Opinion on notifications for Prior Checking received from the Data Protection Officer of the European Anti-Fraud Office regarding the Virtual Operational Cooperation Unit, the Mutual Assistance Broker, and the Customs Information System

Brussels, 17 October 2011 (Joint cases 2010-0797, 2010-0798, 2010-0799)

1. Proceedings

On 11 October 2010, the European Data Protection Supervisor (**EDPS**) received three notifications for prior checking relating to the processing of personal data regarding the Virtual Operational Cooperation Unit (**V-OCU**), the Mutual Assistance Broker (**MAB**) and the Customs Information System (**CIS**) from the Data Protection Officer (**DPO**) of the European Anti-Fraud Office (**OLAF**).

The notifications were accompanied by the following documents:

- for V-OCU:
  - V-OCU Helpdesk Manual
  - Privacy Statement
  - Sample screens for the different modules (Consur, Marsur, Viasur)
- for MAB:
  - Privacy Statement
  - Annex I to the procedures of MAR-/YAC-INFO
- for CIS:
  - Privacy Statement
- attached to all notifications:
  - AFIS Security Policy Document (AFIS-SEC-POL)

A set of questions were asked by the EDPS and answered by OLAF on 20 October 2010. A second set were sent to OLAF on 26 November 2010, replies to which were received on 26 May 2011. In the meantime, the deadline for the prior check Opinion was suspended.

The replies contained the following additional supporting documents:

- for V-OCU:
  - Operational plan for JCO Sirocco
  - Virtual OCU training Consur
  - OCU Helpdesk manual
  - List of third countries and international organisations
- for CIS:
  - User registration tool user manual
  - CIS and V-OCU quality requirements
- on AFIS Security Policy Document (AFIS-SEC-POL):
  - AFIS Terminal Security Guidelines

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

- AFIS Operations Handling Procedure (Annex 1 of the AFIS Security Policy main document)
- AFIS UNIX Security Baseline
- AFIS Windows Security Baseline

On 10 June 2011, the EDPS called for a meeting with OLAF to discuss the outstanding issues not addressed in their replies. This meeting took place on 1 July 2011. In the meantime, the case was again suspended. Following the meeting, OLAF supplied the EDPS with a copy of the MAB Case User Manual. In view of the complex nature of the cases at hand, on 1 July 2011, the EDPS decided to extend the deadline for submitting his Opinion by two months.

The draft Opinion was sent to the DPO for comments on 27 September 2011. The EDPS received a reply on 10 October 2011.

2. The facts

2.1. General remarks

This prior check Opinion considers the three notifications submitted by the DPO at OLAF, which all refer to cooperation in the field of fighting customs and agricultural fraud. Because these notifications are interrelated, the EDPS decided to address all three of them in one Opinion.

All three applications serve closely related purposes, are governed by the same security policy and are partially integrated with each other, which is why a holistic approach is appropriate. The notifications for V-OCU and MAB are updates of an earlier notification on Mutual Assistance Exchanges, while the notification on CIS updates an earlier notification on the same system. For these earlier notifications, the EDPS issued Opinions on 19 October 2007 and 24 July 2007 (EDPS case file numbers 2007-0202 and 2007-0177), respectively. In this regard, this Opinion also serves as a follow-up to the Opinions referred to above and will pay special attention to new aspects of the processing notified. Common points applicable to all notifications will be addressed first before discussing issues only relevant to individual applications. Where appropriate, reference to the earlier prior check Opinions and the recommendations contained therein will be made.

Description and purpose of processing
While there are differences between the applications, all of them serve the general purpose of enhancing cooperation in customs matters between Member States and the Commission, aiming to prevent, investigate and prosecute violations of customs or agricultural legislation. The applications allow the sharing of information between the Member States -both in structured and unstructured (i.e. free text) form- relating to persons who are or are suspected of being involved in such violations as well as to the officials investigating these cases. They are all accessed via the AFIS Portal, a browser application which provides a unified interface to a number of databases and applications. Under certain circumstances, the authority which entered data into the system may also authorise transfers to third countries.

Each of the systems consists of a central database which can be accessed by the Commission, a number of competent authorities in Member States and in some cases certain third countries, international organisations and Europol and Eurojust. Access for third countries and

international organisations[1] is governed by mutual assistance agreements containing clauses to that effect.[2] Europol and Eurojust may be granted access within the remit of their competences, but cannot upload data. V-OCU differs from the other systems in that access is only given for a limited time to authorities in the countries involved in a specific Joint Customs Operation (JCO) as specified in the respective JCO Operational Plan. The processing is, on the whole, carried out automatically. However, the decision to include or exclude data is a manual process. A more detailed description follows in the subsections on the different systems.

