Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office on the Custom Information System

Brussels, 24 July 2007 (Case 2007/177)

1. Proceedings

On 19 March 2007, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the European Anti-Fraud Office ("OLAF") a notification for prior checking (hereinafter "Notification") regarding the Custom Information System (CIS).

On 11 May 2007, the EDPS made a request for further information to which he received the responses on 3 July 2007. The procedure was suspended during this period. The procedure was suspended again on 4 July 2007 to allow comments from OLAF's DPO which were received on 19 July.

2. Examination of the matter

2.1. Background

The current legislation setting up the CIS, i.e. Council Regulation (EC) No 515/97[1] is up for review. A proposal for a Regulation amending Regulation No 515/97 presented by the Commission is currently making its way through the legislative process towards its potential final adoption (the Proposal)[2]. On 22 March 2007, the EDPS issued an Opinion on this Proposal which, among other issues, reminds that, the CIS must be prior checked[3]. However, the current prior checking Opinion only takes into account the data processing actions that take place in CIS today, i.e. under applicable legislation.

2.2. The facts

1 Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

2 Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member Sates and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final).

3 EDPS Opinion of 22 February 2007 on the proposal for a Regulation amending Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final).

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

The Custom Information System is a central database containing personal information developed and managed by the Commission. In accordance with the Commission Decision of 28 September 1999[4], OLAF was appointed as the Commission department responsible for such development and management. The database is accessible by each Member State and by OLAF. Direct access is reserved exclusively for the national authorities designated by each Member State and the departments designated by the Commission.

This database is referred to as the 'Community CIS' or CIS falling under Community action. This is because in fact CIS consists in two separate databases, the one described above falling within the framework of European Community actions, and another one falling under inter-governmental action[5]. This Opinion does not deal with the CIS falling under the third pillar. This is because according to both Article 3 and 27 of Regulation (EC) No 45/2001 processing operations which *(i) fall within the scope of Community law* and (ii) *present specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or their purposes* shall be subject to prior checking by the EDPS. Whereas the inter-governmental CIS fulfils the second requirement *(ii),* particularly as it contains data relating to suspected offences and offences, it does not fulfil the first requirement *(i).*

The overall ***objective*** of the CIS is to assist national authorities in preventing, investigating and prosecuting operations which are in breach of customs or agricultural provisions. Towards this end, personal data included in CIS can be used for the specific purposes of sighting and reporting, discreet surveillance or specific checks.

The ***responsibility*** for the data processing that occurs within CIS resides primarily within OLAF, in particular in Unit C3 that deals with Mutual Assistance and Intelligence. OLAF, as a part of the Commission, is the data controller insofar as it processes the data for the purposes described above and its role is specifically foreseen in Council Regulation (EC) No 515/97 and Commission Regulation No 696/98[6]. In addition to using the data for the purposes outlined above, OLAF also ensures the technical management of the CIS infrastructure.

However, OLAF is not the only authority responsible for the data processed through CIS: Insofar as Member States' authorities have access to CIS, and competence to add data to and further process the data in the CIS for the purposes outlined above, they share with OLAF the responsibility for CIS and are therefore co-controllers of CIS data. Article 34 of Council Regulation (EC) No 515/97 confirms this approach by establishing that each Member State and the Commission should regard CIS as a system governed by the national provisions implementing Directive 95/46/EC. Accordingly, Council Regulation (EC) No 515/97 refers to Member States' authorities and to the Commission as *'CIS Partners'*.

Most of the ***CIS related data processing operations are automated*** and can be described as follows: Certain designated officials of the Commission and Member States have direct, online access with a user ID and a password offering the possibility to draft, upload, read and search in CIS. The designated officials include "case handlers" (also called "normal users"),

---

4 Commission Decision on the reoganisation of the administrative structures of the Commission, PERS(1999)163/4, 28 September 1999.

5 The legal bases for the inter-governmental database is the CIS Convention, Convention drawn up on the basis of Article K.3 of the Treaty of the European Union, on the use of information technology for customs purposes, No C 316, 27.11.1995.

