Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on Regular monitoring of the implementation of the investigative function

Brussels, 19 July 2007 (Case 2007-73)

1. Proceedings

On 9 February 2007, 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 Regular monitoring of the implementation of the investigative function, which is exercised by the Supervisory Committee (SC).

The EDPS requested OLAF to provide some complementary information on 14 February 2007, 22 March 2007 and 26 April 2007. The answers were received on 14 March 2007, 23 April 2007 and 2 May 2007 respectively. The draft was sent for comments on 7 May 2007, and the answer was received on 10 July 2007.

2. Examination of the matter

2.1. The facts

Purpose of processing

The purpose of the processing activity under analysis is to reinforce OLAF's independence, as required by Article 11 of Regulation 1073/99.

Nature of the Supervisory Committee

As stated in the answer received to a question of the EDPS, the Supervisory Committee (SC) is neither part of OLAF, nor part of an institution.

It is a committee set up by the Commission under Community law (Article 4 of Commission Decision 1999/352/EC, ECSC, Euratom and Article 11 of Regulation 1073/99). Just as any other consultative committee established by the Commission, the SC must be considered, for the

purposes of Regulation 45/2001, as an emanation of the Commission and thus bound by the Regulation.

Role of the Supervisory Committee

Article 11(1) of Regulation (EC) No 1073/1999 states: "The Supervisory Committee shall reinforce the Office's independence by regular monitoring of the implementation of the investigative function. At the Request of the Director or on its own initiative, the committee shall deliver opinions to the Director concerning the activities of the Office, without however interfering with the conduct of investigations in progress".

The members of the SC are "independent outside persons", as specified in Article 11(2). The Secretariat of the SC is provided by OLAF, and it is housed within OLAF premises.

Article 11(7) of Regulation (EC) No 1073/1999 stipulates: "The Director shall forward to the Supervisory Committee each year the office's programme of activities referred to in Article 1 of this Regulation. The Director shall keep the Committee regularly informed of the Office's activities, its investigations, the results thereof and the action taken on them". This provision further mentions three specific cases[1]:

- "**Nine month report**: Article 11(7) of Regulation 1073/99 provides that where an investigation has been in progress for more than nine months, the Director General shall inform the SC of the reasons why it has not yet been possible to conclude the investigation, and of the expected time for completion. In practice, the investigator in charge prepares an *Information to the OLAF Supervisory Committee: Investigation open for more than 9 months* form. The report should specify what investigative action has been completed and set out what additional investigative activities are still to be undertaken. If no investigative action has been undertaken since the case was opened, this should be stated, and the reasons for the absence of action should be specified. The nine month report must be prepared and signed by the investigator(s) assigned to the case; the signatures of the Responsible Head of Unit and Director A or Director B are also required.

- **Cases where Community organ failed to act on recommendations**: OLAF must also inform the Committee of cases where the Community organ concerned has failed to act on the recommendations made by it. A *Note*, prepared by the responsible follow-up unit, is sent in this regard.

- **Cases requiring information to be forwarded to judicial authorities**: Article 11(7) of regulation 1073/99 requires that the Director of OLAF inform the Supervisory Committee of cases requiring information to be forwarded to the judicial authorities of a Member State. Accordingly, once the interim case report has been signed, the magistrate from Unit C.1 assigned to the case prepares a *Note to the Supervisory Committee*.

Apart from these obligatory reports, it is for the Director General and Director A or Director B to decide whether information subject to professional secrecy about a specific case should be made available to the Supervisory Committee. Before any documents are provided to the Committee,

[1] OLAF Manual, 25 February 2005, point 3.5.7, pages 118-119.

the *written authorisation* of Director A or Director B is required and a *Record of information put at the disposal of the Supervisory Committee* form must be completed".

The tasks described may require that the SC and its Secretariat receive personal data contained in various documents forwarded by OLAF. The Supervisory Committee has also requested, and received, access to the OLAF Case Management System files for all closed cases and non-cases[2], which enables it to review all documents in the case files.

Furthermore, and according to Article 8(4) of Regulation (EC) No 1073/1999, "Confidentiality and data protection" the Supervisory Committee members have a specific responsibility to ensure the application of provisions relating to personal data and professional secrecy: "the Director of the Office and the members of the Supervisory Committee referred to in Article 11 shall ensure that this Article and Articles 286 and 287 of the Treaty are applied".