Legal bases
All three applications have their legal base at least partly in Regulation (EC) 515/97,[3] most recently amended by Regulation (EC) 766/2008.[4] CIS is governed by specific rules under title V (Articles 23 to 41) of the said Regulation, while the role of the Commission (in this case, OLAF) in MAB and V-OCU relies on title III (Articles 17 and 18). The applications may involve transfers of personal data outside of the EU as set out in title IV (Articles 19 to 22) of Regulation 515/97. The former third pillar part of CIS is governed by Council Decision 2009/917/JHA[5] since its entry into force on 27 May 2011. OLAF itself was established by Regulation (EC) 1073/99.[6]

Controllership & responsibilities
The three applications notified are all managed by OLAF; according to the notifications, an official in unit C.3 (Mutual Assistance & Intelligence) at OLAF is the delegated data controller. The applications use servers located on OLAF premises and managed by OLAF.

Data is added, amended and used by authorities in the Member States (and, in some cases, third countries). Only the authority which has added data can amend it. These authorities act as co-controllers. This issue will be elaborated in section 3.4.

Users and user management
Users of all three applications are managed using a unified tool, the User Registration Tool (URT). A copy of the user manual for this tool has been supplied to the EDPS. There are several categories of users with different privileges. These roles are: normal user, liaison officer, legal authoriser, IT helpdesk. Normal users can either take the form of institutional or personal accounts. These users are managed and created by the national liaison officer. This officer can create requests for new users and organisations and manage their privileges. Requests that imply legal authorisation are checked and validated by the legal authoriser -an official at OLAF- and implemented by the IT helpdesk, also a member of OLAF staff. Requests that do not need legal authorisation are directly implemented by the helpdesk on request of the liaison officer.

Categories of data and data subjects
According to the notifications, all three systems process personal data relating to two different categories of data subjects:

[1] According to information obtained from OLAF, the World Customs Organization (WCO) can receive depersonalised data from MAB on Marinfo, Ciginfo and Yachtinfo cases (p. 23, 28 of MAB case user manual); parts of the information in MAB are available to MarInfo members, not all of which are EU Member States. Interpol participated as observer in at least one JCO (p. 13 in annex 2 to Q12).
[2] See the list available at http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html.
[3] OJ L 82, 22.03.1997, p. 1
[4] OJ L 218, 13.08.2008, p. 48
[5] OJ L 323, 10.12.2009, p. 20
[6] OJ L 136, 31.05.1999, p. 1

Category I: Persons mentioned in cases about which information is held or exchanged.

This refers to persons mentioned in the messages transferred between OLAF and Member States or third countries in the framework of the notified applications, as well as those persons about whom information is held. In particular, this relates to persons who are -or appear to be- involved in operations detected or planned that are in breach of customs and agricultural legislation.

Category II: The officials working on these cases.

In the case of V-OCU and MAB these can be Member State and third country officials working on the cases, while for CIS only Member State officials are mentioned. For V-OCU and MAB, officials in certain international organisations can gain access; however, their staff is not mentioned under this category in the notifications.

In the first category, the amount of information processed differs between the notified systems, but contains at least names, addresses, date and place of birth, as well as information on ID documents. Exhaustive lists are included in the subsections on the different systems below. In some cases, these also contain free text fields or fields referring to physical characteristics, which could theoretically contain information permitting inferences about racial, ethnic or religious origins, health information or other special kinds of data. The handbooks for all systems inform users about the special protection accorded to this kind of data and tell them that such data should not be stored in the systems.

As regards the second category of data subjects -officials working on the cases in question- all three systems use the same list of data fields:

1) surname, name
2) service
3) telephone, mobile phone, fax, email address[7].

Information and rights of data subjects

Category I data subjects are informed about the possible collection of data on them via privacy notices which will be posted on a publicly available part of OLAF's website and the AFIS portal.

The privacy notices for the three systems are largely similar. They inform possible data subjects about the purposes and legal bases of processing, as well as to whom data can be disclosed and retention periods. The notices for V-OCU and MAB mention that under certain conditions data can be sent to third countries and international organisations as well. Only the notice for CIS contains a list of the data fields that may be processed. The rights to access, rectification, and deletion as mentioned in the notices are the same for the three applications: persons may request a copy of data stored about them by contacting the data controller whose name and contact details are provided and may request that inaccurate information be rectified.

