EUROPEAN DATA PROTECTION SUPERVISOR

Case Reference
2011-0471

REPORT

ON

INSPECTION PURSUANT TO ARTICLE 47 (2) OF REGULATION (EC) N. 45/2001

European institution/body concerned:

European Anti-Fraud Office (OLAF)

EDPS
Supervision & Enforcement Unit

INSPECTION TEAM

Maria Veronica PEREZ ASINARI	Team leader
Laurent BESLAY	Inspector
Isabelle CHATELIER	Inspector
Dario ROSSI	Assistant inspector

INSPECTION SUPERVISION

Sophie LOUVEAUX	Head of Unit Supervision & Enforcement

DIRECTOR

Christopher DOCKSEY	Director

ASSISTANT SUPERVISOR

Giovanni BUTTARELLI	Assistant European Data Protection Supervisor

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 41 of Regulation (EC) No. 45/2001 (hereinafter referred to as "the Regulation") responsible for:

- Monitoring and ensuring the application of the provisions of the Regulation and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a EU institution or body;
- Advising EU institutions and bodies and data subjects on all matters concerning the processing of personal data.

To these ends, the EDPS fulfils the duties[1] provided for in Article 46 and exercises the powers[2] granted in Article 47 of the Regulation.

Among his powers to investigate, the EDPS can conduct on-the-spot inspections. The power to inspect is one of the tools established to monitor and ensure compliance with the Regulation[3]. The inspection at the OLAF was designed to investigate and ensure compliance with EDPS decisions in the framework of **prior checking opinions** where regular monitoring exercises had given indications that the compliance mechanism was blocked. The inspection should be viewed as the final stage before formal enforcement action under Article 47(1) of the Regulation.

The scope of the inspection encompassed certain aspects of personal data processing operations in the area of internal and external investigations conducted by OLAF, as well as the OLAF Physical and logical Access control system.

The inspection was carried out at the OLAF premises, rue Joseph II, 30, 1000 Brussels, on 14 and 15 July 2011.

This report summarises the findings identified during the inspection.

The EDPS suggests undertaking a reflexion on the need to fully ensure, by concrete and effective means, the application of the data protection rules within the OLAF. Such exercise should be primarily carried out in respect of the issues raised during the inspection (e.g. identification of data subjects, provision and deferral of information, data transfers). In a long term perspective, it would also benefit the organisation to broaden the scope of the aforementioned reflexion as to tackle also other data protection obligations.

Compliance with the Regulation would be positively affected by the provision by the OLAF of clear and consistent guidance to case handlers on how to classify data subjects in the Case Management System (hereinafter referred to as "the CMS"). The performance of regular quality checks on how the information is recorded in the CMS would also help to ensure an higher level of compliance. Provision of sufficient training to case handlers would contribute

---

[1] See Annex I.
[2] See Annex II.
[3] See EDPS policy paper on Monitoring and ensuring compliance with Regulation (EC) No 45/2001 published on 13 December 2010.

to creating a clear understanding of both data protection rules and the OLAF internal procedures and a consistent application of the data protection principles within the organisation. Such a training should also include specific sessions on the security aspects of processing operations, to help staff understand the internal requirements that they must comply with.

Regarding the issue of identifiability of natural persons from information related to legal persons, a documented methodology should be established and maintained in order to help case handlers to appropriately identify persons in the CMS.

As regard security measures,

The recommendations contained in the report must be implemented to comply with the Regulation. The EDPS will carry out a close follow-up; if need be, powers listed in Annex II may be exercised.

2. INTRODUCTION

2.1. Objective

The inspection exercise was carried out by taking into consideration the overall objectives reported below:

- Enforce controllers' obligations under the Regulation;
- Raise awareness on data protection;
- Support the work of the DPO.

2.2. Scope and limitations

The EDPS inspection team examined on site certain aspects of personal data processing operations in the area of:

(a) Internal and External investigations, with a specific focus on the degree of compliance with the:

- Opinion on five notifications for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on external investigations (Cases 2007-0047, 2007-0048, 2007-0049, 2007-0050 and 2007-0072);
- Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations (Case 2005-0418).

(b) Physical and logical Access control, with a specific focus on the degree of compliance with the:

- Security inspection report on the OLAF IT security infrastructure (Case 2007-0136);
- Opinion on a notification for Prior Checking received from the Data Protection Officer of European Anti-Fraud Office on Identity and Access Control System (premise) (Case 2007-0635);
- Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on CBIS Identity and Access Management System (IT system) (Case 2008-0223).

The decision to carry out an inspection was determined by taking into account the following points:

As to (a):

- The Internal and External investigations Prior Checking Opinions were adopted in 2006 and 2007 respectively. These areas could be identified as OLAF core activities, in the context of which highly sensitive data is processed. For this reason the EDPS has paid special attention to the implementation of the main data protection obligations;

- Each year, a high level meeting takes place between the EDPS and the OLAF with the aim of taking stock of compliance with the Regulation. Information is exchanged and specific areas where implementation might present difficulties are tackled. During the Annual Meeting of 2010[4], an agreement was made as to the standards that the OLAF should achieve in terms of identification of data subjects, provision of information and registration of transfers in the Data Protection Module of the CMS;
- On 28 October 2010, the OLAF sent a letter to the EDPS informing that the standards set for the OLAF backlog and the registration of transfers had been largely achieved. The letter also mentioned the intention of the DPO to conduct an audit;
- On 25 November 2010, the EDPS sent a letter acknowledging these results, and requesting the audit report drafted by the DPO;
- On 16 May 2011, a copy of the DPO's audit report was provided to the EDPS. Some shortcomings are pointed out as to the implementation of certain data protection obligations, mainly as to identification of data subjects and the obligation to inform.[5]

---

[4] During the annual meeting EDPS-OLAF of 2009 it was agreed that the OLAF would submit a plan to deal with the backlog. The EDPS said that substantial effort would be requested as from January 2007. On 3 April 2009, the OLAF submitted the following proposal: *"(1) Investigations initiated after 1 May 2008: staff have already been instructed to satisfy the information requirement for this group of cases; (...)"*.

