed, he/she will receive an invitation to the interview which contains information similar to that described above for the interested party, with appropriate adjustments; at the interview, a similar statement will be read to him/her.

[7] Furthermore, Article 22.b) foresees that, provided some conditions are met, an official can further disclose information to the President of the Commission or of the Court of Auditors or of the Council or of the European Parliament, or to the European Ombudsman, and that shall not suffer any prejudicial effects on the part of the institution to which he belongs.

Whenever a case is regarded as a non-case or, after investigation, is closed without follow-up, the source is systematically informed about this.

-Informants

An informant is an individual who seeks to disclose information concerning a matter within OLAF's competence which has already occurred or is ongoing, who has obtained the information as a consequence of a business or personal relationship, often involving a duty of confidence; who seeks to ensure that disclosure of his identity is withheld, and who is not an official or servant of a Community organ.

Any OLAF official having contact with an informant must assure him that while the Office will make its best effort to respect his desire for anonymity, it cannot guarantee anonymity once the case has been passed to national judicial or prosecution authorities. [8]

Information is provided to informants in accordance with the relevant Member State legal framework governing dealings with informants.

If interviewed, he/she will receive an invitation to the interview which contains information similar to that described above for the interested party, with appropriate adjustments; at the interview, a similar statement will be read to him/her.

Whenever a case is regarded as a non-case or, after investigation, is closed without follow-up, the source is systematically informed about this.

-Witnesses

A witness is an individual who is not an interested party and who provides information concerning a matter within the legal competence of OLAF either in respect of a situation which has already occurred or which is ongoing. Witnesses do not request or require anonymity. The preamble of the record of a witness interview, which is signed by the witness, informs him that his/her testimony may be used in any further criminal, disciplinary or administrative procedure.

If interviewed, he/she will receive an invitation to the interview which contains information similar to that described above for the interested party, with appropriate adjustments; at the interview, a similar statement will be read to him/her.

- Right of access

The notification form and the OLAF Manual point out that the interested party (or his lawyer or other representative) has no right of full access to the OLAF investigation file. This right is provided at a later stage, either during the disciplinary proceeding, when he has a right to “all documents directly related to the allegations made against him,” (Article 2 of Annex IX of the Staff regulations) or during the national judicial proceedings.

According to the information provided by OLAF DPO, as any other member of the public, the interested party may apply for access to documents pursuant to Regulation 1049/2001. However, during the course of the investigation, access would in most cases be denied based

[8] It has to be noted that the use given to the word "anonymity" in the OLAF Manual while referring to informants is that of "confidentiality of his/her identity", what is not the same sense as the one given to "anonymous data" in the Regulation, which indeed excludes the application of this instrument.

on the investigations exception specified in Article 4(2), third indent, as well as the protection of privacy and personal data exception in Article 4(1)(b), and possibly other exceptions. At the close of the investigation, access may be granted in some cases, provided that doing so would not harm follow-up proceedings (such as national judicial proceedings). The names of data subjects and any other personal data would normally be removed before disclosing any document in response to a request under Regulation 1049/2001.

During the meeting with OLAF staff members, it was clarified that the data subject has no right of full access to all the documents in the investigation file because OLAF must observe its obligation of professional secrecy with respect to the information it gathers during an investigation, as specified in Article 8 of Regulation 1073/99. There is no legal basis, among OLAF legal instruments, for providing a data subject – be it the person concerned, whistleblower, informant or witness – with access to all documents in the investigation file. In addition, such files often include personal data of more than one data subject (e.g., the person under investigation and the whistleblower). In any case, OLAF staff members added, if a data subject should request access to his own personal data undergoing processing by OLAF, pursuant to Article 13(3) of Regulation 45/2001, the general rule applied is the provision of access to the personal data of the data subject, unless this access would be harmful to the investigation, which is decided on a case-by-case basis.