Data subjects are informed that restrictions as set out in Article 20 of Regulation (EC) 45/2001 may apply. The notices for V-OCU and MAB additionally mention that if the data in question have been supplied by a Member State, that Member State shall have the opportunity to assert its position on the request before access is granted. These two notices also mention that if information is used in large inter-institutional transfers for the purpose of detecting trends and unusual activity, no individual notice of its use will be provided.

[7] The notification on CIS labels this point "contact data" instead. The content can reasonably assumed to be identical.

The time limit for blocking/erasing data upon a justified request is one month for all three data bases. Data subjects are informed of their right to recourse to the EDPS in all three privacy notices.

OLAF has procedures in place to provide personalised information going beyond what is mentioned in the privacy notices to data subjects.[8] Such information will only be provided with prior consent from the data controller of the operational partner which included the data in the respective system. Additionally, exemptions under Article 20 of Regulation (EC) 45/2001 may apply. The Guidelines in place draw attention to the fact that these exemptions can only be applied on a case by case basis.

For category II data subjects, OLAF asks the respective authorities in the Member States to provide appropriate information to them. The category II data subjects who are OLAF staff also have access to the "Guidelines for OLAF staff regarding practical implementation of data protection requirements", adopted by the Director General of OLAF in October 2010.

Retention of data
OLAF applies the same basic procedures for retention of data to all three systems. According to the information provided in the notifications, personal data in the systems can be retained for a maximum period of ten years. The EDPS had already requested OLAF to give reasons for this retention period in his Opinion of 19 October 2007, which addressed the predecessor systems to V-OCU and MAB and again in a set of questions raised on 26 November 2010.

In its replies, OLAF pointed out that cases have to be reviewed on an annual basis to establish whether there is a need for continued storage. After 11 months, users are informed that data is up for review. In the absence of a positive decision to keep the data within the review period (one month), it is deleted. According to OLAF, positive decisions can only be made for CIS cases. OLAF also informed the EDPS that it did not issue additional guidance for the officers making this decision.

The access logs to systems accessible via the AFIS Portal are stored for 15 years. There is a procedure in place for granting access to these logs to the competent authorities in the Member States for audit purposes. The DPO of Eurojust has introduced a request to receive a monthly extract of the AFIS logs, which has been granted. A procedure will be implemented and notified to the EDPS. The EDPS has been informed by OLAF that the DPO of Europol has launched a similar request.

Security aspects

[...]

These are the key points all three applications have in common. A more detailed description of the properties of each of the systems follows in the specific remarks.

[8] Guidelines for OLAF staff regarding practical implementation of data protection requirements, October 2010, Title 1.5. Annex 5 to OLAF Manual, publicly available at http://ec.europa.eu/dgs/olaf/legal/manual/annexes/Guidelines-October2010.pdf .

2.2. Specific Remarks

2.2.1. V-OCU

V-OCU is a tool to exchange information on unconfirmed suspicions and request actions from other competent authorities. An earlier version of V-OCU had been notified to the EDPS before, which led to the issuing of an Opinion on 19 October 2007 (case number 2007-0202) with a number of recommendations.

Description of processing
V-OCU is a browser application accessible through the AFIS Portal to collect and check information on movements and checks of goods and persons for Member States, as well as for third states and international organisations with whom the EU has entered into mutual assistance agreements containing clauses to this effect. This information relates to unconfirmed suspicions, which can be entered by officials in Member States and those third countries or international organisations that are part of a specific joint customs operations (JCO) and other similar short-term operations. JCOs are coordinated operations carried out by authorities in Member States and possibly third countries. Each JCO has separate access to data in V-OCU only granted to the specific countries involved in the JCO at hand. By way of example, the EDPS has been supplied with a copy of the draft operational plan for a past JCO.

The processing of data is initiated by the entering of data (movement records) into the system by the competent authorities of Member States and other authorities with access to V-OCU. These movement records contain information on suspicious movements (based on a number of indicators, such as known consignors/consignees, inconsistent documentation etc.) of goods and may also include personal data, e.g. of lorry drivers. These entries can also request specific actions to be taken, e.g. checks and x-rays of shipments. Other parties may issue free text comments on records, such as "This person is known in connection with counterfeiting brand goods" or the results of checks. This data is stored in a central database[9] and accessible to other parties in a limited timeframe during the life cycle of concrete JCOs. This life cycle is usually separated into three phases: pre-operational (selection of targets for special watch), operational (carrying out of checks) and post-operational (follow-up).