However, during the annual meeting EDPS-OLAF of 2010, the EDPS expressed some disappointment in respect of the implementation of this plan. In advance of the meeting, the EDPS requested and received the statistics of the Data Protection Module. The figures showed, among other aspects, that the privacy statement had in fact only been sent in 31.5% of the cases belonging to the period where the EDPS requested "substantial effort" (2007-2010).

The EDPS requested, among other things, that the "pendings" (cases where the privacy statement has not been sent, even if data subjects have been identified, and no deferral applies) have to diminish to "5%-10%" over the period 2007-2010.

The issue of the definition of DS1 and DS3, as well as companies as data subjects, have been addressed. The EDPS expressed that *"if the persons have some relevance to the case they have to receive an individual notice, and OLAF has to record the fact that this notice was given"*.

In the context of this meeting, the EDPS also mentioned the information received from the OLAF confirming that the Directorate A, B and C had instructed staff to register transfers, in internal and external investigations, concerning the DS1, DS2 and DS3. The EDPS welcomes that.

[5] The audit focussed on "Directorate B's implementation of the information requirement".

"The main findings of this audit are:
In 53% of the cases, the investigator had not listed in the CMS Data Protection Module (DPM) one or more of the data subjects (DSs) 1, 2 or 3 (corresponding to persons concerned, informants/whistleblowers, and witnesses) whose names appear in the case file. This violates the instructions of the Director General, as set forth in the "Guidelines for OLAF staff regarding practical implementation of data protection requirements" (OLAF DP Guidelines). As a result, the investigator, his/her hierarchy, and any subsequent case handler would have been unable to verify whether a privacy statement had been provided to the unlisted data subjects (unless he/she has gone into the case file and reviewed various documents to find the names of those DSs, determined whether they are DS1, 2 or 3s, and found the privacy statement on a document addressed to them). Moreover, statistical data generated in October 2010 from the DPM on compliance with the information requirement for OLAF's backlog of cases do not accurately portray the reality of the case files at that time. (...)".

The DPO reported that in 64% of the cases audited there was a problem of some sort (not all DS1s, 2s, and 3s appearing in a Report (Mission, On-the spot, Interview) are listed in DPM; DS1, 2 or 3 incorrectly categorised as

Checks were carried out on a sample of randomly selected cases of both the internal and external investigations (Directorate A and B) and were targeted to assess (1) the identification of data subjects; (2) compliance with the obligation to inform; and (3) compliance with registration of transfers and provision of transfer clauses.

As to (b):

- The OLAF has developed several complex and large scale IT infrastructures in order to support its investigation activities and guarantee its operational independence. These tools, which were initially hosted by the Data-centre of the European Commission, have been transferred to OLAF premises and are managed directly by OLAF staff;

- The OLAF has decided to manage physical and logical access controls via the use of biometric matching systems, the processes of which present specific risks;

- The report of the horizontal security inspection (based on a series of Prior Check notifications) conducted in 2007

2.3. Methodology

The inspection was performed in accordance with the procedures established in the EDPS inspection Guidelines and by relying on the cooperation of the staff members and managers of the OLAF to provide requested information, data, documents and access to premises.

In particular, meetings and interviews were set up and held with staff of the OLAF to gather information and obtain access to relevant electronic databases, files and premises. Analysis, reviews and verifications of the information collected coupled with the outcome of physical examinations carried out by the EDPS team constitute the basis for the observations and recommendations in this Inspection report.

Minutes of the meetings were drafted in order to document the inspection procedures applied and to provide for a transcript of the conversations with the OLAF staff. Two original copies of the minutes have been prepared, submitted for comments and signed by the EDPS inspectors and by the representatives of the OLAF[6].

DS4; "No DS" button clicked but DS exists; Information still pending or deferred when should be provided; No privacy statement or incorrect privacy statement on non-CMS form; Information incorrectly listed as deferred when already provided).

[6] For acknowledgement of receipt.

2.4. Schedule

The inspection at the OLAF is part of the EDPS annual inspection plan for 2011. The formal Decision was communicated to the OLAF on 13 July 2011. The fieldwork was carried out on 14 and 15 July 2011.

3. ANALYSIS AND RECOMMENDATIONS

3.1. Part (a): Internal and External Investigations (*Case 2005-0418 and cases 2007-0047, 2007-0048, 2007-0049, 2007-0050, 2007-0072)*

3.1.1. Identification of data subjects

The OLAF has been requested to provide the EDPS with the list of internal and external investigation cases that have been opened since 1 May 2008. The document discloses the following split:

- Internal investigations: 138 cases;
- External investigations: 327 cases.

15 cases (5 internal investigations and 10 external investigations) have been randomly selected by the EDPS to be checked.

Fact(s):

The OLAF has internally elaborated a classification of data subjects by identifying the following 5 categories:

- DS1 - person concerned;
- DS2 - informant/whistleblower;
- DS3 - witness;
- DS4 - other person whose name is in the case file;
- DS 5 - staff of the OLAF operational partner.