The notification form expresses that in cases where a data subject requests access, rectification, blocking, erasure, or information as to notification to third parties from OLAF pursuant to Articles 13 through 17 respectively, OLAF may have to restrict application of these articles in accordance with the exemptions set forth in Article 20(a) or (b). It is said that it may be difficult for OLAF to respond to such requests when an investigation is ongoing, as even revealing the fact that the investigation exists may be harmful to its purpose. Providing any details as to why the exemptions may apply to the data subject at the time of his request may be even more difficult.

- Security

Security measures have been adopted in order to protect both paper and electronic files.

[...]

2.2. Legal aspects

2.2.1. Prior checking

The prior checking relates to the processing of personal data in the context of internal administrative investigations by OLAF (Articles 2(a) and (b) of Regulation (EC) No 45/2001 (hereinafter "the Regulation"). The processing activity is carried out by a European institution, in the framework of Community law[9] (Article 3.1 of the Regulation). The processing of personal data is done partly by automatic means (Article 3.2 of the Regulation). As a consequence, the Regulation is applicable.

The following prior check will not analyse the transfers of data to third countries or/and to international organizations. This issue is being dealt with in the context of case 2005-0154, in

[9] Particularly in the context of administrative investigations the Regulation is of application, regardless of the fact that this would lead to a criminal investigation conducted by national judicial authorities.

the framework of which the EDPS analyses the conformity of OLAF international transfers with the Regulation.

Article 27.1 of the Regulation subjects to prior checking by the EDPS all *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes".* Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks.

Article 27.2(b) of the Regulation stipulates that operations relating to "evaluate personal aspects relating to the data subject, including his or her (...) conduct" shall be subject to prior checking by the EDPS. In the case under analysis, the conduct of the officials is analysed by OLAF.

Furthermore, under Article 27.2(a) of the Regulation, 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, the processing operation could be related to the processing of this type of data.

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

The notification of the DPO was received on 3 January 2006. According to Article 27(4) the present Opinion must be delivered within a period of two months. Complementary information was requested on 14 February, 10 March and 11 April 2006. The answers were received on 2 March, 23 March and 17 May, respectively. Given the complexity of the subject matter analysed in this ex-post prior check, the EDPS has decided to extend the period to deliver his Opinion for two months, decision which was taken on 23 March 2006. The procedure was suspended during 71 days. The Opinion will therefore be adopted no later than 3 July 2006.

2.2.2. Legal basis for and lawfulness of the processing

The processing of data in the context of internal administrative investigations is based on Article 4 of Regulation 1073/1999 and Article 2 of Commission Decision 1999/352.

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").

These internal investigations shall be carried out subject to the rules of the Treaties, in particular the Protocol on privileges and immunities of the European Communities, and with due regard for the Staff Regulations under the conditions and in accordance with the procedures provided for in this Regulation and in decisions adopted by each institution, body, office and agency. The institutions shall consult each other on the rules to be laid down by such decisions.

2. Provided that the provisions referred to in paragraph 1 are complied with:

- the Office shall have the right of immediate and unannounced access to any information held by the institutions, bodies, offices and agencies, and to their premises. The Office shall be empowered to inspect the accounts of the institutions, bodies, offices and agencies. The Office

may take a copy of and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies and, if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearing,

- 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. Under the conditions and in accordance with the procedures laid down by Regulation (Euratom, EC) No 2185/96, the Office may carry out on-the-spot inspections at the premises of economic operators concerned, in order to obtain access to information relating to possible irregularities which such operators might hold.

The Office may, moreover, ask any person concerned to supply such information as it may consider pertinent to its investigations.

(...)

6. Without prejudice to the rules laid down by the Treaties, in particular the Protocol on privileges and immunities of the European Communities, and to the provisions of the Staff Regulations, the decision to be adopted by each institution, body, office or agency as provided for in paragraph 1, shall in particular include rules concerning:

(a) a duty on the part of members, officials and other servants of the institutions and bodies, and managers, officials and servants of offices and agencies, to cooperate with and supply information to the Office's servants;

(b) the procedures to be observed by the Office's employees when conducting internal investigations and the guarantees of the rights of persons concerned by an internal investigation."