Depending on the kind of entry at hand, the screens -called modules- take different forms, detailing information on the shipment or sighting at hand and the comments made by other parties. The different modules are the following:

- **Viasur** concerns the collection of intelligence on road traffic;
- **Consur** does the same for containerised maritime traffic;
- **Marsur** serves the same purpose related to non-commercial maritime traffic.

OLAF has provided the EDPS with screenshots of these modules. Exchanges of information occur as structured messages in the mailing application of the AFIS system, i.e. MAB-mail (see section 2.2.2 on MAB below). Additionally, V-OCU contains a messaging application to exchange free-text messages between participants.

Legal basis
The notification only contains a general reference to Regulation (EC) 515/97 as the legal basis. In more detail, the Commission's involvement is based on Title III of this Regulation

[9] This is the main difference to the so-called traditional exchange formats, in which there was no central storage of data.

(Articles 17 and 18). Access for third countries is governed by Title IV of said Regulation and the mutual assistance agreements in place. V-OCU aims to facilitate "special watch" requests under Article 7 of Regulation (EC) 515/97.

Categories of data
The specific list of personal data on category one data subjects (see 2.1 general remarks, above,) to be stored in V-OCU contains the following items:

1) surname, first name
2) place and date of birth
3) nationality
4) ID document
5) case involvement data (free text)

OLAF confirmed that data on family members of suspects will only be included in the free text field on case involvement data if they are relevant to the case at hand; maiden names of women may be included for the same reason. This had been requested in the recommendations in the earlier prior check. Users of V-OCU are informed of the applicable data quality principles, both in writing and in training sessions (e-learning or hands-on) prior to the start of a JCO.

Recipients of data
As regards possible recipients, the notification mentions designated officials of the competent authorities in the Commission and the Member States responsible for the applying of Regulation (EC) 515/97. The privacy notice refers to designated officials in the *"competent administrative, legislative, and judicial authorities in Member States, EU institutions, bodies, offices and agencies, international organisations and/or to administrative authorities in third countries*". Both the notification and the privacy statement also mention that data may be transmitted to authorities in third countries if there are mutual assistance agreements in place between the Union and these third countries.[10] International organisations as recipients are mentioned in the processing description of the notification, but not in the field on recipients. The technical aspects of user management have been described in the general section above.

According to the privacy notice attached to the notification, "*information is analysed using IT tools and may be used by OLAF for intelligence purposes (see notifications DPO-88: Information and intelligence data pool, and DPO-89: Intelligence databases)"*. These notifications led to the issuing of a joint prior check Opinion on 21 November 2007.

Data subject rights
An account of data subject rights can be found in the discussion of the privacy policies in the general remarks. In its replies submitted on 26 May 2011, OLAF highlighted that access requests would likely be declined through the duration of the JCO (usually 10-14 days).

2.2.2. MAB

MAB is a case management system for the exchange of information on a variety of customs-related databases. An earlier version of MAB has been notified to the EDPS before. A prior check Opinion for this system was published on 19 October 2007 (case number 2007-0202) and included a number of suggestions OLAF should implement to be in compliance with Regulation (EC) 45/2001.

[10] See http://ec.europa.eu/dgs/olaf/assist_3rd/index_en.html.

Legal basis
The legal basis for the Commission's involvement is the same as for V-OCU, Title III of Regulation 515/97/EC.

Description of processing
MAB provides a common interface for five information exchange systems. These are Yachtinfo, Marinfo, Ciginfo, MAB mail and CIS.

- **Yachtinfo** relates to information and confirmed seizures on non-commercial vessels. [...].
- **Marinfo** relates to information on and confirmed seizures in containerised maritime traffic. [...].
- **Ciginfo** relates to information on and confirmed seizures of cigarettes and tobacco goods as well as counterfeit goods.
- **CIS** helps participating customs authorities to cooperate with each other by allowing information exchange on (suspected) breaches of customs and agricultural legislation. It will be described in further detail below, as it is the subject of one of the three notifications on its own.
- **MAB Mail** allows the sending of unstructured messages (free text) to other participants in the system. It is the same system as the previous AFIS Mail. As mentioned above, it is also used to exchange messages in the context of V-OCU.

The first four subsystems are used to create cases and exchange structured information;[11] the last one allows the exchange of free text messages between participants.