The classification is defined in the Guidelines for OLAF staff regarding practical implementation of data protection requirements[7]. It serves to differentiate the way data protection obligations are implemented, taking into account the relevance of certain categories for the investigation, the risks for the protection of personal data and other fundamental rights.

The EDPS has endorsed the classification proposed by the OLAF. However, it has to be noted that it stands as an internal classification which cannot undermine compliance with the Regulation.

[7] Guidelines were adopted in December 2008; new Guidelines were adopted in October 2010.

The Director General has instructed case handlers to list in the CMS Data Protection Module (DPM) the data subjects identified in the course of the case handling, in accordance with the agreed classification.

Action(s):

Case handlers were asked to show the EDPS inspection team the identification of relevant DS 1, 2 and 3 in the DPM, and to explain the criteria followed to classify a person as DS4. For the selected external investigation cases where no data subjects were identified, the EDPS carried out an in-depth check and reviewed the documents in the file. In case of legal persons, case handlers were asked to explain which parameters they took into account to determine the non-identifiability of DS1s.

Findings:

- Internal investigations: Data subjects (DS1, DS2, DS3, DS4) have been correctly identified in the 5 selected cases.
- External investigations:
  - Data subjects have been correctly identified/not identified in 6 out of the 10 selected cases (properly identified in 3 cases; correctly not identified in the other 3 cases since there were no valid or sufficient elements for identification);
  - Data subjects have been incorrectly identified/not identified in the remaining 4 cases (not identified in 3 cases, even where there would have been elements to proceed to the identification; wrongly identified as DS4 in one case).

The low level of identification of data subjects in the CMS in external investigation cases is particularly regrettable, especially in the light of OLAF's own commitments, from 7 May 2008 onwards, that all case handlers would fill in the "Persons" tab in the CMS.

This low level of identification of data subjects in the CMS in turn results in a low level of compliance with data protection requirements.

Lack of consistency of the instructions to case handlers was noticed (particularly for those in Directorate B who received internal guidance which contradicts the OLAF Guidelines). This created confusion for case handlers as to what a DS1 is.

In a nutshell, shortcomings relating to the identification of data subjects in external investigations are of the following nature:

1. Identification as DS1:

[redacted]

[8] Evidence 17 is a copy of a *"Verbale di controllo e verifica sul posto"*. The following elements are observed:

- When a case handler was asked "Is it correct to say that you consider a person as DS1 only when he/she is declared guilty by a judge?", he answered: "

In one case, the notice given to a person (see evidence number 17[8]) is similar to those given in the context of a "suspect's statement in Court". The person who received such notice in this case was, nonetheless, classified as DS4, i.e. not relevant for the case. Considering the notice provided, which contained a statement of his/her judicial rights such as the right not to incriminate oneself, it cannot be sustained that the person was not at all relevant for the case and that he/she was not a person concerned. It would therefore have seemed logical to classify him/her as DS1.
And even in cases where individuals are being investigated at national level, they have not been marked as DS1 by the OLAF[9];

2. Identification as DS3:

3. Identifiability of natural persons (relevant for the investigation) from information related to legal persons:

In this context, the EDPS notes that there is no uniform criteria or methodology providing a description on when such identification is necessary and what steps should be followed, what the limits are, etc. to determine whether personal data relating to a natural person is being processed;

---

1) Mention is made of the *"Operatore economico presso il quale il controllo viene effettuato"*, as well as of the *"Rappresentanti dell'operatore economico"*;
2) The description of facts reads as follows: *"Al predetto rappresentante dell'operatore economico (responsabile legale) è stata data comunicazione che: (...)*

- *Della sua possibilità di esprimersi in una delle lingue ufficiali dell'Unione Europea. (...)*
- *Del mandato dei funzionari che incontra, così come da lettera d'incarico esibita.*
- *Che il presente atto potrà essere utilizzato quale fonte di prova in procedimenti legali di natura penale, civile, amministrativa o disciplinare.*
- *Che ha il diritto d'essere assistito da un legale o da altra persona di fiducia che sia presente alla redazione del presente atto.*
- *Che ha il diritto di non rendere dichiarazioni autoincriminanti"*

[9] In the context of the same case for which evidence 17 was collected, a letter was sent by the OLAF on

4. Practical problems mentioned by some case handlers:

- Difficulty to check the identity of people:

-

Recommendations:

Taking into account the findings reported above, the EDPS recommends the OLAF to:

1. Make sure that clear and consistent guidance is issued and provided to the case handlers on how to apply the criteria for classifying data subjects, particularly DS1 and DS3 which have proved to be the most problematic ones with a view to ensure that **all** data subjects are properly and duly informed. From a data protection perspective, a person must be considered as a data subject when information relating to him/her is collected. This is clearly stated in the OLAF Guidelines[10]. It was previously emphasized by the EDPS[11] and was clearly endorsed by OLAF[12]. In the cases dealt with by OLAF, data subjects can be identified as the natural persons who have some relevance for the case, whatever the person under investigation (natural person or legal person) and whatever the reason for such relevance. Therefore, a person may have relevance for the case not necessarily because he/she is considered as a suspect or he/she has any responsibility in the matter under investigation; the concept of data subject is more neutral. It simply indicates the physical person to whom the data relate. The obligation to provide information to data subjects should therefore not be unduly limited to only those persons who are considered to be suspects, but should include all persons relating to whom data have been collected on an identified basis. While the EDPS understands that the internal classification of data subjects by OLAF has been implemented to help provide information to data subjects, and therefore to ensure respect of the data protection obligation set forth in Articles 11 and 12 of the Regulation, it should be ensured that the notion of data subjects is clearly understood by case handlers so as not to undermine data subjects' right to data protection.

---

[10] See footnote 7.