The relevant part of Article 2 of Commission Decision 1999/352 foresees 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 Officials of the European Communities and the Conditions of Employment of Other Servants of the Communities. (...)"

Taking into account this legal basis, the lawfulness of the processing operation must be considered. Article 5(a) of the Regulation stipulates that personal data may be processed only if: *"processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed"*. Article 5(b) of the Regulation stipulates that personal data may be processed only if: *"processing is necessary for compliance with a legal obligation to which the controller is subject"*. The instruments quoted above show that the administrative investigations conducted by OLAF are tasks carried out in the public interest (combat fraud, corruption, etc., as pointed out in Article 2 of Commission Decision 1999/352). Furthermore, OLAF carries out those activities in the

legitimate exercise of official authority (Article 4 of Regulation 1073/1999) and thus is complying with its legal obligation to investigate matters within its scope of competence. The "necessity" of the processing has to be analysed *in concreto*. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the investigations has to be proportional to the general purpose of processing (combat fraud, corruption, etc., as pointed out in Article 2 of Commission Decision 1999/352) and to the particular purpose of processing in the context of the case under analysis (considering, for instance, the seriousness of the fact under investigation, the sort of data needed to clarify the facts, etc.). Thus, the proportionality has to be evaluated on a case-by-case basis.

2.2.3. Processing of special categories of data

Article 10.5 stipulates what follows: *"[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.

Apart from that, according to Article 10.1 of the Regulation, the processing of special categories of data (that is *"data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life"*) is prohibited. The Regulation foresees certain exceptions in Article 10(2). However, it seems most likely that, if any exception would apply, only those of sub-paragraph (b) or (d) would possibly be relevant.

In any case, consideration will also be given to Article 10.4 of the Regulation if necessary, which stipulates that: *"[s]ubject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor".*

Indeed, the type of data described in Article 10.1 would only be processed exceptionally. However, it could happen, for instance, that while conducting forensic examinations of computers, e-mails exchanged by the data subject with trade unions or with the EU Sickness insurance scheme may be found, revealing political opinions or data concerning health respectively. In the event that this happens, the general rule of Article 10.1 has to be respected, or, otherwise, it has to be evaluated in a restricted manner whether the application of an exception would be "necessary". In any case, OLAF staff in charge of the files must be aware of this rule and avoid the inclusion of special categories of data unless one of the circumstances foreseen in Article 10.2 (in a restricted sense, as mentioned above) is present in the particular case under investigation or Article 10.4 is to be applied.

2.2.4. Data Quality

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

Even though certain standard data will always be present in the internal investigation files such as the name, date of birth, etc., the precise content of a file will of course be variable according to the case. Guarantees must however be established in order to ensure the respect

for the principle of data quality. This could take the form of a general recommendation to the persons handling the files reminding them of the rule and recommending them to ensure the respect of the rule.

This principle is also of relevance in the processing involved in forensic examinations of computers. Regarding seizures in physical premises, the OLAF Manual expresses in point 3.4.4.1 : "[a]ddress books or diaries that are found on the premises may be considered to be used for professional purposes and may be seized if relevant to the goal of the inspection, unless it is clearly indicated that they are used only for private purposes. Wallets, handbags, and obviously private papers should not be seized." These precautions should also be taken regarding the access to the contents of a computer belonging to a Community institution or body since it may also contain files used by the data subject for private purposes (for instance in the folder "My documents", or e-mails marked as "private"), or files not relevant or excessive for the purposes of the investigation. The EDPS welcomes the existence of particular authorization mechanisms to allow the conduction of such computer forensic examinations. Moreover, the EDPS recommends in this regard that whenever the access to files that are apparently of a private nature appears to be necessary for the investigation, this access be conducted respecting adequate guarantees, and considering any potential risk of inadmissibility of the evidence in a possible future criminal case that could arise if the fundamental rights to privacy and personal data protection are not respected in the collection of evidence (see point 2.2.10 below). Furthermore, the EDPS recommends the adoption of a formal Protocol of "Standard Operating Procedures" for the conduction of computer forensics investigations by OLAF, which will also contribute to the safeguard of the data quality principle (see point 2.2.10 below).