When creating a case, officers can select multiple case types; for example, a Marinfo case combined with a Ciginfo one. Data entered at the case creation stage will then automatically be introduced into all cases, in so far as they share data fields.[12] Once they are created, however, the cases become independent of each other, with no transfer of data occurring between them. The data is held centrally by OLAF.

Categories of data
The data fields which can be included in the structured part (the first three subsystems mentioned above, CIS will be discussed in point 2.2.3) of MAB are the following:

1) surname, first name, maiden name, alias, gender
2) physical characteristics
3) place and date of birth
4) nationality
5) profession
6) a warning indicating any history of being armed, violent, drug addict, suicidal and other warnings (to be selected from a list as well as free text)
7) ID document (type, number, date and place of issue)
8) address (PO box, Street, House No, Box, Postal code, City, Country)
9) involvement description (to be selected from list, as well as free text, including an evaluation of the quality of the information)
10) suggested action.

[11] These exchanges take place as structured messages in the AFIS mailing application (i.e. MAB Mail).
[12] For example, cigarettes smuggled in a container on a commercial vessel could be entered into CIS, MarInfo and CigInfo; however, the bill of lading would only be included in MarInfo.

The field for warnings can include information on drug habits and suicidal tendencies which were not included in the previous notification of mutual assistance exchanges (EDPS case file number 2007-0202). The field on physical characteristics could in principle also include data allowing inferences to racial, ethnic, or religious origins or health.

MAB Mail in turn is a message application that allows its users to exchange unstructured (i.e. free text) messages. In training sessions prior to being granted access, users are instructed not to enter sensitive data in those free text messages and the other fields.

Recipients of data
Regarding possible recipients, the notification mentions designated officials of the competent authorities in the Commission and the Member States responsible for the application of Regulation (EC) 515/97. The privacy notice refers to designated officials in the "*competent administrative, legislative and judicial authorities in Member States, EU institutions, bodies, offices and agencies, international organisations and/or to administrative authorities in third countries*". Additionally, information may be exchanged with the members of the MarInfo and YachtInfo groups, not all of whom are EU Member States. Data may also be transmitted to authorities in other third countries if there are mutual assistance agreements in place between the Union and these third countries. Information from Yachtinfo, MarInfo and CigInfo cases may also be forwarded to the World Customs Organisation (WCO); in this case, only a depersonalised subset of the information[13] is sent. However, there is no mention of international organisations as recipients of personal data in the notification.

According to the privacy notice included in the notification, data may be used for intelligence purposes. The EDPS published a joint prior check Opinion on two notifications on processing for intelligence purposes ("*Information and intelligence data poo*l" and "*Intelligence databases*") on 21 November 2007 (EDSP case file numbers 2007-0027 and 2007-0028).

Data subject rights[14]
It is noteworthy that the privacy notice for MAB does not contain a list of data items to be stored. As concerns the use of the CIS in the scope of MAB, the privacy notice refers to the CIS as notified in DPO-17, i.e. the old version of the notification, and not the updated version DPO-17-2 which is the object of this prior check.

2.2.3. CIS

An earlier version of this system has already been the subject of a prior checking Opinion issued on 24 July 2007 (EDPS case file number 2007-0177). However, as its legal basis has been amended by Regulation (EC) 766/2008 in the meantime, and the processing of personal data within the system has changed, a new prior check Opinion is appropriate.

Description of processing
The purpose of CIS is to assist competent national authorities and the Commission ("CIS partners") in preventing, investigating, and prosecuting operations that are in breach of customs and agricultural provisions. To this end, it allows CIS partners to put up alerts in the system requesting other CIS partners to take certain actions. More specifically, these are: sighting and reporting, discreet surveillance, specific checks and operational analysis. These alerts can relate to commodities, means of transport, businesses and persons. For the users,

[13] See MAB Case User Manual p. 23.
[14] See discussion of privacy notices in the general remarks.

there is no visible difference between CIS as established under Regulation (EC) 515/97 and Council Decision 2009/917/JHA.

Legal basis
CIS is based on Title V of Regulation (EC) 515/97 and the CIS Council Decision (2008/917/JHA) which, as of 27 May 2011, replaced the CIS Convention. Article 23(2) of Regulation 515/97 defines its purposes as assisting in "*preventing, investigating and prosecuting operations which are in breach of customs or agricultural legislation by making information available more rapidly and thereby increasing the effectiveness of the cooperation and control procedures of the competent authorities referred to in this Regulation*". Article 25(2) sets out an exhaustive list of data categories that may be included which is identical to the one implemented in the database as listed below. The relationships with third countries are governed by title IV (articles 19 to 22) of the same regulation. The CIS Council Decision contains provisions to the same effect.