6 Commission Regulation (EC) No 696/98 of 27 March 1998 implementing Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

and “central authorisers” (also called “privileged users”). Case handlers can read or search in the CIS, and submit drafts to their central authoriser. The central authoriser, who is the only person with the capacity to upload a case directly into CIS, then checks each draft with a view to lawfulness, opportunity and data protection issues. When the authoriser uploads the draft to the central database, all other CIS partners (both normal and privileged users) can read the data on their terminals and use the data for the purposes outlined above. Only the central authoriser that has supplied the information has the right to amend, supplement, correct or delete it. After a certain time, the data included in CIS are transferred automatically to parts of CIS to which access is limited. ***Manual data processing operations*** that take place in CIS are rather limited but nevertheless important. The decision about which data is inserted in CIS is not an automated decision. Other manual operations include the making of some print outs of information contained in CIS.

The ***data subjects*** whose data may be uploaded in CIS may be categorised as follows: First, they are persons involved in operations which constitute, or appear to constitute, breaches of the Community provisions and the associated implementing provisions governing the import, export, transit and presence of a) goods traded between Member States and third countries; b) between Member States in the case of goods that do not have Community status within the meaning of Article 9 (2) of the Treaty or goods subject to additional controls or investigations for the purposes of establishing their Community status; and c) goods resulting from the processing of agricultural products. Second, they are the officials of the Member States' authorities and OLAF working on the matter.

The ***categories of personal data*** to be included in the CIS are listed in Article 25 of Council Regulation (EC) No 515/97 and Commission Regulation (EC) 696/98. These categories refer to individuals involved in operations and include the following: *(i)* Typically identification data such as name, maiden name, forenames and aliases; (date and place of birth), nationality, sex as well as particularities and permanent physical characteristics. *(ii)* Information related to the activities that justify the inclusion of the individual in CIS, which comprises the reason for inclusion of data; the suggested action; a warning code indicating any history of being armed, violent or escaping; and the registration number of the means of transport. In addition to the above, CIS also contains some identification information regarding the officials of the Member States officials dealing with the underlying matters.

The above categories of personal data can only be included in CIS if, especially on the basis of prior illegal activities, there is evidence to suggest that the person concerned has committed, is committing or will commit actions which are in breach of customs or agricultural legislation and which are of particular relevance at Community level.

CIS does not include **special categories of data**, i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. However, CIS obviously includes data relating to alleged offences, in particular actions in breach of customs or agricultural legislation.

As far as the ***conservation of the data*** is concerned, the data included in the CIS are kept only for the time necessary to achieve the purpose for which they were included. The need for their retention is reviewed at least annually by the supplying CIS partner. After a year has elapsed and the supplying partner has decided to withdraw the data, the data will still be retained for an additional year but its accessibility will be limited and is deleted definitively after this period has expired.

The supplying CIS partner may, within the review period of one year, decide to retain data until the next review if their retention is necessary for the purposes for which they were included.

According to the Notification, data may be ***transferred*** to the following entities: *(i)* Officials of the competent authorities of the Member States and the European Commission responsible for the application of Regulation (EC) 515/97. Among these officials, direct access to CIS is restricted to those with a user ID and a password. *(ii)* With the prior authorization of, and subject to any conditions imposed by, the Member States or the Commission which included them in the system, data obtained from the CIS may, on a case-by-case basis, be communicated for use by national authorities other than those designated by third countries and by international or regional organisations in accordance with Article 30.4 of Regulation 515/97.

As far as the ***right to information is concerned***, OLAF has provided together with the Notification a privacy statement addressed to those people whose personal data are included in CIS. The privacy statement will be available on the home page of the AFIS Portal, which is accessible to the users of AFIS, and on the data protection page of OLAF Europa site, which is accessible to the general public. In addition, OLAF has informed the EDPS that if the information is used in OLAF operational activities (assessment, investigation, monitoring case, criminal assistance cases, follow-up intelligence, etc), then the information is provided to the data subject as specified in the notification for that processing operation. The privacy statement contains information about the identity of the data controller, the types of data collected, the purposes for the collection and potential transfers. It also includes information about how to exercise the right of access and the retention periods.

OLAF has informed the EDPS that it has put a procedure in place to react to ***access and rectification requests*** from data subjects. Access requests must be sent to the data controller for Customs Information System, Mr. Eddy Weyns, and an e-mail address is provided to this end in the privacy statement. The privacy statement informs that if personal data for which an application for access has been made have been supplied by another Member State, access shall be permitted only if the supplying partner has been given the opportunity to state its position.