Finally, the enumeration made in point 2.1 of the present opinion concerning the categories of data mentions two items, "marital status" and "children", that do not seem, in principle, relevant for an internal investigation. The EDPS recommends the suppression of them as standard practice, unless evidence exists suggesting their relevance to the case under investigation.

According to Article 4.1(d) of the Regulation, 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 2.2.8 below). Furthermore, an investigation system that guarantees the inclusion of evidence of charge and discharge as the one being analyzed is of relevance as concerns the accuracy and the completeness of the data being processed. This particular characteristic of the evidence is mentioned neither in Regulation 1073/99 nor in the OLAF Manual, but it was clarified during the meeting referred to in point 1 of the present Opinion. As a consequence, and considering its importance from a data quality perspective, the EDPS recommends its inclusion in the next version of the OLAF Manual. Moreover, the EDPS welcomes the inclusion of Article 7*a*.1 in the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), insofar as it specifies that in its investigation the Office shall seek evidence for and against the person concerned[10].

[10] The EDPS will issue his formal opinion once the adopted Proposal is sent to him under Article 28(2) of the Regulation.

Data must also be *"processed fairly and lawfully"* (Article 4.1(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, considerable attention must be paid to this in the context of such a sensitive subject. It is related to the information given to the official who is the subject of an investigation (and other data subjects), and the speed with which this information is given, so that the right of defence can be respected (see point 2.2.9 below)

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. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes"* (Article 4(1)(e) of the Regulation).

The legal basis for the conservation period of 20 years applied by OLAF is:

- Article 10(2) of Regulation 1073/99 (which indicates that OLAF shall forward to national judicial authorities the information obtained during internal investigations into matters liable to result in criminal proceedings).

- Article 10(3) of Regulation 1073/99 (which indicates that OLAF may at any time forward to the institution, body, office or agency concerned the information obtained during internal investigations), together with Article 10(h) and (i) of Annex IX of the Staff Regulations, which relate to the determination of the penalty to be imposed in disciplinary proceedings.

The DPO has expressed that, as a practical matter, OLAF has only been in existence since 1999, and thus has no experience to date as to whether a 20 year conservation period is sufficient or excessive. "At this point, it is our best estimate of the reasonable period required to meet our legal obligations under Article 10 of Regulation 1073/99. Experience may teach that this period should be changed". Considering these reasons, the EDPS suggests that when OLAF has experienced 10 years of existence a preliminary evaluation of the necessity of the 20 years period *vis-à-vis* the purpose of such conservation frame should be conducted. A second evaluation will be conducted when OLAF has experienced 20 years of existence.

Moreover, the EDPS would like to point out that in those situations where the case is "closed without follow-up", the period of 20 years is excessive, since it will not be necessary either for judicial or disciplinary investigations. From this perspective, the conservation period should be reduced for the mentioned cases to the time during which an action for liability of whistleblowers, informants or witnesses could be intended.

2.2.6. Transfer of data

- **Transfer of personal data within or between Community institutions or bodies**

Article 7.1 of the Regulation stipulates: *"Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".*

Article 9.4 of Regulation 1073/99 foresees: *"Reports drawn up following an internal investigation and any useful related documents shall be sent to the institution, body, office or agency concerned. The institution, body, office or agency shall take such action, in particular disciplinary or legal, on the internal investigations, as the results of those investigations warrant, and shall report thereon to the Director of the Office, within a deadline laid down by him in the findings of his report".*

Article 10.3 of Regulation 1073/99 reads as follows: *"Without prejudice to Articles 8 and 9 of this Regulation, the Office may at any time forward to the institution, body, office or agency concerned the information obtained in the course of internal investigations".*

The mentioned rules of Regulation 1073/99 foresee cases where the transfer would be operated between OLAF and other Community institutions or bodies. It has to be noted, not only concerning the point under analysis but also in general, that both Regulation 1073/99 and Regulation 45/2001 have to be applied together where relevant. That means that, regarding the aspect being referred to, the reports and/or the related documents (personal data), shall be transferred only if "necessary" for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard, taking into account, for instance, the nature of the data collected and further processed, and the competence of the recipient.