Formally speaking, there are two separate parts of CIS: one established under Regulation 515/97 ("CIS EU") and one established under Council Decision 2009/917/JHA ("CIS MS"). The difference between them lies in the types of goods they relate to: CIS under the Council Decision refers to drugs, weapons and some other categories such as laundered money and stolen cars, while all other categories are dealt with by CIS as established under Regulation 515/97. The earlier EDPS prior check Opinion referenced above only addressed CIS as established under Regulation 515/97.

Data categories
Data can be entered by the designated authorities in Member States. The distinction in the legal basis is reflected in the two different case types "CIS EU" and "CIS MS", based on the commodity in the case in question. For cases dealing with commodities, means of transport, businesses and persons, the following data fields can be included:

1) name, maiden name, forenames, former surnames and aliases;
2) date and place of birth;
3) nationality;
4) sex;
5) number and place and date of issue of the identity papers (passports, identity cards, driving licences);
6) address;
7) particular objective and permanent physical characteristics;
8) a warning code indicating any history of being armed or violent or of having escaped;
9) reason for inclusion of data;
10) suggested action;
11) registration number of the means of transport.

For cases dealing with detained, seized, or confiscated cash and goods, only items 1 to 4 and 6 of the list above will be included. Finally, for cases dealing with the availability of expertise, only surnames and first names of the experts will be stored.

When a requested action has been taken, the CIS partner that carried out the check or other requested action can transmit this information to the requesting CIS partner.

Users and user management
As mentioned in the general part above, user management is handled via URT. In the case of CIS, there is an additional obligation under Article 29(2) of Regulation 515/97 to publish the list of authorities having access in the Official Journal of the European Union (OJ). OLAF informed the EDPS that a review of the list is underway. This list is independent from the one established via URT; for the future, OLAF has announced that it will update and publish this list on a regular basis.

Recipients of data and data transfers
According to the notification, access is restricted to officials in the European Commission and the Member States responsible for the application of Regulation (EC) 515/97. Among these, direct access is only available for those with a user ID and a password. With prior approval of and subject to the conditions imposed by the CIS partner who uploaded the data, information may also be transferred to other authorities in Member States. OLAF does not upload own data to the system and is therefore not in a position to authorise such transfers. While both the notification and the privacy notice mention that transfers of personal data stored in CIS to third countries are possible, OLAF maintained in its replies submitted to the EDPS on 26 May 2011 that it does not transfer data to third countries, or to other EU institutions, bodies or agencies, nor to Member States; as mentioned, transfers to third countries may occur upon authorisation by the Member State which uploaded the data.

Data subject rights[15]
Contrary to the MAB notice, this notice contains a list of data categories. Compared to the list in the notification it does not mention information on identity documents and addresses.

3. Legal analysis

3.1. General remarks

Those parts of the following analysis which apply equally to all three notifications will be addressed jointly. Notably, this concerns the applicability of Regulation 45/2001[16] ("the Regulation"), the issue of controllership, rights of access and rectification, as well as the security measures. Where the notifications differ from each other, they will each be addressed in turn.

3.2. Prior checking

3.2.1. Applicability of the Regulation

Article 3(1) of the Regulation lays down that it "*shall apply to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*". Article 2 (a) of the Regulation defines personal data as "*any information relating to an identified or identifiable natural person*". Article 3(2) of the Regulation establishes that it shall apply "*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 or are intended to form part of a filing system*".

[15] See the discussion in the part "general remarks".
[16] OJ L 8, 18.12.2000, p. 1

The processing of data in the three applications constitutes a processing of personal data. The data processing is performed by an EU body in the exercise of activities which fall within the scope of EU law (Article 3(1) of the Regulation, in the light of the Lisbon Treaty). The processing of the data is done at least partly through automatic means. This applies to all three notified systems. Therefore, the Regulation is applicable.

3.2.2. Grounds for prior checking

Article 27(1) of the Regulation subjects all "*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*" to prior checking by the EDPS. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes -among others- processing "*related to [...] suspected offences, offences, criminal convictions or security measures*" (Article 27(2) a). Such data may be processed in the course of all three notified applications. As OLAF indicated in the notifications, these processing operations also serve to "*evaluate personal aspects relating to the data subject*" (Article 27(2) b)). Case involvement data serves to evaluate the conduct of data subjects as to the breach of customs and agricultural legislation. The applications are thus subject to prior checking by the EDPS.