[11] In the annual meeting between the OLAF and the EDPS on 2 March 2010, the EDPS stressed that "The point is that if the classification you have created -DSs1, 2, 3, 4 and 5- does not respond to the reality you can change it. However, if the persons have some relevance to the case they have to receive an individual notice, and OLAF has to record the fact that this notice was given. You have some flexibility in the way you can do so, but it has to be clear in your rules of procedure. Imagine that you are in a mission in '. You have people around the table from whom you collect information. In your mission report it has to be clear that all these data subjects have received individual notification."

[12] See letter from Mr Illet to the EDPS of 13 April 2010, where Mr Ilett stated: "OLAF agrees that all person from whom information is gathered in the context of an external investigation or other type of cases are data subjects. Depending on their role they may fit into different categories. In the context of a meeting in a third country, where the role of each person is not yet determined, OLAF intends to provide the privacy notice to every

2. Ensure, by concrete and effective means, the application of the data protection rules, as foreseen in the OLAF Guidelines. The OLAF should at least make sure that case handlers are reminded of their duty to register data subjects in the data protection module and should monitor the effective and correct application of the instructions by performing regular quality checks;
3. Elaborate and document clear criteria and guidance on the identifiability of natural persons from information related to legal persons and provide clear instructions on how to register them in the DPM;
4. Provide the EDPS with further explanations on how the difficulty to check the identity of people might interfere with compliance with data protection obligations. The EDPS underlines that even when the case handler cannot prove with certainty the identity of particular persons, he/she should still identify these persons and respect data protection obligations. If need be, the identity can always be corrected in the DPM later on.
5. Provide training to case handlers, in order to ensure (a) a clear understanding not only of data protection rules but also of the OLAF internal implementation particularities (b) uniformity in the implementation of data protection obligations, irrespectively of the Directorate under which the data processing activity is carried out.

3.1.2. Compliance with the obligation to inform

Fact(s):

Information under Articles 11 and 12 of the Regulation may be provided at different stages of an investigation depending on the need to apply Article 20 exceptions (i.e. whenever providing the notice would be harmful for the investigation).
In its Prior Checking opinions on the OLAF external[13] and internal[14] investigations, the EDPS made the following recommendations regarding the obligation to inform:

- "respect the content of the information to be given to the data subject as mentioned in paragraph 1 of Article 11 and 12 of the Regulation (including sub-paragraph f)";
- "acknowledge in the files when any restriction based on Article 20 of the Regulation is operated";
- "inform the data subject in compliance with Article 20.3 and 20.4 of the Regulation where appropriate".

Action(s):

---

person whose name is recorded at the time they are met, and to register that fact, together with the names of the persons who have received the notice, in its mission report. OLAF will not record the names of those data subjects in the Data Protection Module. When it is clear that an identifiable data subject has relevance to an investigation, and can be categorised as DS1, 2 or 3, OLAF will provide an individual privacy notice if the data subject has not yet received the required information."

[13] Cases 2007-47, 2007-48, 2007-49, 2007-50, 2007-72.

[14] Case 2005-418.

For the selected cases, case handlers were asked to explain to which data subjects (DS1, DS2, DS3) the information notice had been sent and to provide the EDPS with evidence that this had actually been done. In case the obligation to inform had been deferred, case handlers were asked to show (a) the note to the file evidencing and justifying the decision taken, (b) the reason for the restriction and (c) proof that the decision for deferral was still valid at the date of the EDPS inspection.

- **Findings:**

  - Internal investigations: The privacy notice has been correctly provided in the 5 selected cases.
  - External investigations:
    - The privacy notice has been correctly provided/not provided in 6 out of 10 selected cases (appropriately provided in 4 cases; correctly not provided in 2 cases since there were no valid or sufficient elements for identification of the DSs);
    - The privacy notice has incorrectly not been provided in the remaining 4 cases.

Problems detected with respect to the provision of information in the framework of external investigations can be summarised as follows:

- Case 1: Though certain persons had provided information to the OLAF in the context of a mission, they were not identified as DS3 and, consequently, did not receive a privacy notice;
- Case 2: Most of the data subjects have been identified as DS4 (according to the OLAF classification, the DS4 is a person considered to be as not relevant for the investigation, therefore, supposed not to receive the privacy notice), even if elements have been found in the file which show that, in some cases, they could have been identified as DS1 (i.e. evidence number 17 above mentioned, letter of
- Case 3: A person from a company provided information to the OLAF during a mission. This person has not been identified as DS3, therefore, he/she did not receive a privacy notice;
- Case 4: . However, no data subjects were identified in the DPM and no provision of a privacy notice was registered in the DPM.

  The EDPS staff was unable to check whether the provision of information was registered there.

The EDPS notes that there exists a clear connection between the shortcomings observed in the identification of the DSs and the lack of compliance with the obligations imposed by Article 11 of Regulation (provision of information to the data subject).

Recommendations:

Taking into account the findings reported above, the EDPS recommends the OLAF to:

1. Fully implement the obligation to inform the data subjects. A new assessment of the state-of-play of the implementation of this obligation should be carried out after clear guidance as to the identification of DSs has been provided;
2. Ensure that a note is registered in the CMS file in all cases where there is a reason to defer the obligation to inform pursuant to Article 20 of the Regulation, specifying the reasons for such a deferral.

3.1.3. Compliance with the registration of transfers and provision of transfers clauses

Fact(s):

In the context of internal and external investigations, the OLAF may transfer data to the following recipients:

- To concerned EU institutions and bodies, in order to allow them to take appropriate measures to protect the financial interests of the EU, in accordance with paragraphs 9(4) and 10(3) of Regulation 1073/99[15];
- To competent Member State judicial authorities, to allow them to take appropriate judicial follow-up measures, in accordance with paragraph 10(2) of Regulation 1073/99;
- To competent third country authorities and international organisations.