In any case, 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.

- **Transfer of personal data to Member States**

Two scenarios can be observed in Member States: (a) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC covers every sector of the national legal system, including the judicial sector; and (b) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC does not cover every sector, and particularly, not the judicial sector.

As to the first scenario, Article 8 of the Regulation foresees: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, (...)."*

Regulation 1073/99 stipulates, in its Article 10.2, as follows: *"Without prejudice to Articles 8, 9 and 11 of this Regulation, the Director of the Office shall forward to the judicial authorities of the Member State concerned the information obtained by the Office during internal investigations into matters liable to result in criminal proceedings. Subject to the requirements of the investigation, he shall simultaneously inform the Member State concerned."*[11]

Thus, even if judicial authorities do not fall within the scope of application of Directive 95/46/EC, if the Member State, when transposing Directive 95/46/EC into internal law, has

[11] It has to be borne in mind, as already mentioned, that the nature of the investigations conducted by OLAF is administrative, even if, when the transfer is decided, the issues involved can be qualified as "matters liable to result in criminal proceedings". The criterion of the Judgement of the CJEC of 30 May 2006, in cases C-317/04 and C-318/04, in so far as it is based on Article 3(2), first indent, of Directive 95/46/EC is not applicable, because the decision takes into account specific facts and Regulation 45/2001 has not a parallel provision.

extended its application to these public authorities, Article 8 of the Regulation has to be taken into account.

As to the specific wording of Article 8 of the Regulation ("... if the recipient establishes..."), here again Regulation 1073/1999 and Regulation 45/2001 have to be read together. As in the present context, the data are not required by the recipient, but it is OLAF who decides unilaterally on the transfer, it flows from Regulation 1073/1999 that OLAF has to establish the "necessity" of the transfer in a reasoned decision in this regard.

For those countries that have not extended their implementation of Directive 95/46/EC to judicial authorities, consideration to Article 9 of the Regulation has to be given. In those cases, Council of Europe Convention 108, which for the matter under analysis can be considered as providing an adequate level of protection, is in any case applicable to judicial authorities.

- **Transfer to third country authorities and/or international organizations**

As has already been noted, this subject matter is evaluated in case 2005-0154 and for this reason it is not analysed herein.

2.2.7. Processing including a personal number or other identifier of general application

OLAF uses the personnel number of an official under investigation, which is included in the final case report. The usage of a personal number can have consequences such as the interconnection of data processed in different contexts. The EDPS will not determine, in the present case, the conditions under which a personal number may be processed, as foreseen in Article 10.6 of the Regulation, but would like to draw the attention to the implications of this rule in the context of the Regulation. In the case under analysis, the use of the personnel number is reasonable, due to the fact that it is done only with the purpose of identifying the person involved in the dossier. The EDPS considers that this number can be processed in the mentioned scenario.

2.2.8. Right of access and rectification

According to Article 13 of the Regulation, 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 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. As a matter of principle, this right has to be interpreted linked to the concept of personal data. Indeed, the Regulation has adopted a broad concept of personal data, and the Article 29 Working Party has also followed a broad interpretation of this concept.[12] The respect of the rights of access and rectification is directly connected to the data quality principle and, in the context of investigations, it overlaps to a great extent with the right of defence.

[12] See Working document on data protection issues related to RFID technology, adopted on 19 January 2005, WP 105, p. 8: "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated".

Furthermore, the right of access is also applicable when a data subject requests access to the file of others, where information relating to him or her would be involved. This would be the case of whistleblowers, informants or witnesses who demand access to the data relating to them included in an investigation conducted on another person.