Moreover, Article 17(1) of the Rules of Procedure of the Supervisory Committee (OJ L33 2.2.07) "Confidentiality and processing of personal data" states: "The Supervisory Committee shall ensure that Article 8 of Regulation (EC) No 1073/1999 and Article 8 of Regulation (Euratom) No 1074/1999 are applied".

Data subjects

The data subjects concerned are: (1) staff of the EU institutions, bodies, offices and agencies subject to OLAF investigations or otherwise involved in the matters under investigation (as whistleblowers or witnesses); (2) persons outside the EU institutions, bodies, offices and agencies subject to OLAF investigations or otherwise involved in the matters under investigation (as informants, witnesses, economic operators and/or managers of companies concerned); (3) staff of the judicial authorities of the Member States or third countries in charge of the case which OLAF has forwarded to such authorities; and (4) OLAF's staff members who are responsible for the investigations.

Data categories

The data categories are: surname, forename, nickname, birthday, birthplace, case involvement, address, profession, organisation, function, and telephone number, fax number, e-mail address, activities related to matters which are the subject of OLAF investigations/follow-up. Then, the data fields can be identified as: identification and contact data, professional background, case involvement. The data categories mentioned are a comprehensive list of all data fields that may be included in any given document, but all of those fields are not necessarily included.

[2] "A matter is classified as a non-case where there is no need for OLAF to take any investigation, coordination, assistance or monitoring action. Non-cases result from assessments that conclude that EU interests appear not to be at risk from irregular activity, or other relevant factors indicate that no case should be opened. This would occur, for example, if only one Member State is concerned, and is already dealing with a matter in a satisfactory manner. This process may result in the transmission to Member States of information about possible offences not related to the protection of EU interests." OLAF Manual, 25 February 2005, point 3.3.3.1, page 76.

Information to be given to data subjects and procedures to grant rights of data subjects

Regarding the information to be provided to the data subjects, the EDPS was informed that the SC does not provide information directly to OLAF officials, because they are deemed to already have this information since they prepare the documentation which includes their own personal data that is sent to the Committee. It was also said that the SC has no direct contact with persons concerned, whistleblowers, witnesses and informants and does not receive or send any information from or to them. As a result, the EDPS was informed that, for such cases, the SC does not provide individuals with information about the SC's processing of their personal data. The SC does, from time to time, receive complaints concerning OLAF, to which the Committee replies and gives appropriate follow-up if necessary. Hereafter, the reply will include the following Privacy Statement text also:

> "Pursuant to Article 11 of Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, personal data received by the Supervisory Committee in correspondence regarding OLAF's practices will be stored in the Committee's electronic and paper files for a maximum period of 10 years to allow us to ensure an appropriate treatment of such correspondence. The categories of personal data being processed are identification data, professional data and other data relating to the allegations which have been made.
>
> The Supervisory Committee has implemented appropriate technical and organisational measures designed to protect information in its possession from loss, misuse, unauthorized access, disclosure, alteration or destruction.
>
> You have the right to access the personal data we hold regarding you and to correct and complete it. Any such request should be addressed to Eberhard Brandt, the Head of the Supervisory Committee's secretariat. You may also contact him in case of any difficulties, or for any questions relating to the processing of your personal data.
>
> You may lodge a complaint concerning the processing of your personal data with the European Data Protection Supervisor."

Automated / Manual processing operation

Both automated (e.g. access to CMS) and manual operations take place. An individual profile for access of the secretariat of the SC was created in April 2006. The profile allows READ ONLY access to cases in the following stages only:

- -Follow-up
- -Follow-up completed
- -No Follow-up
- -Monitoring cases
- -Closed Irene (which was the name of the system preceding the CMS).

Ad hoc access to specific paper case files has also been given to the SC upon request.

All staff members of the SC secretariat (including all grades) have been granted such access, based on a request made by the controller. As with any authorised user of the CMS, the access rights are controlled by the Information Services unit (D.8), based on instructions they have received from management. Once their access rights have been entered in the system, they have free access to the cases falling within those rights. The only record of access is the electronic log files of the CMS.

Regarding manual processing, a filing system has been developed comprised of general/pertinent information (Commission/Council documents, etc.); documents transmitted by OLAF; minutes, agendas, etc.; documents from the former SC.