In its Prior Checking opinions on the OLAF external[16] and internal[17] investigations, the EDPS made the following recommendations:

- "include, in compliance with Article 7.3 of the Regulation, notice to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted";
- "transfer the reports and/or the related documents (personal data) only if necessary for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard";
- "establish the necessity of the transfer to judicial authorities in a reasoned decision, in the light of Article 8 of the Regulation".

Although the modalities of transfers to third country authorities and international organisations have subsequently been dealt with in a separate file and not in the context of the above mentioned Prior Checking procedures, in the working document of 2005 the EDPS requested the OLAF to register them. In the context of the 2010 annual meeting, the EDPS

[15] Regulation (EC) No. 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), O.J. L 136, 31.5.1999, p. 1-7.
[16] Cases 2007-0047, 2007-0048, 2007-0049, 2007-0050 and 2007-0072.
[17] Case 2005-0418.

was informed that the OLAF Directorate A, B and C had instructed staff to register transfers in internal and external investigations concerning DS1, DS2 and DS3.

Action(s):

For the selected cases, case handlers were asked to explain to whom data had been transferred and when. They were also asked to show the EDPS the clause on transfer that was provided to comply with Articles 7, 8 and/or 9 of the Regulation.

- Findings:
  - Internal investigations: The registration of transfers and the inclusion of the transfer clause have been correctly carried out in the 5 selected cases.
  - External investigations:
    - No issue has been identified in 9 of the selected cases, either because the obligation was correctly implemented (1 case) or because no transfers took place (8 cases);
    - A shortcoming has been spotted in 1 case (a transfer was registered in the DPM but no transfer clause was included in the letter of transfer).

  The registered transfers fall under the provisions set forth in Articles 7 and 8 of the Regulation. No Article 9 transfer has been detected.

- **Recommendation:**

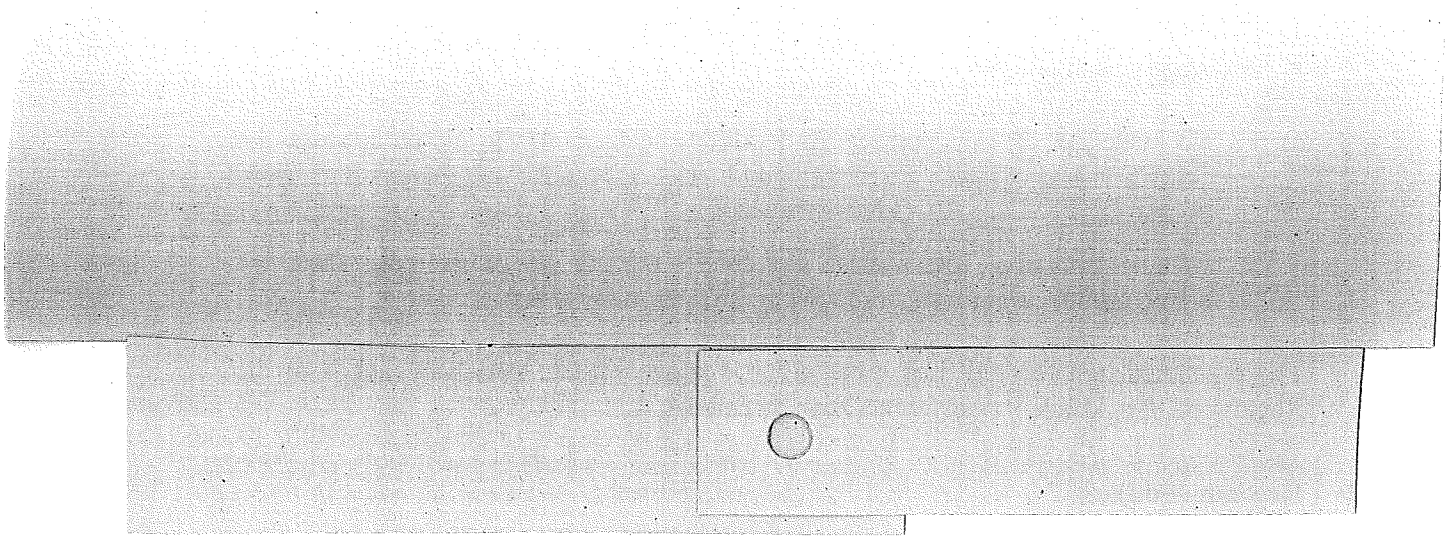
  Taking into account the findings reported above, the EDPS recommends the OLAF to ensure full compliance with the obligations relating to transfers, in particular that every transfer includes the proper transfer clause (or corresponding notice in compliance with Articles 7, 8 or 9 of the Regulation).