Security measures have been adopted.

2.3. Legal aspects

2.3.1. Prior checking

Presence of the elements that trigger the application of Regulation (EC) No 45/2001

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001") applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law*"[7].

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

For the reasons described below, the EDPS considers that all the elements that trigger the application of the Regulation exist in CIS:

First, the EDPS notes that information uploaded in CIS includes *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, CIS includes identification data as well as information justifying the inclusion of the individual's data, i.e. the alleged wrongdoing. Secondly, the Notification clearly points out that the data collected undergo "processing" operations, as defined under Article 2 (b) of the Regulation (EC) No 45/2001 which include the collection, uploading, consultation, storage, etc. Finally, the EDPS confirms that the processing is carried out by a Community institution, in this case by OLAF, the European Anti-Fraud Office, which is part of the European Commission, in the framework of Community law (Article 3.1 of the Regulation (EC) No 45/2001). Therefore, clearly all the elements that trigger the application of the Regulation exist in CIS.

Assessment of whether the data processing operations fall under Article 27 of the Regulation

Article 27.1 of the Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes".* Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks.

The EDPS considers that the prior checking Notification regarding CIS clearly falls under Article 27.2. of Regulation (EC) No 45/2001.

In the first place, such data processing operations fall under Article 27.2(a) of Regulation (EC) No 45/2001, which establishes that processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" shall be subject to prior checking by the EDPS. In the case in point, CIS contains information about persons who have committed or there is evidence to suggest that they have committed or are committing or will commit actions which are in breach of customs or agricultural legislation and which are of particular relevance at Community level.

The EDPS considers that the processing of data that occurs within CIS also falls under Article 27.2(b) of the Regulation (EC) No 45/2001 which stipulates that data operations which *"evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall be subject to prior checking by the EDPS. Indeed the data included in CIS may be used to evaluate the conduct of the individuals who are alleged to be involved in wrongdoings in order to determine the appropriate measures to take (apprehension, etc) and ultimately bring them to Court.

Since prior checking is designed to address situations that are likely to present specific risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have 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 19 March 2007. Complementary information was requested on 11 May 2007. The answers were received on 3 July 2007. Pursuant to Article 27.4 of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended during such interval. The procedure was suspended again on 4 July 2007 until 19 July 2007 to allow comments from the DPO. The Opinion will

therefore be adopted no later than 26 July 2007 (deadline was 22 May plus 67 days of suspension).

2.3.2. Lawfulness of the processing

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

As pointed out in the Notification for prior checking, of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed only if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001 three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out by OLAF, second, whether the processing operations are performed in the public interests and, third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

The EDPS notes that ***relevant legal grounds justifying the creation of CIS exist in EU legislation***. In particular, the EDPS notes that Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters foresees the creation of the Customs Information System.

Council Regulation (EC) No 515/97 not only foresees the creation of CIS but also sets forth in significant detail the features of CIS. For example, Article 23 deals with the establishment of CIS, Article 24-31 with the operation and use of the CIS, Articles 32 and 33 with the amendment of CIS data, Article 33 with data retention, Article 37 with supervision and Article 38 with security aspects. The types of data to be included in CIS are regulated by Article 25 which is complemented by Commission Regulation (EC) no. 696/98 of 27 March 1998[8].

The EDPS notes that OLAF carries out the processing activities in the **public interest.** The processing of CIS data serves to fight fraud in the context of the customs union and common agricultural policy, in particular, to assist Member States authorities in their efforts. Such assistance must be considered as serving to the overall public interest.

According to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "***necessary for performance of a task***" as referred to above. It is clear that cooperation and exchange of information among Member States and the Commission strengthen the fight against fraud. In this regard, CIS can be deemed as a necessary tool towards fighting fraud in the context of the customs union and common agricultural policy. Taking into account that Council Regulation EC) No 515/97 confers upon OLAF the competence and the obligation to

[8] Commission Regulation (EC) no. 696/98 of 27 March 1998 implementing Council Regulation (EC) No 515/97 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

manage CIS and use it to assist national authorities, it can be said that CIS is a necessary tool to fight fraud.

