Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on Information and Intelligence Data Pool and Intelligence Databases

Brussels, 21 November 2007 (Joint Cases 2007-27 and 2007-28)

1. Proceedings

On 17 January 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 OLAF Information and Intelligence Data Pool and Intelligence Databases.

The cases under analysis have been notified separately.[1] However, they overlap in most of the aspects to be analysed. Therefore, the EDPS has decided to make a joint assessment, and where necessary, address the specificities of the Intelligence Databases. Indeed, the Intelligence Databases involve specific analytical projects attaining a critical mass of complexity or volume, with a unique data control environment. The Intelligence Databases can be identified as one of the tools used by the Information and Intelligence Data Pool.

The EDPS requested OLAF to provide some complementary information on 29 January, 15 March 2007, 6 September 2007, 11 October 2007 and 26 October 2007. The answers were received on 6 March, 6 July 2007, 9 October 2007, 26 October 2007 and 6 November 2007 respectively. On 7 November 2007, the EDPS sent his draft Opinion to the DPO with a request to comment on it. The comments reached the EDPS on 16 November 2007.

2. Examination of the matter

2.1. The facts

a. Purpose of the processing

"Information and Intelligence Data Pool" is the description given to all data held within the remit of Operational Intelligence Unit C4 in OLAF, including the Intelligence Databases.

Operational Information and Intelligence support are essential aspects of OLAF's mandate to fight fraud, corruption, and any other illegal activity affecting the financial interests of the European Community, and serious matters relating to the discharge of professional duties, as established in Article 1 of Regulation (EC) No 1073/1999 and Commission Decision 1999/352/EC Article 2 (5).

[1] Case 2007-0027 corresponds to "Information and Intelligence Data Pool" and Case 2007-0028 corresponds to "Intelligence Databases".

The purpose of the processing under analysis is then to further OLAF intelligence/analysis and operational activity, and to support specific case requests, operations and investigations with a view to ensuring the optimum accuracy and relevance of information received, disseminated and otherwise processed for intelligence, financial, administrative, disciplinary and judicial use. This support may be provided throughout the various stages of OLAFs investigation and operational activities, over all sectors[2] and is recorded within the CMS where applicable. OLAF's operational intelligence role also includes supporting the control, intelligence and enforcement activities in Member States, for OLAF partners and Operational DGs. Chapter 2.4.3 of the OLAF Manual[3] further explains the role of OLAFs operational intelligence.

b. Data subjects

The data subjects concerned are: (1) staff of the EU institutions, bodies, offices and agencies subject to OLAF investigations or assessments or otherwise involved in the matter under investigation or assessment (whistleblowers, informants and witnesses); (2) persons outside the EU institutions, bodies, offices and agencies, who are mentioned in the documents kept in the file as a result of the investigative or assessment activities (e.g. managers of the companies concerned, informants and witnesses); (3) persons outside the EU institutions, bodies, offices and agencies, who are involved in matters which are the subject of operational activity by OLAF and its operational partners.[4]

c. Data categories

The data categories processed within the scope of this processing activity are the following: surname, forename, maiden name, alias, date of birth, place of birth, country of birth, passport number, nationality, gender, marital status, family members, address, communication details (telephone and fax number), e-mail address, and website. OLAF's DPO has mentioned in the notification that the EDPS indicated in his opinion regarding OLAF's internal investigations that the marital status and children data fields should not be processed in the context of such investigations, unless they are relevant to the matter under investigation (e.g. falsely claimed allowances or conflict of interest) (Case 2005-418, opinion dated 23/06/2006.) As a result of a CMS request, OLAF intelligence extracts data from personnel management information systems such as SYSPER II. [5] Due to the nature of the SYSPER II, details of children and marital status are included by default in the information thereby gathered. These data fields are not, however, extracted or processed unless they are relevant to the specific case in question.