Retention policy

The SC may keep both electronic and paper files relating to investigations and follow-up activities for up to 10 years after the date on which the follow-up has been completed in line with OLAF's retention policy. The legal basis of the Supervisory Committee does not specify a conservation period for its documents. The Committee deems a 10 year conservation period to be necessary to ensure that documents are available in case it must provide information for audits by the Court of Auditors, responses to Parliamentary questions, or litigation.

Time limits for blocking and erasure

The time limit for blocking and erasure of the different categories of data (on justified legitimate request from the data subject) is one month.

Data transfers

The Opinions of the SC will be delivered to the Director of OLAF.

Security measures

Security measures have been adopted. It has to be noted that the SC makes use of OLAF IT infrastructure and building premises.

2.2. Legal aspects

2.2.1. Prior checking

The prior checking relates to the processing of personal data in the context of the Regular monitoring of the implementation of the investigative function conducted by the Supervisory Committee (Articles 2(a) and (b) of Regulation (EC) No 45/2001 (hereinafter "the Regulation"). The processing activity is carried out by a committee set up by the Commission,[3] and thus, for the purposes of Regulation (EC) No 45/2001, an emanation of the Commission, in the framework of Community law[4] (Article 3.1 of the Regulation). The processing of personal data is done

[3] It has to be noted that the SC is *"appointed by common accord of the European Parliament, the Council and the Commission"* (Article 11.2, second paragraph of Regulation (EC) N. 1073/1999).
[4] The SC was created by Community law and its tasks are determined by Community law.

partly by automatic means (Article 3.2 of the Regulation). As a consequence, the Regulation is applicable.

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

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 operations could typically involve this type of data.

Furthermore, Article 27.2(b) of the Regulation stipulates that operations intended 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 could be analysed by the SC in its monitoring tasks, and it may draw conclusions which affect the investigators.

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

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 9 February 2007. According to Article 27(4) the present Opinion must be delivered within a period of two months. Complementary information was requested on 14 February 2007, 22 March 2007 and 26 April 2007. The answers were received on 14 March 2007, 23 April 2007 and 2 May 2007 respectively. The draft was sent for comments on 7 May 2007, and the answer was received on 10 July 2007.The procedure was suspended during 64 days. The Opinion will therefore be adopted no later than 20 July 2007.

2.2.2. Lawfulness of the processing

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 processing of data in the context of the Regular monitoring of the implementation of the investigative function falls within the scope of the legitimate exercise of official authority vested in the SC. Thus the lawfulness of processing is respected in principle. This follows from Article 11 of Regulation 1073/1999 and Article 4 of Commission Decision 1999/352.

Article 11 of Regulation 1073/1999 stipulates the following:

"1. The Supervisory Committee shall reinforce the Office's independence by regular monitoring of the implementation of the investigative function. At the request of the Director or on its own initiative, the committee shall deliver opinions to the Director concerning the activities of the Office, without however interfering with the conduct of investigations in progress.
(...)
8. The Supervisory Committee shall adopt at least one report on its activities per year which it shall send to the institutions. The committee may submit reports to the European Parliament, the Council, the Commission and the Court of Auditors on the results of the Office's investigations and the action taken thereon."

Article 4 of Commission Decision 1999/352 foresees the following:

"A Surveillance Committee shall be established, the composition and powers of which shall be laid down by the Community legislature. This Committee shall be responsible for the regular monitoring of the discharge by the Office of its investigative function."

It should be noted that Article 11(1) of Regulation 1073/1999 reads as a legal obligation. However, it leaves a fairly large discretion to the SC as to the way in which it should exercise its authority, within the limits imposed by Community legislation, particularly when it comes to the processing of personal data. Article 5(a) of Regulation 45/2001 is therefore the appropriate legal basis for such processing and not Article 5(b) of the Regulation.

The "necessity" of the processing, as required in Article 5(a) of the Regulation, 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 regular monitoring of the implementation of the investigative function has to be proportional to the general purpose of processing ("reinforce OLAF's independence") and to the particular purpose of processing in the context of the case under analysis. This implies, for instance, considering whether the specific monitoring activity deals with an investigation which has been in progress for more than nine months; an institution, body, agency or office which has failed to act on the recommendations made by OLAF; or cases requiring information to be forwarded to the judicial authorities of a Member State. Furthermore, the seriousness of the fact under investigation, the sort of data needed to clarify the facts, etc., also have to be considered to determine the "necessity". Thus, the proportionality has to be evaluated on a case-by-case basis (see point 2.2.4 below). In this respect, the SC has to first analyse whether information with no personal data or information describing the external circumstances of a case would satisfy their task. In case such approach is insufficient, the SC may need personal data to be provided by OLAF or by direct access to the file.