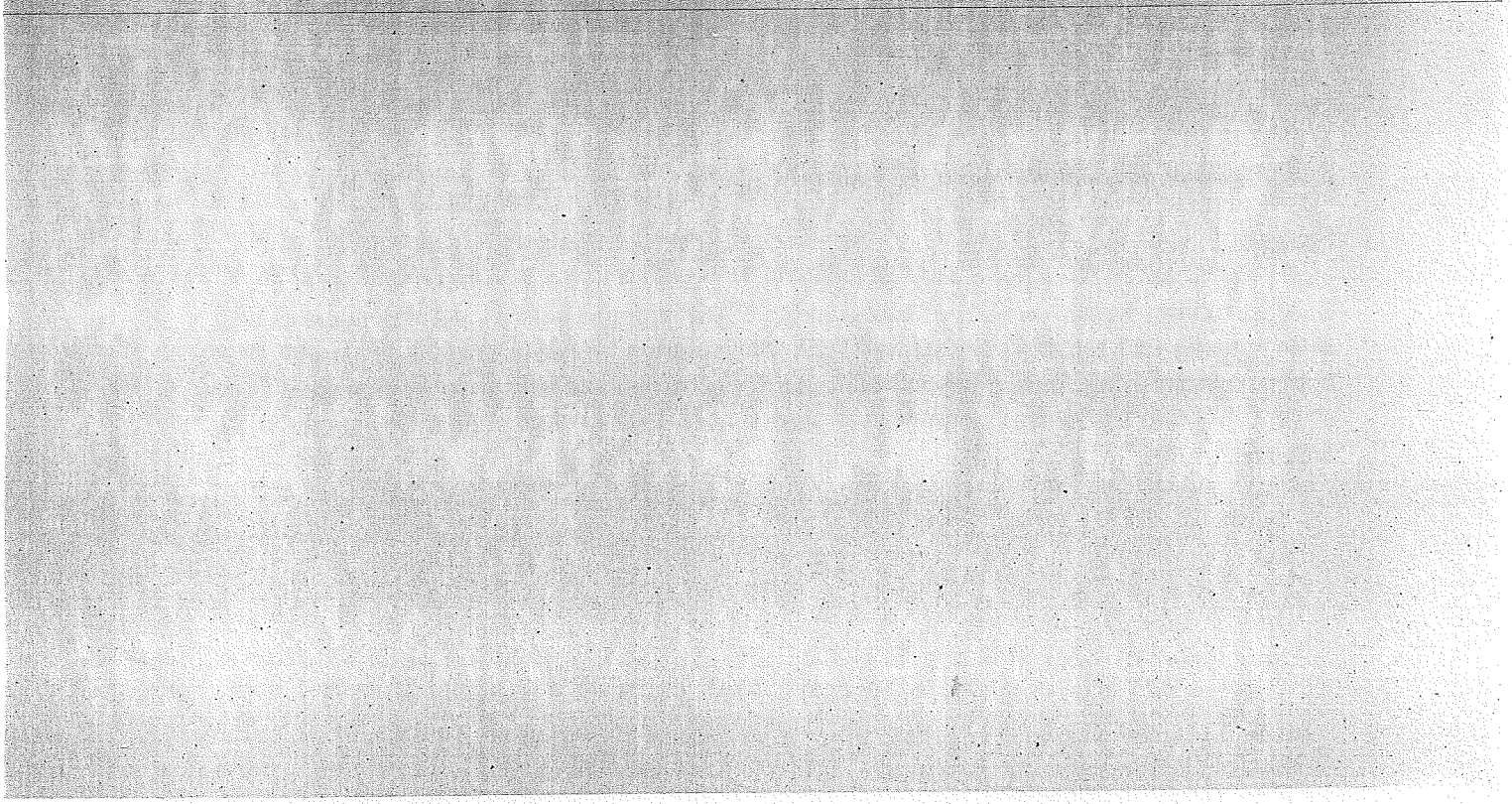
3.2. Part (b): Physical and logical Access control

3.2.1 Follow-up of the security inspection report (case 2007-0136)

Fact(s):

In 2007, the EDPS conducted an horizontal security inspection (based on a series of Prior Check notifications) in order to assess the compliance of the OLAF independent IT system with the security requirements defined by the security regulatory framework of the Commission and completed by the one of the OLAF.





3.2.2 Physical access control system (case 2007-0635)

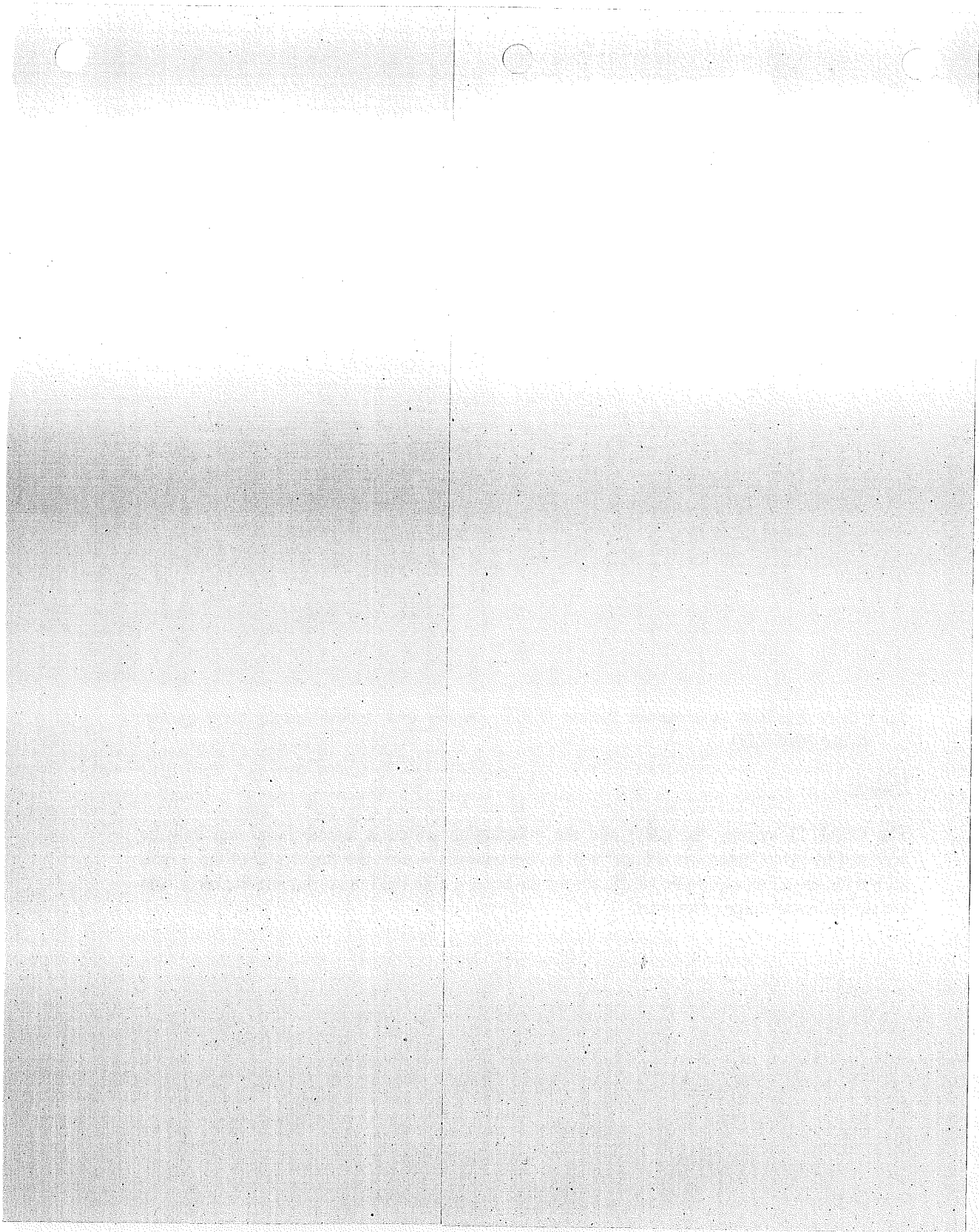
Fact(s):