---

[2] This refers to all possible sectors which may be the subject of OLAF operational activities. In the Case Management System (CMS), the sectors are described as: Agriculture; Alcohol; Anti-Corruption; Cigarettes; Customs; Direct Expenditure; ESTAT; External Aid; Multi Agency Investigations; Precursors; Structural Funds; Trade; VAT.

[3] OLAF Manual of 25 February 2005 (Office for Official Publications of the European Communities 2005).

[4] The difference between (2) and (3) is in the type of activity related to the intelligence. Whereas (2) refers to the framework of operational activities carried out by OLAF in its independent function (these intelligence activities are linked to cases that have been allocated a CMS number), (3) refers to the framework of activities carried out by OLAF in support of "operational activity by OLAF and its partners" and includes mutual assistance activities based on sectoral legislation such as Regulation 515/97.

[5] Personnel management system of the European Commission.

The EDPS has asked the OLAF DPO whether the type of special categories of data described in Article 10.1 of the Regulation were processed in the context being assessed. The answer was that no data of this kind is processed in the present arena.

c.1. Description of data categories contained in the Intelligence Databases standard templates

Concerning the data categories, the standard templates for the two key iBase entities in relation to personal data, i.e. persons and organisations, present the following fields:

- Organisation

-Icon[6]
-Organisation name
-Name Tradestyle
-Criminal
-Commercial
-Terrorist organisation
-ID-Number
-D&B Number[7]
-D&B date checked
-SIC Code
-Country
-Comments
-Out of Business
-Source hyperlink
-Evaluation of Info & Source
-Creation Date
-Creation User
-Last Update Date
-Last Update User
-Record ID
-Review 3 year
-Review 1 year
-Data Access control

- Person

-Icon
-Person implication
-Surname
-Firstname
-Maiden Name
-Alias
-DOB[8]

[6] This field would contain a graphical icon. The system provides for a set of standard icons to represent a person, a company, a location, etc. The user is not bound to use these standard icons, and could choose to enter a more personal style.

[7] Dun and Bradstreet, a company that provides information on over 100 million businesses worldwide.

[8] Date of Birth.

-Age
-Incomplete DOB
-Place of Birth
-Area of Birth
-Country of Birth
-Gender
-Nationality 1
-Nationality 2
-National ID number
-Comment
-Marital Status
-Source hyperlink
-Picture[9]
-Criminal antecedents
-URN[10]
-Evaluation of Info & Source[11]
-Creation Date
-Creation User
-Last Update Date
-Last Update User
-Record ID
-Review 3 year[12]
-Review 1 year
-Data Access Control

These templates are used for data entry when creating a new iBase database. Occasionally, an analyst may need an additional field.[13] According to OLAF, no data fields which fall under Article 10 of the Regulation are included.

---

[9] This field may contain a picture of the person concerned.

[10] Unique Reference Number or unique ID to differentiate records.

[11] The evaluation grid in use by most of the Member States, and built into iBase, is the following:
Evaluation of the information:
1. accuracy is not in doubt;
2. known personally to source;
3. known personally to source and corroborated;
4. known personally to source but not corroborated.
Evaluation of the source:
A. no doubt;
B. in most cases reliable;
C. in most cases unreliable
X or D. reliable
This results visually in:
A1, A2, B1, B2: Confirmed link.
All the others: A3, A4, B3, B4, C1, C2: Unconfirmed link

[12] When entering the source, a time stamp is attached to it by the iBase system. The iBase template used by OLAF will trigger the review action when the deadline is attained. If no particular indication is available that this information is of further interest, the analyst will delete the information. Otherwise the analyst will earmark an extension of the retention period.

[13] Until now, no new field has ever been created. Rather, the "comments" field has been used to provide further information for an already existing data field. OLAF has explained to the EDPS that there may be circumstances in the future when it could be necessary to add a new data field, such as if there were a change in OLAF's mandate or in relevant legislation.