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

3.2.3. Procedure

The notification of the DPO was received on 11 October 2010. According to Article 27(4) of the Regulation, the present Opinion must be delivered within a period of two months. In total, the period for delivery was suspended for 215 days while waiting for replies to requests for further information, a meeting and comments on the final draft Opinion. Due to the complexity of the cases, the deadline was extended by two months. Additionally, the cases were suspended during August 2011. Taking these suspensions and the extension into account, the opinion should be delivered by 15 October 2011; taking into account that this date falls on a Saturday, the EDPS delivers his Opinion by 17 October 2011.

3.3. Lawfulness of the processing

Personal data may only be processed if grounds can be found in Article 5 of the Regulation. In the cases at hand, Article 5(a) is applicable. It declares lawful processing that 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* [...]". This provision contains three elements, all of which must be fulfilled: 1) the processing must be based on a legal instrument (either the Treaties or another act), 2) it must be in the public interest and 3) it must be necessary for achieving this public interest.

All three instruments are at least partly based on Regulation (EC) 515/97. V-OCU and MAB rely entirely on it, while CIS also has its own provisions in this Regulation, as well as in Council Decision 2009/917. The legal bases of V-OCU and MAB will thus be discussed together.

3.3.1. V-OCU and MAB

These two instruments have their legal basis in Regulation (EC) 515/97. Articles 17 and 18 of this Regulation form the base for the Commission's involvement in these exchanges and establish that the competent authorities in the Member States shall communicate relevant information to the Commission.

According to Article 17, the competent authorities in the Member States shall communicate to the Commission any information they consider relevant concerning goods that have been or are suspected to have been the object of breaches of customs or agricultural legislation, requests for assistance, actions taken and information exchanged in the application of Articles 4 to 16 (spontaneous assistance and assistance on request) of Regulation 515/97.[17] The Commission in turn shall communicate any information that could help the competent authorities in the Member States to enforce customs and agricultural to them as soon as it becomes available.[18]

Article 18(1) obliges the Member States to inform the Commission of actions that constitute or appear to be breaches of customs and agricultural legislation, and obliges the Commission to convey this information to all the Member States.[19]

Article 7 of Regulation 515/97 establishes that upon request, competent authorities in the Member States shall "*keep a special watch*" on movements of persons and means of transport if there are reasonable grounds for believing that they are involved in operation in violation of customs or agricultural legislation.[20] V-OCU serves the purpose of implementing this Article.

Relations with third countries are governed by Article 19 of this Regulation and the mutual assistance agreements in place between the Union and third countries. Possible transfers to third countries occur directly between the Member States who included personal data and third countries; OLAF is not involved in them.

3.3.2. CIS

CIS differs from the other processing operations notified in that it has its own explicit legal basis in Regulation (EC) 515/97. Its aim is stated in Article 23(2), which reads as follows:

---

[17] Article 17(1) of Regulation 515/97: "*The competent authorities of each Member State shall communicate to the Commission as soon as it is available to them:*
(a) any information they consider relevant concerning:
— goods which have been or are suspected of having been the object of breaches of customs or agricultural legislation, [...]
— requests for assistance, action taken and information exchanged in application of Articles 4 to 16 which are capable of revealing fraudulent tendencies in the field of customs and agriculture; [...]".

[18] Article 17(2) of Regulation 515/97: "*The Commission shall communicate to the competent authorities in each Member State, as soon as it becomes available, any information that would help them to enforce customs or agricultural legislation.*".

[19] Article 18 (1) of Regulation 515/97: "*Where a Member State's competent authorities become aware of operations which constitute, or appear to constitute, breaches of customs or agricultural legislation that are of particular relevance at Community level, and especially: — when they have, or might have, ramifications in other Member States or in third countries, or — where it appears likely to the above authorities that similar operations have also been carried out in other Member States, they shall communicate to the Commission as soon as possible* [...]*, any relevant information [...].The Commission shall convey this information to the competent authorities of the other Member States.*".

[20] "*Special watch*" may also be requested for movements of goods and storage places; in these cases, it suffices if they are "*indicated as being the object of potential breaches*", or if they are used to "*store* [goods*] in a way that gives grounds to suspect*" they might be used to supply such operations.