2.2.3. Processing of special categories of data

Article 10.5 stipulates as 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, to the extent in which such processing is necessary for the SC to properly execute its tasks.

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.

According to the notification form, the type of data described in Article 10.1 would not be processed. However, it could happen, for instance, that the file that is being analysed by the SC contained exceptionally such data and, according to the nature of the case, it is relevant to evaluate the independence of OLAF in this context. In the event that this occurs, the general rule of Article 10.1 has to be respected. In the alternative, it has to be evaluated in a restricted manner whether the application of an exception would be "necessary". In any case, the members and staff of the SC must be made aware of this rule.

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."*

The amount and type of data processed in each monitoring activity conducted by the SC may vary according to the specific function/task that it is performing (monitoring nine month reports, monitoring cases of failure to act, etc). Furthermore, within each category of functions, the amount of data needed for each specific case may also vary. In certain situations, the SC may need access to a whole CMS file of the case investigated by OLAF in order to fulfil its obligation. In others, it can perform its role in a different manner, for instance, analysing external circumstances (not including personal data) that could have caused a given investigation to be in progress for more than nine months, or having access to an anonymised file. In any case, access to the whole CMS file should be avoided, in principle, as a first step. Only when the knowledge of the external circumstances of the file proves to be insufficient to conduct the monitoring task, or when the anonymisation of the file by OLAF requires a disproportionate effort, the SC can have access to the whole file.

Therefore, the EDPS considers that the SC must put in place guarantees in order to ensure the respect for the principle of data quality in the exercise of its monitoring activities. This could take the form of a reference to the principle in the SC rules of procedure.

Furthermore, a methodology shall be established describing the different steps to be followed in any access request, previous to the access to the whole CMS file. In the last step it has to be to the SC to decide whether the previous steps have been insufficient for the performance of its role and therefore there is a need to access the whole file. OLAF has to include a note in the CMS file

containing the reasons invoked by the SC for such need to access. Furthermore, the requirement is subject to EDPS supervision.

The EDPS considers that full access to the CMS files for all closed cases and non-cases (as well as for any other type of cases) is excessive in relation to the general purpose of the SC processing. It is recommended that access to those files should not be automatic; instead the SC should seek such access on a case-by-case basis, using the same methodology mentioned in the paragraph above.

In any case, OLAF must see to it that the information given is sufficient to enable the Committee to fulfil its function, i.e. to monitor, at systemic level, the implementation of the investigative function in order to reinforce OLAF's independence.

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 2.2.7 below).

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. It is related to the information given to the data subjects (see point 2.2.8 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).

Like OLAF, the SC has only been in existence since 1999, and thus has no experience to date as to whether a 10-year conservation period is sufficient or excessive. The EDPS suggests that when the SC has experienced 10 years of existence, an evaluation of the necessity of the 10-year period *vis-à-vis* the purpose of such conservation frame should be conducted.

2.2.6. Transfer of data

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"*.

The opinions of the SC have to be delivered to the Director of OLAF. In case the opinions include personal data, this inclusion should be limited to what is necessary for the legitimate performance of OLAF tasks. Members and staff of the SC must be aware of this rule.

2.2.7. 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.[5] The respect of the rights of access and rectification is directly connected to the data quality principle.

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

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).

The general rule applied by the SC is the provision of access to the personal data related to the data subject. The general rule is applied unless this access would be harmful to the monitoring activity, or any other exception would apply (see paragraph below), which is determined on a case-by-case basis and never applied systematically. Furthermore, in most cases, the application of an exception by OLAF would result in the parallel application of the same exception by the SC. In any case, specific acknowledgement of any restriction based on Article 20 of the Regulation must be included in the file held by the SC. In the EDPS view, this practice is in line with Regulation 45/2001, provided that the SC takes the following into account when assessing whether an exception to the right of access applies.

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; (d) the national security, public security or defence of the Member States; (e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the*

[5] See Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, WP 136, as well as 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".

cases referred to in (a) and (b)." 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 monitoring activity conducted by the SC, or the OLAF investigation case to which it could be connected, even though it is not a criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001.