The categories of data fields of data subjects can then be identified as: (1) identification and contact data; (2) professional data; and (3) case involvement data.

d. Information to the data subject

Where intelligence is conducted as part of an investigative process, at any moment from the time of receipt of initial information until the final closure of follow-up, information to the data subject would be given in the framework of the investigation or follow-up phase. Data Subjects are advised of their rights through the OLAF standard letters and clauses addressed to whistleblowers, informants, witnesses and persons concerned.

The provision of this information may be restricted, when necessary to safeguard the investigation, detection and prosecution of fraud or irregularities affecting the EU budget. Individuals whose names appear in the documentation under analysis, but who are not persons concerned, witnesses, whistleblowers or informants, do not receive an individual "information to be given to the Data Subject" because, as pointed out in OLAF's notification, the provision of such information would be impossible or would involve a disproportionate effort, in light of the large number of individuals concerned. These individuals have no relevance to the matter under investigation.

If, however, intelligence is conducted independent of an investigation, the data subject would not receive the information within such framework. Accordingly, a privacy statement will be placed on the OLAF "Europa" site to cover such instances.

e. Procedures to grant rights of data subjects

Both the letters and the privacy statement describe the procedures to follow in order to exercise the data subject's rights of access and rectification.

f. Types of requests for information and intelligence

Pursuant to OLAF internal operational instructions, several types of requests for information and intelligence are possible:

1. OLAF case handlers (investigators and follow-up agents)[14] may submit a request for operational (case-related) information and intelligence through the CMS intelligence module using the relevant CMS case number.

2. Requests for non-case related information and intelligence from investigators must be submitted through an OLAF head of unit or head of operations through the CMS intelligence module.

3. Requests for non-case related information and intelligence from Commission services, national or international services particularly received through the AFIS system[15] are introduced into the CMS intelligence module by OLAF information support staff.

---

[14] A case handler may be an investigator (who may be responsible for the assessment phase or the active phase of the case) or a follow-up agent (responsible for follow-up).

[15] Anti Fraud Information System. Since 1997, the name AFIS has been adopted as the umbrella of all applications used for mutual assistance in combating fraud. OLAF is responsible for the analysis, development, support and operation tasks for the application. This is explained fully in the EDPS opinion concerning Mutual Assistance Exchanges (Case 2007-202, 19 October 2007).

4. Certain requests may evolve into tactical operations when the intelligence request points to a wider spread of the problem examined. In these cases, broader and systematic checks of the modus operandi in question will be conducted. Such operations are generally agreed with the operational DG and OLAF heads of unit from the intelligence and operational side after assessing their appropriateness and proportionality.

5. Others are simply ongoing activities that have been agreed upon to support a permanent operational check of flows of incoming information that are systematically matched against the existing data collection of a specific operational domain.

6. Before mid-2007, a request could, exceptionally and in a highly sensitive matter, be submitted orally. Since mid-2007 this practice no longer exists. All requests must now be made through the intelligence module of the CMS.[16]

Upon receipt, the staff member assigned to handle the request determines which information sources and analysis tools can best be used to satisfy the request.

g. Types of activities carried out

Various types of activity can be carried out: background information checks on natural persons as well as simple or complex research to assess and evaluate information, producing analyses to build a clearer picture of connected factors, including personal data. The outcome of the processing in the pre-assessment phase therefore may indicate either that the data are of further relevance or that they are not, thus leading to a non-case within OLAF or to no further action by a Member State or EU Institution. Relevant source, additional and comparative data are identified, extracted manually and electronically and used for individual searches as well as simple and complex queries.

g.1. Specific activities concerning the Intelligence Databases

Concerning the processing activities themselves, some specific analytical projects attaining a critical mass of complexity or volume require an intelligence database in an iBase environment. iBase is at the heart of a group of inter-linked analytical tools that allow management of data.