However, the EDPS notes that the real "necessity" of the data processing has to be analysed *in concreto,* for each particular case when information is uploaded. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the uploading and using CIS data has to be proportional to the objectives of processing (combat fraud in the context of customs union and common agricultural policy etc) and to the particular purpose of each particular case. Thus, the proportionality has to be evaluated on a case-by-case basis.

2.3.3. Processing of special categories of data

The Notification states that no data falling under the categories of data referred to in Article 10.1 are processed in the context of the CIS. This is in line with the Article 25 of Council Regulation EC) No 515/97 which establishes that "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical believes, trade union membership and data concerning the health or sex of live of an individual shall not be included {*in CIS}".

However, CIS obviously includes data relating to alleged offences, in particular actions in breach of customs or agricultural legislation. In particular, one of the data fields of CIS calls for information explaining the reason for inclusion of the data, which is likely to be a description of the alleged wrongdoings regarding an or various individuals. Another data field calls for information regarding any history of the individual being armed, violent or escaping, which relates to offences. In this regard, the EDPS recalls the application of Article 10.5 of Regulation (EC) No 45/2001 which establishes that *"[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor."* In the present case, processing of the mentioned data is expressly authorised by the legal instruments mentioned in point 2.3.2 above.

2.3.4. Data Quality

Pursuant to Article 4.1.c of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which it was collected and/or further processed. This is referred to as the data quality principle.

The EDPS notes the types of data included in CIS as stated in sections 17 and 18 of the Notification for prior check. Such data coincides with the categories of data that CIS must contain in accordance with Article 25 of Council Regulation (EC) No 515/97 and by the Commission Regulation (EC) no. 696/98 of 27 March 1998.

The EDPS considers that the data quality principle is respected in CIS insofar as: *(i)* there is a defined list of personal data that may be included, whose content seems reasonable for the purposes sought by CIS; *(ii)* the data can only be included if "especially on the basis of prior illegal activities, there is evidence to suggest that the person concerned has committed, is committing or will commit actions which are in breach of customs or agricultural legislation and which are of particular relevance at Community level"[9] and, *(iii)* the number of

[9] Article 27(2) of Regulation (EC) No 515/97.

individuals empowered to access the data is limited to national authorities designated by each Member States.

This being said, it is not possible for the EDPS to determine whether such data are appropriate in *all* specific cases. Whether such data are appropriate or not will depend on the particular case at stake. In order to ensure that Member States and OLAF agents process data in accordance with the data quality principle, the EDPS suggests issuing guidelines addressed to agents with access to CIS reminding and describing the rules to follow towards ensuring the quality principle.

In addition to the above, it is important to recall the application of Article 4.1(d) of the Regulation (EC) No 45/2001 requires that personal data must be "*accurate and where necessary kept up to date",* and "*every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."* The procedures described under Section 2.5. requiring the annual review of the information by the supplying partner contribute towards the accuracy of the data stored in CIS insofar as these procedures require an ongoing analysis of the information. The EDPS considers that all in all the current practices at OLAF ensure that the personal data kept in CIS are accurate and complete and calls upon OLAF to continue implementing such procedures.

2.3.5. 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".*

According to OLAF's Notification, the data included in the CIS are kept only for the time necessary to achieve the purpose for which they were included. The need for their retention is reviewed at least annually by the supplying CIS partner, in accordance with the provisions contained in Article 33 of Council Regulation (EC) No 515/97. The EDPS considers that the practice of annual review of whether the information must be withdrawn is a positive practice and encourages CIS partners to comply with this rule. In accordance with Article 33, the supplying CIS partner may, within the review period of one year, decide to retain data until the next review if their retention is still necessary for the purposes for which they were included. In this regard, the EDPS calls upon OLAF to limit the use of this possibility for extending the retention of the information only when there is a real necessity to keep the data.

2.3.6. Transfer of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made *ex* Article 7 within or between Community institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46 or to other types of recipients *ex* Article 9.

According to the Notification for prior checking, OLAF transfers personal information to recipients within OLAF, to recipients subject to Directive 95/46 and to other types of recipients, thus, triggering the application of Article 7, 8 and 9 of Regulation (EC) No 45/2001.