In order to improve the security of access to the OLAF premise outside working hours as well as to specific and sensitive areas (greffe, IT room) during working hours, a physical access control system using fingerprints stored in the badge of the staff has been implemented. The system comes in addition to the traditional access control check conducted by the guards at the entrance.

3.2.3 Core Business Information System (CBIS) Identity and Access Management System (Case 2008-223)

Fact(s):

The OLAF IT system -the CBIS and the information which is stored there- can only be accessed by investigators via a fingerprint access control system. The fingerprint of the person allows the use of an electronic certificate for the access; both the fingerprint and the certificate are stored in the badge of the user.



ANNEX I – DUTIES OF THE EDPS

Art 46 of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter referred to as "Regulation 45/2001") sets forth the duties of the European Data Protection Supervisor as follows:

"...

(a) *hear and investigate complaints, and inform the data subject of the outcome within a reasonable period;*

(b) *conduct inquiries either on his or her own initiative or on the basis of a complaint, and inform the data subjects of the outcome within a reasonable period;*

(c) *monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;*

(d) *advise all Community institutions and bodies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;*

(e) *monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;*

(f) (i) *cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC in the countries to which that Directive applies to the extent necessary for the performance of their respective duties, in particular by exchanging all useful information, requesting such authority or body to exercise its powers or responding to a request from such authority or body;*

(ii) *also cooperate with the supervisory data protection bodies established under Title VI of the Treaty on European Union particularly with a view to improving consistency in applying the rules and procedures with which they are respectively responsible for ensuring compliance;*

(g) *participate in the activities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by Article 29 of Directive 95/46/EC;*

(h) *determine, give reasons for and make public the exemptions, safeguards, authorisations and conditions mentioned in Article 10(2)(b),(4), (5) and (6), in Article 12(2), in Article 19 and in Article 37(2);*

(i) *keep a register of processing operations notified to him or her by virtue of Article 27(2) and registered in accordance with Article 27(5), and provide means of access to the registers kept by the Data Protection Officers under Article 26;*

(j) *carry out a prior check of processing notified to him or her;*

(k) *establish his or her Rules of Procedure.*

..."

ANNEX II – POWERS OF THE EDPS

Art 47 of the Regulation 45/2001 sets forth the powers of the European Data Protection Supervisor as follows:

"...

1. The European Data Protection Supervisor may:

(a) give advice to data subjects in the exercise of their rights;

(b) refer the matter to the controller in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

(c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;

(d) warn or admonish the controller;

(e) order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;

(f) impose a temporary or definitive ban on processing;

(g) refer the matter to the Community institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;

(h) refer the matter to the Court of Justice of the European Communities under the conditions provided for in the Treaty;

(i) intervene in actions brought before the Court of Justice of the European Communities.

2. The European Data Protection Supervisor shall have the power:

(a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;

(b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

...".

ANNEX III – DECISION

Brussels, 12.07.2011

Decision of the European Data Protection Supervisor
requiring the

EUROPEAN ANTI-FRAUD OFFICE

(OLAF)

to submit to an inspection
pursuant to Article 47 (2)
of Regulation (EC) No 45/2001

Case Number
2011-0471

Decision of the European Data Protection Supervisor

of 12.07.2011

requiring the

EUROPEAN ANTI-FRAUD OFFICE

(OLAF)

to submit to an inspection
pursuant to Article 47 (2)
of Regulation (EC) No 45/2001

(Case Number 2011-0471)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000[18] on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data, hereinafter referred to as the "Regulation", and in particular Article 47(2) thereof,

Having regard to the obligation of the controller under Article 25 of the Regulation to give prior notice to the Data Protection Officer of any processing operations, some of which may be subject to prior checking under Article 27 of the Regulation by the European Data Protection Supervisor ("EDPS"),

Having regard to the EDPS Opinions on five notifications for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on external investigations (Cases 2007-0047, 2007-0048, 2007-0049, 2007-0050, 2007-0072), and on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations (Case 2005-0418),

Having regard to Security inspection report on the OLAF IT security infrastructure (Case 2007-0136), the Opinion on a notification for Prior Checking received from the Data Protection Officer of European Anti-Fraud Office on Identity and Access Control System (premise) (Case 2007-0635), and the Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on CBIS Identity and Access Management System (IT system) (Case 2008-0223),

Whereas:

1. Article 16 of the Treaty on the Functioning of the European Union enshrines the right to the protection of personal data.