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 the monitoring of the breaches related to the independence of OLAF in the context of its investigative function is also covered by the provision.[6]

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 therefore no reason to believe that a restriction on the right of access may not be justified by the fact that a monitoring activity conducted by the SC is underway.

In any case, paragraph 3 of Article 20 has to be considered and respected by the SC: *"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 2.2.8).

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

[6] See: 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), page 20, available at:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Prior checks/Opinions/2006/06-06-23_OLAF_internal_investigations_EN.pdf

existence of the monitoring activity conducted by SC, 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 the SC to defer such information in accordance with this provision, in order to safeguard the monitoring activity, or the investigation case to which it could be connected. 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.[7] Therefore, the EDPS recommends the respect of the confidentiality of the identity of whistleblowers during the SC monitoring activity in as much as this would not contravene national rules regulating judicial procedures.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. This right is of key importance, in order to guarantee the quality of the data used. 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.

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. Then, for instance, the nature of certain cases will not always justify the denial of access and rectification during an SC monitoring activity.

2.2.8. 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 (e.g. letters of complaint received by the SC) and could also be collected indirectly (e.g. through the reports sent by OLAF, thought access to the CMS, etc.).

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

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

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, for instance, through the information notice sent by OLAF, where the data subject is informed that data contained in a case file can be transferred to the SC.

In accordance with the above, the EDPS calls upon the SC to ensure the notification to all the individuals whose data are processed in the context of its monitoring functions. As to individuals with whom the SC has no direct contact (persons concerned, whistleblowers, witnesses and informants), the EDPS suggests that the SC agrees with OLAF for the latter to include in its privacy statement addressed to these individuals a paragraph informing them of the possibility for their data to be transferred to the SC for monitoring purposes. If such information is given by OLAF, then, the SC will not be under obligation to provide it again (ex Article 12.1 "Where the data have not been obtained from the data subject, the controller shall... provide the data subject with at least the following information *except where he or she already has it*")

The Privacy Statement mentioned in point 2.1 of the present Opinion describes the kind of information that is given to complainants from whom the SC has obtained the data directly. The EDPS recommends to add the information mentioned in Article 11.1(c) to this statement (in conformity to what is described in point 2.2.6 of the present Opinion).

Article 20 of the Regulation, as referred to above, provides for certain restrictions to the right of information. Indeed, in certain cases it may be necessary not to inform the data subject so as not to harm the proper functioning of the monitoring activity, or the investigation case to which it could be connected, 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).

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, the Supervisory Committee must:

- evaluate the proportionality of the processing activities on a case-by-case basis;

- make its members and staff aware of the rule contained in Article 10.1 of the Regulation concerning special categories of data, even if this kind of data would only be processed exceptionally;
- guarantee the respect for the data quality principle. This could take the form of a reference to the principle in the SC rules of procedure. Furthermore, a methodology should be established describing the different steps to be followed in the access' requests, previous to the access to the whole CMS file;
- have access to the CMS files (on-going, closed and non-cases) only on a case-by-case basis. When such access is requested, a note should be included in the CMS file specifying the reasons that justify the provision of access;
- conduct an evaluation of the necessity of the 10 years conservation period *vis-à-vis* the purpose of such conservation when the SC has experienced 10 years of existence;
- make its members and staff aware of the rule contained in Article 7.1 of the Regulation;
- acknowledge in the files kept by the SC when a restriction based on Article 20 of the Regulation has been used to defer the provision of access/information.
- apply any restriction based on Article 20 of the Regulation on a case-by-case basis;
- inform the data subject in compliance with Article 20.3 and 20.5 of the Regulation where appropriate;
- respect the confidentiality of the identity of whistleblowers;
- add the information mentioned in Article 11.1(c) to the privacy statement;
- respect Article 12 of the Regulation regarding the persons concerned, including whistleblowers, witnesses and informants, in case any processing activity is conducted concerning their data in the context of the monitoring activity, and provided the data subject has not received the information before. The SC could agree with OLAF for the latter to include in its privacy statement addressed to these individuals a paragraph informing them of the possibility for their data to be transferred to the SC for monitoring purposes.

Done at Brussels, 19 July 2007

Peter HUSTINX
European Data Protection Supervisor