Transfers to OLAF staff competent for the application of Regulation (EC) No 515/97, thus, covered by Article 7.

According to the Notification, OLAF staff with direct access to CIS may transfer CIS data on a case-by-case basis to OLAF Staff competent for the application of Regulation (EC) No 515/97. These are OLAF agents outside the Unit C3 who have some responsibility for the application of the above mentioned regulation.

The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data shall only be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, OLAF must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. In other words, even if the transfer of information is foreseen in relevant legislation, such transfer is only lawful if it meets these two additional requirements.

Whether a given transfer meets such requirements will have to be assessed on a case by case basis. Accordingly, OLAF agents should apply this rule for each particular data transfer. Doing so will avoid unnecessary transfers of information as well as transfers of information to parties that do not have the appropriate competences.

Transfers to competent Member State authorities subject to Directive 95/46/EC ex Article 8 of Regulation (EC) No 45/2001

When uploading information in CIS, the information is immediately available to all other users ("normal users" and "privileged users") designated by each national authority and by the Commission (OLAF), with access to CIS. Although they do not receive any notice that new information has been uploaded, this information would be visible if the user makes a search in the database, for example, to carry out a specific check on individuals involved in a particular type of fraud or modus operandi at issue. Thus, every time that OLAF uploads information in CIS, such information is transferred to Member State authorities, subject to Directive 95/46/EC.

In addition, on a case-by-case basis, such data may also be transferred spontaneously or on request to officials of competent Member State authorities, as foreseen by Regulation (EC) No 515/97. Yet, such transfers must comply with Article 8 Regulation (EC) No 45/2001, which offers several legal grounds authorising the transfer of personal information. Given the circumstances in this case, OLAF may avail itself of Article 8 (a) according to which personal data can be transferred if the data will be used to perform a task in the public interest or subject to public authority. Whereas under Article 8 (a) of Regulation (EC) No 45/2001 it is up to the recipient to establish the interest, the EDPS understands this provision to mean that if the sending of the information is not carried out at the request of the recipient, it is up to the sender to accredit such a need. Accordingly, each time that OLAF decides to upload the information into CIS on its own initiative, OLAF must accredit the necessity of the data transfer. This is an assessment that OLAF agents must carry out seriously each time they transfer information. OLAF agents responsible for CIS should be made aware of this rule.

Compliance with Article 8 (a) 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 data to CIS partners fulfils the conditions of Article 8 (a) insofar as the public authorities to whom the information is sent are the 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, in this case the prevention, investigation and prosecution of operations that are in breach of customs or agricultural legislation.

Transfers to other types of recipients *ex* Article 9 of Regulation (EC) No 45/2001

Article 30.4 of Council Regulation (EC) No 515/97 foresees the possibility for the transfer of CIS data to national authorities of third countries. In transferring CIS data to third countries, OLAF must ensure compliance with Article 9 of (EC) No 45/2001. OLAF's compliance with Article 9 is being dealt with in the context of case 2005-0154 and case 2006-0493, in the framework of which the EDPS analyses the conformity of OLAF international transfers taken as a whole with Regulation (EC) No 45/2001. For this reason, this Opinion will not further analyse the data transfers covered by Article 9 of Regulation (EC) No 45/2001 (i.e. transfers of personal data to recipients other than Community institutions and bodies, which are not subject to Directive 95/46/EC)[10].

2.3.7. Right of access and rectification

The EDPS notes that under Article 36.1 of Council Regulation (EC) No 515/97 individuals whose data are inserted in CIS have the right of access, which is governed by Member States' laws or the data protection rules applicable to the Commission depending on whether such rights have been invoked respectively in Member States or within the EU institutions. Accordingly, access requests addressed to OLAF should be assessed in the light of Regulation (EC) No 45/2001.

The EDPS notes that OLAF has confirmed that it has put a procedure in place to react to access requests from data subjects. According to the privacy statement and prior checking Notification, individuals who want to have access/rectify the information that relates to them which is included in CIS must send a request to the data controller for the Customs Information System. The privacy statement informs that if personal data for which an application for access has been made have been supplied by another Member State, access shall be permitted only if the supplying partner has been given the opportunity to state its position.