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 noted in point 2.1.2, the general rule applied by OLAF is the provision of access to the personal data related to the data subject contained in the file. The general rule is applied unless this access would be harmful to the investigation, which is decided on a case-by-case basis and never applied systematically. This rule is not reflected in the OLAF Manual, where Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, is applied to any request for access by the data subject him/herself, and not Article 13 of Regulation 45/2001, which is the relevant provision. Therefore, the EDPS recommends its inclusion in a future version given the importance from a data protection guarantees perspective. Furthermore, specific acknowledgement of any restriction based on Article 20 of the Regulation must be included in the file.[13]

Indeed, Article 20 of the Regulation provides for certain restrictions to this right 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."* Moreover, in certain cases it may be necessary not to give direct access to the data subject so as not to harm the proper functioning of the inquiry even though it is not a criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001, but a pre-disciplinary or pre-criminal investigation (OLAF administrative investigation).

The EDPS considers that Article 20 must take account of the *ratio legis* of the provision and must allow for restrictions on the obligation to provide direct access during a pre-disciplinary or pre-criminal investigation. This is backed up by the fact that Article 13 of Directive 95/46/EC makes provision for limiting the right to access of the data subject when such a restriction *"constitutes a necessary measure to safeguard...: (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions"*. Article 13(d) is therefore wide-ranging and extends from prevention, investigation, detection and prosecution of criminal offences to breaches of ethics for regulated professions. Even though this is not explicitly stated, there is reason to believe that breaches of discipline by public servants are also covered by the provision.

Regulation (EC) No 45/2001 must be read in the light of Directive 95/46/EC. Paragraph 12 of the preamble encourages *"consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data"*. Article 286 of the Treaty also provides "*Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty*." There is

[13] The reference to the data subject's right of access, which has possible limitations, would be most welcome in the abovementioned Proposal amending Regulation 1073/1999.

therefore no reason to believe that a restriction on the right of access may not be justified by the fact that a disciplinary procedure is underway.

In any case, paragraph 3 of Article 20 has to be considered and respected by OLAF: *"If a restriction provided for by paragraph 1 is imposed, 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 right to have recourse to the European Data Protection Supervisor."* Concerning the right to information, this provision has to be read jointly with Articles 11, 12 and 20 of the Regulation (see below point 2.2.9).

Moreover, account should also be taken of paragraph 4 of Article 20: *"If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made."* The indirect right of access will then have to be guaranteed. Indeed, this provision will play a role, for instance, in those cases where the data subject has been informed about the existence of the process, or has knowledge of it, but the right of access is still being restricted in the light of Article 20.

Paragraph 5 of Article 20 establishes that *"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."* It may be necessary for OLAF to defer such information in accordance with this provision, in order to safeguard the investigation. The necessity of such deferral must be decided on a case-by-case basis.

As already mentioned, the right of access involves the right of the data subject to be informed about the data referring to him or her. However, as noted above, this right can be restricted to safeguard "the protection of the (...) rights and freedoms of others". This has to be taken into account in the framework that is being analysed regarding access by the person concerned to the identity of whistleblowers. The Article 29 Working Party has made the following statement: "[u]nder 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." The same approach has to be applied concerning the informants.[14] Therefore, the EDPS recommends the respect of the confidentiality of the identity of whistleblowers during OLAF internal investigations and in the later stages (if, for instance, disciplinary and judicial authorities request for this identification) in as much as this would not contravene national rules regulating judicial procedures. Furthermore, the EDPS is of the opinion that the guarantees protecting whistleblowers during OLAF investigations must be legally reinforced, as they are now only established in a Commission Communication (SEC/20004/151/2)[15].

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the sensitivity, in most cases, of the investigations conducted by OLAF, this right is of key importance, in order to guarantee the quality of the data used, which, in this specific case, is connected to the right of defence. Any restriction, as provided in Article 20 of the Regulation, has to be applied in the light of what has been said regarding the right of access in the paragraphs above.

[14] Witnesses, on the contrary, do not require the confidentiality of their identity.

[15] The Proposal amending Regulation 1073/1999 would be an excellent occasion to guarantee the confidentiality of the identity of whistleblowers.

Moreover, it has to be borne in mind that the restrictions to a fundamental right can not be applied systematically. Indeed, 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, and as well as the right of information, the right of access and rectification will have to be provided "*as long as this would not be harmful to the investigation"* (see below point 2.2.9). Then, for instance, the nature of certain cases, will not always justify the denial of access and rectification during an OLAF internal investigation.