The processing conducted is automated. iBase is both a database application and a modeling and analysis tool. The data objects, such as vehicles, people and addresses, are linked to demonstrate relationships with other data objects, such as owner, associate, and account holder. Each entity or link is represented by a database record. iBase environments assist analysts in the process of analysing. For instance, they support the data entry process, automatically highlight information already known to the system, and analyse and display complex information and relationships between or among entities.

h. Sources

---

[16] Before mid-2007, with regard to the small number of oral requests received, the procedure was the following: a record of the request in the CMS module was required. If this was not done by the case handler making the request, then it was done by the intelligence officer handling it. The record included the name of the person making the request, minimum information about the request, and the fact that a reply was provided to the investigator (in a paper document). This was done in order to create a record of the request and its treatment, thereby ensuring accountability.

The sources include:

- Commission and European Development Fund (EDF) data extracted in support of internal investigations and for OLAF operational purposes;

- OLAF CMS data for OLAF operational purposes;

- Data resulting from forensic examinations;

- Data exchanged under specific legislation (or where there is an agreement or arrangement to permit use of the data) with OLAF's control or enforcement partners within the institutions and in the Member States, international organisations, third countries via controlled access and special security measures. To enhance this data for analysis purposes, it may be put in one format, cleaned, standardised and consolidated into dedicated databases with restricted and controlled access;

- Company or trade data, which is freely accessible;

- Open sources such as in the media, the internet, library sources, directories, websites for international organisations;

- Commercial, company or trade data where OLAF or the Commission may pay for direct access for OLAF and/or for its partners and where there is an agreement, arrangement or contract;

- Commercial, company or trade data purchased in one format, cleansed, standardised and consolidated into dedicated databases for analysis purposes with restricted and controlled access;

- High volume commercial, company or trade data gathered and consolidated for analysis purposes working together with other Commission DGs. This may be stored in another DG's server with password access for OLAF users.

i. Automated/Manual processing operations

The processing is both manual and automated. Data entry may also involve high volume paper scanning. The quality of the analysis depends on the quality of data preparation. Data preparation tools, such as ACCESS, DOCTUM, ULTRAEDIT, EXCEL, ACL, AskSam, and text mining are used for this purpose. Once the research is completed, the response is provided to the operational staff member or service (Commission, national or international service) who requested it in the form of a report, which is provided through the CMS intelligence module or through the AFIS system.

j. Data recipients

The recipients or categories of recipients to whom the data might be disclosed are: (1) OLAF case handler responsible for the relevant case; (2) concerned EU institutions, bodies, offices or agencies; (3) competent national authorities; (4) competent third country authorities; and (4) international organisations. Intelligence data is first transferred internally within OLAF to the case handler or the person dealing with the request received from another EU institution or body, national authority, third country authority or international organization. Indeed,

intelligence is part of the whole investigative process from the initial information until the final closure of all OLAF action. Therefore, intelligence units do not directly communicate with any person or body when they act in support of the case handler. The transfer would be through an investigator in the framework of an investigation, in accordance with Articles 8 and 10 of 1073/1999. In contrast, transfers to national authorities and third countries can take place within the context of operational activity of which the information/intelligence officer is a part (e.g. providing live support during joint customs operations), and direct information support is requested from or offered to external competent authorities.

k. Retention policy

Concerning the retention period, the policy adopted is the following:

- Where an initial assessment is made and no investigation is thereafter open, the personal data will be deleted from the information and intelligence data pool after five years in accordance with the policy related to "non-cases" (with respect to which the EDPS has issued an opinion on a notification submitted for prior checking, Case 2007-0205, 3 October 2007).

- Where intelligence is done in the context of an investigation or operational activity, the data will be retained in accordance with the retention policy related to investigations (maximum 20 years). (Internal investigations: Case 2005-418, 23 June 2006; External investigations: Cases 2007-47-48-49-50-72, 4 October,2007).