2. The Internal and External investigations prior checking Opinions were adopted in 2006 and 2007 respectively. These areas could be identified as OLAF core activities, in the context of which highly sensitive data is processed. For this reason the EDPS

[18] OJ L 8 of 12.1.2007

has paid special attention to the implementation of the main data protection obligations.

3. Each year a high level meeting takes place with the aim of taking stock of compliance with Regulation. Information is exchanged and specific areas where implementation might present difficulties are tackled with.

4. During the Annual Meeting of 2010, an agreement was made as to the standards that OLAF has to achieve in terms of identification of data subjects, provision of information and registration of transfers in the Data Protection Module of the Case Management System.

5. On 28 October 2010, OLAF sent a letter to the EDPS informing that the standards set for the OLAF backlog and the registration of transfers have been largely achieved. The letter also mentioned the intention of the DPO to conduct an internal audit.

6. On 25 November 2010 the EDPS sent a letter acknowledging these results, and requesting the report of the DPO audit.

7. On 16 May 2011 a copy of the DPO internal audit report was sent to the EDPS.

8. OLAF has decided to manage its physical and logical access control with the use of biometric matching systems, the processes of which present specific risks.

9. On 11 December 2007, the EDPS report of the horizontal security inspection (based on a series of prior check notifications) underlined that several parts of the overall security infrastructure were still under development and that their compliance will only be checked at a later stage.

10 [redacted]

HAS ADOPTED THIS DECISION:

The OLAF is hereby required to submit to an inspection concerning:

(c) **Internal and External investigations**, with a specific focus on the degree of compliance with the:

- Opinion on five notifications for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on external investigations (Cases 2007-0047, 2007-0048, 2007-0049, 2007-0050, 2007-0072).
- Opinion on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations (Case 2005-0418).

(b) **Physical and logical Access control** with a specific focus on the degree of compliance with the:

- Security inspection report on the OLAF IT security infrastructure (Case 2007-0136).
- Opinion on a notification for Prior Checking received from the Data Protection Officer of European Anti-Fraud Office on Identity and Access Control System (premise) (Case 2007-0635).
- Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on CBIS Identity and Access Management System (IT system) (Case 2008-0223).

The inspection is carried out to verify facts and practices and to check, in practice, the full implementation of the recommendations contained in the various prior check Opinions issued by the EDPS, as well as the implementation of recommendations issued in the context of the security inspection that took place in 2007, in order to ensure compliance with Regulation (EC) n. 45/2001.

The inspection can take place at any premises of the institution concerned where activities covered by the Regulation are carried out and, in particular, at the premises of the head office in Brussels.

The OLAF shall permit the staff members authorised by the EDPS to carry out the inspection. It shall permit them to enter any premises during normal office hours. It shall produce any books, documents, electronic files, personal data and any other information and records related to its data processing operations, irrespective of the medium on which they are stored, as required by the said staff members. It shall permit EDPS inspectors to examine the said books, documents, electronic files, personal data, other information and records in situ and make copies of them.

It shall immediately give on the spot oral explanations relating to the subject matter and purpose of the inspection as the EDPS inspectors may require. It shall allow any representative or member of staff to give such explanations. It shall allow the explanations given to be recorded in the Minutes of the inspection.

The inspection will begin at 9:00 am on 14 July 2011.

This Decision will be notified to the OLAF on 13 July 2011.

An action against this decision may be brought before the Court of Justice of the European Union pursuant to Article 32(3) of the Regulation.

Done at Brussels on 12 July 2011

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor

ANNEX

Extracts from Official Journal of the European Communities L 8, 12.01.2001, p. 1:

Regulation 45/2001 of 18 December 2000 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

Article 30 **Obligation to cooperate**

At his or her request, controllers shall assist the European Data Protection Supervisor in the performance of his or her duties, in particular by providing the information referred to in Article 47(2)(a) and by granting access as provided in Article 47(2)(b).

Article 32 **Remedies**

1. [...]

3. Actions against decisions of the European Data Protection Supervisor shall be brought before the Court of Justice of the European Communities.

4. [...]

Article 41 **European Data Protection Supervisor**

1. [...]

2. With respect to the processing of personal data, the European Data Protection Supervisor shall be responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies.

The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and any other Community act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a Community institution or body, and for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data. To these ends he or she shall fulfil the duties provided for in Article 46 and exercise the powers granted in Article 47.

Article 46 **Duties**

The European Data Protection Supervisor shall:

(a) [...]

(c) monitor and ensure the application of the provisions of this Regulation and any other Community act relating to the protection of natural persons with regard to the processing of personal data by a Community institution or body with the exception of the Court of Justice of the European Communities acting in its judicial capacity;

(d) [...]

Article 47 Powers

1. [...]

2. The European Data Protection Supervisor shall have the power:

(a) to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his or her enquiries;

(b) to obtain access to any premises in which a controller or Community institution or body carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.