EDPS recalls that OLAF may restrict this right if one of the specific conditions justifying a restriction applies. Neither the privacy statement not the prior check notification refers to the possibility to restrict this right. For example, OLAF may be able to rely on Article 20.1 (a) which allows suspension of access for the prevention/detection/prosecution of a criminal offence. Also, if OLAF considers that the suspension of access/rectification is necessary in order to safeguard an economic or financial interest of the Community or of the Member States, OLAF may avail itself of the exception foreseen in Article 20.1.(c) according to which access can be denied where such restriction constitutes a necessary measure to safeguard "*an*

[10] However, as the EDPS said in its Opinion on a Proposal for a Regulation amending Regulation No 515/97, it would have been appropriate for Article 30.4 to be amended to ensure compliance with legislation applicable to the transfer of personal data to third countries. The EDPS hopes that this problem will be fixed as the Proposal is making its way through the legislative process. See EDPS Opinion of 22 February 2007 on the proposal for a Regulation amending Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final).

important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters".[11]

In accordance with the above, if OLAF uses an exception to suspend access, it should take into account that the restrictions to a fundamental right can not be applied systematically. OLAF must assess in each case whether the conditions for the application of one of the exceptions, for example, Article 20.1.a, or 20.1.c or others apply. In addition, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis. For example, if OLAF wishes to rely on the exception of Article 20.1.c it must assess whether it is necessary to suspend access in order to safeguard an important economic interest. In making such an assessment, OLAF must establish a clear link between the need to suspend access and the safeguard of an economic interest. Furthermore, OLAF should also recall that the exceptions to the data protection rights only apply temporarily. Finally, if OLAF uses an exception, it must comply with Article 20.3 according to which "*the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor*". The provision of information can be deferred "*for as long as such information would deprive the restriction imposed by paragraph 1 of its effect*" *ex* Article 20.5. of Regulation (EC) 45/2001.

2.3.8. Information to the data subject

Pursuant to Article 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to. The right of information is in itself essential and also enables individuals to exercise other rights such as the right of access. Obviously if individuals are not aware that their personal information is being processed, they will not be able to exercise other rights such as the right of access and rectification. Article 11 applies when the data has been obtained from the data subject. Article 12 applies when the data has not been obtained from the data subject.

The EDPS notes that most of the data contained in CIS, namely information about individuals who are alleged to be engaged in wrongdoings, are likely to have been collected not directly from the individual. Thus, in most cases, Article 12 will apply. Yet, in some exceptional cases it is possible for the data to be supplied by the suspected individual. Also, data regarding officials with access to CIS is likely to be included by the individuals themselves.

The EDPS considers that the information that OLAF foresees to provide to individuals as described in its privacy statement as being in line with Article 11 and 12 of Regulation (EC)

[11] In his Opinion on the Proposal for a Regulation Council Regulation (EC) No 515/97, the EDPS pointed out that the second paragraph of Article 36.2 of Council Regulation (EC) No 515/97 should have been amended in order to bring it in line with Regulation (EC) No 45/2001. Article 36.2 establishes that "access shall be denied during the period when sighting, reporting operations analysis or investigation is ongoing". The EDPS stated that he favoured an amendment that reads "access may be denied" (as opposed to "access shall be denied"). This is because under Regulation (EC) No 45/2001, as a matter of general principle, individuals are entitled to exercise the right of access to their personal data. However, as outlined above, Article 20 of Regulation (EC) No 45/2001 recognises that such a right can be restricted if one of the specific conditions justifying a restriction applies. In other words, individuals have the right of access in principle, but such access can be restricted. Conversely, the language of Article 36.2 "access shall be denied" gives no room for assessment on whether access can be granted or not.

45/2001. However, the EDPS considers that various aspects of this statement could be improved:

First, the privacy statement contains some references that are likely not to be understood by the addressees of the privacy statement. Notably, the statement contains various references to other Notifications by OLAF data controllers to the OLAF data protection Officer. For example, it refers various times to OLAF DPO 77. It is unlikely that most addressees of the privacy statement will understand what this means and it would therefore cause confusion. Furthermore, we consider that such references are not necessary. Therefore we suggest deleting these references.