- Where personal data are processed from data exchanged under Mutual Assistance, the data will be retained in accordance with the retention policy related to mutual assistance (maximum 10 years). (Case 2007-202, 19 October 2007).

- Where personal data are processed as a result of data exchanged under "Irregularities", the limit is three years following the payment by the Commission of the final balance. (Cases 2007-84-85-86-87, 29 June 2007)

- Where no other rule applies, retention policy is set at a maximum of 5 years.

- Where a review of the personal data at any time indicates that it is no longer relevant to the conduct of any designated matter, it will be removed from the information and intelligence data pool.

l. Time limits for blocking

Time limit to block/erase data on justified legitimate request from the data subjects is one month.

m. International transfers

Transfers may be made to competent third countries and international organisations where this is supported by legislation (for example under Regulation 515/97 during a specific time frame of a joint customs operation. (See EDPS Opinion in Case 2007-202 concerning Mutual Assistance Exchanges).

n. Security measures

Security measures have been adopted. A specific document was submitted to the EDPS. It provides a background for intelligence/information management at Directorate C - OLAF. Some complementary questions on the security aspects have been asked and clarifications have been received.

2.2. Legal aspects

2.2.1. Prior checking

The prior checking relates to the processing of personal data[17] in the context of the Information and Intelligence Data Pool and Intelligence Databases made by OLAF (Articles 2(a) and (b) of Regulation (EC) No 45/2001 (hereinafter "the Regulation"). The processing activity is carried out by a Community institution, in the framework of Community law[18] (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.

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.

Under Article 27.2(a) of the Regulation, processing of data relating to "suspected offences, offences or criminal convictions" shall be subject to prior checking by the EDPS. In the present cases, the processing operation may well involve this type of data.

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 cases under analysis, the conduct of people is analysed by OLAF.

The following prior check will not analyse the transfers of data to third countries or international organizations. This issue is being dealt with in the context of case 2005-0154, in the framework of which the EDPS analyses the conformity of OLAF international transfers with the Regulation.

The EDPS notes that the security measures set forth in the present context are, in principle, 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 make a full assessment of the security measures since the analysis will be carried out in a different Opinion which will address security issues only. However, certain specificities will be underlined.

---

[17] Data on Organizations (as described in point 2.1.c.1 above) may be "related to" physical persons. See Opinion of 30 June 2006 on a notification for prior checking relating to the EU-China Agreement - Approved Destination Status (ADS) (Case 2006-192), available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2006/06-06-30_Commission_EU-China_EN.pdf , p. 5.

[18] Particularly in the context of administrative investigations the Regulation applies, regardless of the fact that this might lead to a criminal investigation conducted by national judicial authorities.

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 17 January 2007. According to Article 27(4) the present Opinion must be delivered within a period of two months. Complementary questions have been asked on 29 January, 15 March 2007, 6 September 2007, 11 October 2007 and 26 October 2007. The answers were received on 6 March, 6 July 2007, 9 October 2007, 26 October 2007 and 6 November 2007 respectively. On 7 November 2007, the EDPS sent his draft Opinion to the DPO with a request to comment on it. The comments reached the EDPS on 16 November 2007. All ex-post prior checks have been suspended during the month of August 2007. Therefore, the Opinion will be adopted no later than 21 November 2007 (208 days of suspension + month of August).

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 Information and Intelligence Data Pool and Intelligence Databases is based on Article 1 of Regulation 1073/1999 and Article 2(5) of Commission Decision 1999/352.