Finally, rules must be established to the effect that at the moment an investigation is closed, the official under investigation can rectify any data relating to him or her by requesting the inclusion in the investigation file of documentation related to any subsequent developments during the follow-up phase of the case (a decision by the Court ruling otherwise, for instance).

Therefore, it is observed that OLAF respects the obligations established by Article 13 and should integrate the recommendations made regarding Article 14 of the Regulation.

2.2.9. Information to the data subject

The Regulation states that the data subject must be informed where his or her personal data are being collected and lists a number of obligatory points to be included in the information, in order to ensure the fairness of the processing of personal data. In the case at hand, the data could be collected directly from the data subject and could also be collected indirectly, for instance, through informants.

The provisions of Article 11 of the Regulation (*Information to be supplied where the data have been obtained from the data subject*) and Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) are thus both applicable to the present case. This means that the relevant information must be given, either at the time of collection (Article 11), or when the data are first recorded or disclosed (Article 12), unless the data subject already has it. The latter may be the case, *inter alia*, if the same information has been given before.

The Memorandum has thoroughly described the kind of information that is given to the different data subjects (person concerned, whistleblowers, informants, witnesses). However, even if the content of the information given can sometimes partially match the information to be provided in the context of Articles 11 and 12, it is observed that not all the information pointed out in those rules is actually made available. It has to be taken into account that all the requisites mentioned in paragraph 1 of Articles 11 and 12 must be complied with, including sub-paragraph f), since, given the sensitivity of the cases normally dealt by OLAF, the data subjects must have knowledge of all the guarantees they are entitled to be covered by.

As concerns the moment to provide this information, it has been already said in point 2.1.2 of the present Opinion that Article 4 of the Model Decision annexed to the Inter-institutional Agreement concerning internal investigations by OLAF provides: *"Where the possible implication of a member, manager, official or servant emerges, the interested party shall be informed rapidly as long as this would not be harmful to the investigation. (...)."*

Article 20 of the Regulation, as referred to above, 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." Indeed, in certain cases it may be necessary not to inform the data subject so as not to harm the proper functioning of the inquiry even though it is not a criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001. The interpretation of this Article *vis-à-vis* the right of access in cases of pre-disciplinary or pre-criminal investigations has to be extended to the right of information.

Furthermore, paragraph 5 of Article 20 of the Regulation will have to be applied in specific circumstances: *"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 paragraphs 1 of its effect."* (paragraph 3 foresees the right of the data subject to be informed of the reasons why a restriction has been imposed as well as his right to have a recourse to the EDPS; paragraph 4 foresees the indirect right of access to be conducted by the EDPS and the information of its results to be provided to the data subject).

2.2.10. Confidentiality of communications

Article 36 of the Regulation stipulates that *"Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law"*. The concept of "general principles of Community law" refers to the notion of fundamental human rights notably as laid down in the European Convention on Human Rights. Any restriction to the confidentiality of communications must comply then with Article 8.2 of the said instrument: *"[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"*.

This provision has to be respected while conducting forensic examinations of computers, especially as concerns the examination of e-mails.

After considering the requisites contained in Article 8.2 of the European Convention on Human Rights and Fundamental Freedoms, the restrictions to the principle of confidentiality will therefore have to be examined according to the following criteria[16]:

- Is the restriction authorised by a legal provision or equivalent measure?

- Is it necessary? Could the same result be obtained without breaching the principle of confidentiality? It would only be in exceptional circumstances that the monitoring of an agent's personal use of the e-mail (apart from scanning viruses) or internet would be considered as necessary.

- Is it proportionate to the concerns it tries to ally? The principle of proportionality implies that the application of the restrictions to the confidentiality of communications will be different if we are in the case of personal communications or business communications. It also implies that if it is necessary to check the e-mail accounts of workers in their absence, this should in principle be limited to e-mails that are not marked as private or personal or that are addressed to the address of the institution.