Second, the references to the identity of the data controller could be more precise. Indeed, the EDPS considers that an explicit reference to OLAF would be more appropriate and provide more transparency. The reference to Commission services is too general.

Third, the EDPS also considers that the privacy statement should not refer to another privacy statement which may not be available to the addressee, as it is done in the section on technical means (when it refers to the privacy statement related to AFIS infrastructure).

Fourth, as far as the right of access and rectification are concerned, the EDPS would find it more appropriate if the language used in the statement was replaced by a sentence plainly acknowledging that individuals have such rights ("You have the right to access the personal data we hold regarding you and to correct and complete it") as opposed to the current sentence "Upon request, you may be sent a copy of your own personal data to correct or complete" which may be read as somehow limiting the scope of the right of access.

Regarding the moment in time when the information will be provided, the EDPS recalls that *ex* Article 11 of the Regulation 45/2001, individuals should be informed at the time of the recording of the data or, if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed. In the case in point, this means that the information should be provided to the individual when or immediately after the information is uploaded in CIS. When the content of the entry is used in an OLAF investigation/case, or in a mutual assistance exchange, the information will become part of the case file or the mutual assistance communication. Thus, the data subject may be informed in the context of the case or the mutual assistance exchange as established in the prior checks of the various types of OLAF cases and the mutual assistance exchange. As noted above regarding the right of access, the provision of information may be deferred if one of the exceptions to Article 20 applies.

Regarding the manner in which information must be provided, the EDPS considers that the provision of information through the web site as a positive step towards complying with Article 11 and 12 of Regulation (EC) No 45/2001 and 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 investigations may not visit the web site, 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. As described above, such personalised notices should be provided at the time of the recording of the data or in the context of OLAF investigation/cases, when the data becomes part of an investigation/case. This obligation applies to information uploaded by OLAF. For information regarding data subjects which has been uploaded by the Member States, it appears more appropriate and straightforward for them to ensure the provision of information. Indeed in such cases, Member States are in more direct contact with such individuals with whom they are also more likely to share the language. In any event, the

situation where individuals are not informed either because OLAF relies on Member States or vice versa should be avoided. Accordingly, the EDPS calls upon OLAF to request the Member State authorities to make a commitment to notify the data subject in accordance with the requirements of their national data protection legislation.

2.3.9. Security measures

In order to ensure a consistent approach to OLAF security measures, the EDPS has decided to analyse the security measures in a horizontal way, rather than doing it in the context of each particular prior checking notification. Accordingly, this Opinion will not deal with security measures and the analysis will be carried out in a different Opinion which will address security issues only.

3. 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:

- Ensure that OLAF agents and Member States upload personal data in CIS data in accordance with the data quality principle. Towards this end, OLAF should consider issuing guidelines addressed to OLAF agents and Member State authorities with access to CIS describing the application of the quality principle in CIS.
- Ensure that OLAF agents and Member States use the possibility for extending the retention of the information only when there is a real necessity to keep the data. Consider issuing guidance in this regard.
- Ensure on a case by case basis that data transfers under Article 7 only take place if the requirements of Article 7 are met.
- Ensure that data transfers under Article 8 take place only "if necessary" so that unnecessary transfers will not occur. Make sure that OLAF agents apply this rule on a case by case basis. Towards this end, consider issuing guidance in this regard.
- Ensure compliance with Article 9 when CIS data are transferred to third countries that do not provide adequate protection.
- Ensure that individuals are personally informed of their data being uploaded in CIS when such data have been uploaded by OLAF. Do not restrict this right systematically. When data concerning an individual in a Member State is uploaded by OLAF, and used in an OLAF investigation/case or a mutual assistance exchange, the data subject may be informed in the context of the case or the mutual assistance exchange. When data concerning an individual in a third country is uploaded by OLAF, and the entry is eventually used in an OLAF investigation/case or a mutual assistance exchange, the data subject may be informed in the context of the case if this would not involve a disproportionate effort.

- Request the Member State authorities to make a commitment to notify the data subject in accordance with the requirements of their national data protection legislation when they upload data into the CIS.
- Modify the privacy statement to implement the suggestions made in this Opinion.

Done at Brussels, 24 July 2007

Peter HUSTINX
European Data Protection Supervisor