Article 1 of Regulation 1073/1999 stipulates the following:

"1. In order to step up the fight against fraud, corruption and any other illegal activity affecting the financial interests of the European Community, the European Anti-Fraud Office established by Commission Decision 1999/352/EC, ECSC, Euratom (hereinafter `the Office') shall exercise the powers of investigation conferred on the Commission by the Community rules and Regulations and agreements in force in those areas.
2. The Office shall provide the Member States with assistance from the Commission in organising close and regular cooperation between their competent authorities in order to coordinate their activities for the purpose of protecting the European Community's financial interests against fraud. The Office shall contribute to the design and development of methods of fighting fraud and any other illegal activity affecting the financial interests of the European Community.
3. Within the institutions, bodies, offices and agencies established by, or on the basis of, the Treaties (hereinafter `the institutions, bodies, offices and agencies'), the Office shall conduct administrative investigations for the purpose of:
-fighting fraud, corruption and any other illegal activity affecting the financial interests of the European Community,
-investigating to that end 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 (`the Staff Regulations')".

Article 2(5) of Commission Decision 1999/352 foresees the following:

"The Office shall be responsible for any other operational activity of the Commission in relation to the fight against fraud as referred to in paragraph 1, and in particular:

(a) developing the necessary infrastructure;

(b) ensuring the collection and analysis of information;

(c)giving technical support, in particular in the area of training, to the other institutions or bodies as well as to the competent national authorities."

The instruments quoted above show that the processing activity done in the context of Information and Intelligence Data Pool and Intelligence Databases by OLAF is a task carried out in the public interest (combat fraud, corruption, etc., as pointed out in Article 1 of Regulation 1073/1999). Furthermore, OLAF carries out those activities in the legitimate exercise of official authority (Article 1 of Regulation 1073/1999 and 2(5) of Commission Decision 1999/352). By conducting the activities described above OLAF 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 Information and Intelligence Data Pool and Intelligence Databases 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). This implies the analysis of whether there exist other less intrusive means that can be used for the same purposes. Furthermore, the necessity has to be evaluated in connection 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.

In certain cases, the picture of the person concerned may be included in the Intelligence Database. A picture may reveal racial or ethnic origin, and therefore, Article 10.1 of the Regulation has to be considered. The processing of this data is, in principle, prohibited. However, in the present context, the exception of Article 10.5 of the Regulation may be applicable. Nevertheless, a picture should not be systematically included, and consideration has to be given to the nature of the case, and the necessity to process this data to fulfil the mandate entrusted to OLAF by the Treaties and legislation above mentioned. The EDPS recommends evaluating the inclusion of a picture of the person concerned on a case-by-case basis.

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."*

Given the purpose of the processing activity described, the data categories used can be considered, in principle, as respecting the legal obligation mentioned in the paragraph above.

Nevertheless, considering the different types of requests for information and intelligence that OLAF may receive, as described in point 2.1.f, consideration of this principle must be taken on a case-by-case basis each time that an answer is delivered. The data category(ies) that is/are non-adequate, non-relevant or excessive in the light of the particular case to which the request is connected must then be excluded.

This can take the form of a general recommendation to the persons handling the requests reminding them of the rule and recommending that they ensure respect of the rule.

The explanation given in the notification concerning the processing of "marital status" and "family members" data categories (i.e., that they are not processed unless relevant to the specific case in question) is accepted by the EDPS, provided those categories are not further processed. This means that the reports to be created can not contain such categories unless relevant for the case.

In what concerns the Intelligence Database, not all the entries would be relevant for all the cases. More precisely, this principle has to be borne in mind specially in connection to open fields, such as "comments", where there is a risk to include data that are not adequate, relevant or could be excessive. Furthermore, this principle has to be respected also regarding the data related to "Organisations", when these data could be related to individual persons.

Therefore, a general recommendation to the persons handling the Intelligence Databases, reminding them of the rule and recommending them to ensure the respect of the rule has to be drafted.

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."*

The system, as described, has certain features that aim at achieving data accuracy. 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 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 (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).

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 relates 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 has suggested in case 2005-0418 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. The same position is adopted by the EDPS herein.

The retention policy described in point 2.1.k of the present Opinion for the other cases can be considered as respecting Article 4(1)(e) of the Regulation.

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".*

As described in point 2.1 of the present Opinion, intelligence data is transferred internally within OLAF. 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.