[16] The EDPS has issued a draft paper on "The processing of personal data related to the use of the communications network in EU institutions and bodies: ensuring compliance with Regulation (EC) 45/2001", which has been distributed for preliminary discussion among the DPOs, and is likely to be published in the course of 2006. For further reference on the subject matter consultation of this paper is suggested.

In the particular case of OLAF internal administrative investigations, the potential restriction to the right to privacy and personal data protection is foreseen in Article 4.2 of Regulation 1073/1999 as follows: *"(...). The Office may take a copy of and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies and, if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearing, (...)"*.

As specified in section 3.4.4.2 of the OLAF Manual, in conducting a forensic examination of a computer, OLAF may take the computer itself or make a "disk image" of its contents. In either case, OLAF will have in its possession all of the data stored on the computer hard disk. The necessity and proportionality of access to any of the data contained therein (e.g. e-mails) have to be evaluated by OLAF on a case-by-case basis considering the orientations given above by the EDPS.

Regarding the methodology used by OLAF to conduct such investigations, certain principles are followed, as specified in point 2.1.2 of the present Opinion. However, the EDPS considers that the methodology should be developed in a systematic and formal fashion, and recommends the adoption of a formal Protocol of "Standard Operating Procedures" for the conduction of computer forensic investigations by OLAF, what will contribute to safeguard the confidentiality of communications, as well as to preserve the validity of the evidence.

2.2.11. Security measures

After careful analysis by the EDPS of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

[...]

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 the proportionality of the processing activities on a case-by-case basis;
- make its staff aware of the rule contained in Article 10.1 of the Regulation concerning special categories of data, even if this kind of data is processed exceptionally;
- guarantee the respect for the data quality principle. This could take the form of a general recommendation to the persons handling the files reminding them of the rule and recommending them to ensure the respect of it;
- consider that whenever the access to files that are apparently of a private nature (in the course of forensic examinations of computers) appears to be necessary for the investigation, this access be conducted respecting adequate guarantees;
- suppress the systematic inclusion in the files of the "marital status" and "children" categories of data. For their inclusion, evidence must exist of their relevance for the case under investigation;
- include, in a future version of the OLAF Manual, reference to the existence of a system of evidence of charge and discharge in the internal investigations' files;

- conduct a preliminary evaluation of the necessity of the 20 years conservation period *vis-à-vis* the purpose of such conservation when OLAF has experienced 10 years of existence. A second evaluation should be conducted when OLAF has experienced 20 years of existence;
- reduce the conservation period of data in files "closed without follow-up";
- include, in compliance with Article 7.1 of the Regulation, notice to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted;
- transfer the reports and/or the related documents (personal data) only if necessary for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard;
- establish the necessity of the transfer to judicial authorities in a reasoned decision, in the light of Article 8 of the Regulation;
- reflect in a future version of the OLAF Manual the general rule concerning the exercise of the right of access by the data subject, on the grounds of Article 13 of the Regulation, access that could be restricted if it is harmful to the investigation, which is decided on a case-by-case basis;
- acknowledge in the files when any restriction based on Article 20 of the Regulation is operated;
- inform the data subject in compliance with Article 20.3 and 20.4 of the Regulation where appropriate;
- respect the confidentiality of the identity of whistleblowers during OLAF internal investigations and in the later stages when appropriate; legal reinforcement of the guarantees protecting whistleblowers is needed;
- establish rules for the moment when the investigation is finished so that the data subject can rectify his/her personal data to ensure that they are updated in the light of subsequent developments;
- respect the content of the information to be given to the data subject as mentioned in paragraph 1 of Article 11 and 12 of the Regulation (including sub-paragraph f);
- evaluate the necessity and proportionality of the examination of e-mails on a case-by-case basis and in the light of Article 8.2 of the European Convention on Human Rights and Fundamental Freedoms;
- adopts a formal Protocol of "Standard Operating Procedures" for the conduction of computer forensic investigations;

Done at Brussels, 23 June 2006.

Peter HUSTINX
European Data Protection Supervisor