Furthermore, OLAF must include a note in the file acknowledging the transfer of intelligence data.

- Transfer of personal data to Member States

As explained in point 2.1.j, transfers to national authorities can take place within the context of operational activity of which the information/intelligence officer is a part and direct information support is requested from or offered to competent authorities.

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 all sectors, including judicial authorities in criminal matters; and (B) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC does not cover judicial authorities in criminal matters.

As to scenario (A), Article 8 of the Regulation should be recalled by OLAF: *"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, (...)."*

Where under Article 8(a) of the Regulation, it is up to the recipient to establish the interest and necessity to receive the information, given the specific activities of OLAF, the EDPS understands this provision to mean that if the sending of the information is not carried out at the request of the recipient, the sender should accredit such a need. Accordingly, each and every time when OLAF sends personal information to competent national authorities on its own initiative, OLAF should establish that the data are necessary for the performance of a task carried out in the public interest. This is an assessment that OLAF agents must carry out each time when they transfer personal information. OLAF agents responsible for mutual assistance exchanges should be made aware of this rule.

Compliance with Article 8(a) of the Regulation requires the addressees of the information to use the data to perform a task in the public interest. The EDPS considers that the sending of the personal data in mutual assistance exchanges *in abstracto* can be seen to fulfil the conditions of Article 8(a) insofar as the national authorities to whom the information is sent are authorities of Member States that are competent for the carrying out the purposes of the processing. Such authorities will use the data to perform tasks in the public interest by carrying out related intelligence, investigation and operational activities for the prevention, investigation and prosecution of (suspected) breaches of customs and agricultural regulations.

As to scenario (B): for those Member States that have not extended their implementation of Directive 95/46/EC to judicial authorities in criminal matters, 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 those 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. 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.[19] 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.

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 intelligence activity 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).

The general rule applied by OLAF is the provision of access to the personal data related to the data subject contained in the intelligence documents. 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. Furthermore, specific acknowledgement of any restriction based on Article 20 of the Regulation must be included in the file related to the specific request.

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 intelligence activity, 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, to which the intelligence activity is linked. 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

[19] See Opinion 4/2007 on the concept of personal data (WP 136), adopted on 20 June 2007.

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 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 2.2.8).

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 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.[20] Therefore, the EDPS recommends the respect of the confidentiality of the identity of whistleblowers during OLAF intelligence operations and in the later stages (if, for instance, disciplinary and judicial authorities request their identity) in as much as this would not contravene national rules regulating judicial procedures.

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

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 intelligence operations 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.

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).

Therefore, it is observed that OLAF respects the obligations established by Article 13 and 14.

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 is always collected indirectly, for instance, through different databases, whistleblowers or informants.

The provisions of Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) are thus applicable to the present case. This means that the relevant information must be given 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.

As concerns the moment to provide this information, when intelligence activities are conducted as part of an investigation, the information has to be given when appropriate and thus when it will not hamper the investigation. Indeed, the moment of the provision of the information may be different from the moment when the data are first recorded or disclosed, in the light of Article 20 of the Regulation (see below). Therefore, the EDPS considers that information provided through the use of letters in the proper moment of an investigation, as described in point 2.1, is respectful of the Regulation.

As to the data subjects whose names appear in the documentation under analysis, but who are not persons concerned, witnesses, whistleblowers or informants, the obligation to provide directly the information could only be replaced by the indirect provision through the privacy statement published on OLAF website, when such activity would be impossible or would involve a disproportionate effort (the fact that "these individuals have no relevance to the matter under investigation", as mentioned in point 2.1, is not decisive from a data protection perspective).

The same principle has to be applied when intelligence is conducted independently of an investigation. Indeed, the EDPS considers that the provision of information through the OLAF Europa website when intelligence is conducted independently of an investigation is a positive step towards complying with Article 12 of the Regulation and it is a measure to enhance transparency regarding the data processing operations in which OLAF is engaged.

However, the EDPS is concerned by the fact that many data subjects which are the object of these activities may not visit OLAF website, and thus, may never have access to such information. This emphasizes the need to supplement the publication on the web site with personalised information notices addressed to individuals. The EDPS therefore calls upon OLAF to develop practices in providing personalised information to the individuals concerned to the degree it is appropriate in the context of intelligence activities and inform the EDPS about such guidelines.

As far as the exception to the rule of Article 12 is concerned, 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 intelligence activity, 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 paragraph 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).

A final point to be considered is Article 43a of the Implementing Rules of the Financial Regulation,[21] which requires the provision of information in the grant or procurement calls, that for the safeguarding of the financial interest of the Communities, beneficiaries' personal data may be transferred, among others, to OLAF. This general information should in no way prejudice the right of data subjects to receive from OLAF the information listed in Articles 12, where applicable. In the case of OLAF, which is an investigative body, contrary to auditing bodies where the processing in most cases is a mere storage and the assessment of personal aspects is not the purpose, the personal data processing by OLAF is focused on personal behaviours and specific risks are present (hence Article 27 of the Regulation), which makes it necessary, for the processing to be fair, to inform data subjects in a more detailed way. The inclusion of information regarding OLAF has been promoted by the EDPS as a transparency measure, but cannot be understood as a sufficient condition to fulfil the exception of Article 12 *"except where [the data subject] already has [the information]"*.[22]

---

[21] Commission Regulation (EC, Euratom) No 2342/2002 of 23/12/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 357, 31/12/2002, p. 1); Amended by the Commission Regulation (EC, Euratom) No 1261/2005 of 20/07/2005 (OJ L 201, 02/08/2005, p. 3), the Commission Regulation (EC, Euratom) No 1248/2006 of 07/08/2006 (OJ L 227, 19/8/2006, p. 3), and the Commission Regulation (EC, Euratom) No XXX of 23/04/2007 (OJ L 111 of 28/04/2007)

[22] For this exception being applicable to OLAF, see the EDPS' opinion on the special case of Monitoring by OLAF (case 2006-0548, point 2.2.8.)

2.2.9. Security measures

[...]

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 inclusion of a picture of the person concerned on a case-by-case basis;
- evaluate the proportionality of the processing activities on a case-by-case basis;
- guarantee the respect for the data quality principle. This could take the form of a general recommendation to the persons handling the intelligence requests, reminding them of the rule and recommending them to ensure the respect of it;
- respect the data quality principle regarding data related to "Organisations", when these data could be related to individual persons.
- not include in the reports it issues the references to the "marital status" and "family members", unless this is relevant for the specific request being dealt with;
- 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;
- 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. Furthermore, OLAF must include a note in the file acknowledging the transfer of intelligence data;
- establish the necessity of the transfer to national authorities in a reasoned decision, in the light of Article 8 of the Regulation;
- acknowledge in the intelligence 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 intelligence activities and in the later stages when appropriate;
- conduct a necessity test when any restriction to the right of information is applied;
- provide the information (Article 12 of the Regulation) to the data subjects whose names appear in the documentation under analysis, but who are not persons concerned, witnesses, whistleblowers or informants, unless such activity would be impossible or would involve a disproportionate effort, in which case the obligation to provide directly the information could only be replaced by the indirect provision through the privacy statement published on OLAF website. Apply the same principle when intelligence activities are conducted independently of an investigation;
- supplement the publication on the web site with personalised information notices addressed to individuals (unless such activity would be impossible or would involve a disproportionate effort). The EDPS therefore calls upon OLAF to develop practices in providing personalised information to the individuals concerned to the degree it is

appropriate in the context of intelligence activities and inform the EDPS about such guidelines;

- [...]

Done at Brussels, 21 November 2007.

Peter HUSTINX
European Data Protection Supervisor