> "The aim of the CIS, in accordance with the provisions of this Regulation, shall be to assist in preventing, investigating and prosecuting operations which are in breach of customs or agricultural legislation by making information available more rapidly and thereby increasing the effectiveness of the cooperation and control procedures of the competent authorities referred to in this Regulation.".

Article 24 establishes that in order to attain this end, CIS "*shall comprise exclusively data necessary to fulfil its aim as stated in Article 23(2), including personal data*" in a number of categories, which are exhaustively listed in Article 25.

The second part of its legal basis is provided by Council Decision 2009/917/JHA, Article 1(2) of which reads as follows:

> "The aim of the Customs Information System, in accordance with this Decision, shall be to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly, thereby increasing the effectiveness of the cooperation and control procedures of the customs administrations of the Member States.".

Article 4(2) of this Decision provides an exhaustive list of categories personal data which may be included in CIS.

3.3.3. Public interest and necessity

In order to be lawful under Article 5(a) of the Regulation, the processing must also contribute to the public interest. The aim of the three applications that have been notified to the EDPS is to enhance cooperation between the Commission, Member State authorities and in some instances third country authorities in preventing, investigating and prosecuting violations of customs and agricultural legislation. Ensuring the efficient application of customs and agricultural legislation safeguards the financial interests of the Commission and the Member States and is also in the public interest. The processing operations should be regarded, therefore, to be in pursuit of the public interest.

In abstracto, such exchanges can help to protect the financial interests of the Commission and the Member States. Without them, the enforcement of agricultural and customs legislation would be seriously hampered. Implementing "*Special watch*" requests would on a bilateral basis would likely be ineffective for movements crossing several countries. In this sense, V-OCU, MAB and CIS can be regarded as necessary instruments for fighting fraud. Whether the inclusion of data in them is necessary in a given case cannot be evaluated on an abstract level. Here, necessity has to be proved *in concreto* on a case-to-case basis for each and every case.

3.4. Controllership

Article 2 (d) of the Regulation defines "*controller*" as the "*Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data*." The assessment of who is the controller shall be based on who actually does this.

The notification only referred to an official at OLAF as the person responsible for the processing. From the description of the processing operations it is clear, however, that the

competent authorities in the Member States should also be considered controllers besides OLAF.

The setup of the systems implies that some of the tasks of a controller cannot be fulfilled by OLAF but only by the competent authorities in the Member States. For example, Article 4 (2) of the Regulation obliges the controller to ensure that the principle of data quality is respected. OLAF can contribute to this by setting up the system in a way that no clearly irrelevant data may be processed and by providing information on its proper use, but the actual uploading and amending of data, the decision on whether or not to extend storage for CIS cases[21], as well as the assessment *in concreto* which data should be uploaded is done by the competent authorities in the Member States. Similarly, as they are the only ones capable of changing data uploaded by them, the right to rectification which according to Article 14 is incumbent on the controller needs to be ensured by them. They, and not OLAF, are the ones authorising transfers to third countries where possible.[22] This shows that they cannot be regarded as mere users of the system, as their decisions have significant impact on the purposes of processing.

For CIS, this approach is also confirmed by Article 34(3) of Regulation (EC) 515/97, which establishes that the Member States and the Commission "*shall regard the CIS as a personal data-processing system which is subject to national provisions implementing Directive 95/46/EC, Regulation (EC) 45/2001, and any more stringent provisions of this Regulation*". If OLAF was the only controller, the reference to the national provisions implementing Directive 95/46/EC would be superfluous. Accordingly, Regulation (EC) 515/97 refers to the competent authorities and the Commission as the "CIS partners".

In this regard, V-OCU, MAB and CIS mirror other large-scale IT systems such as Eurodac or the Internal Market Information System in which the Commission is responsible for the setting up and the operational management, but not for the actual content of the data uploaded to the system. OLAF is the party setting up the system, giving concrete form to the authorisation in the legal basis. In this sense, it (partly) determines the means and purposes of processing. The competent authorities in turn are more than just users of the system and partly determine the purpose of the processing. It is thus appropriate to consider the competent authorities connected to the systems and OLAF as joint controllers of the systems. This has implications for liability as well, with each controller being responsible for its own processing operations. OLAF is responsible for the management of the central system, including its security. The competent authorities in the Member States are responsible for the uploading and amending of data and their own use of the systems.

3.5. Processing of special categories of data

According to Article 10(1) of the Regulation, the processing of personal data revealing racial or ethnic origin, political Opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life is generally prohibited, subject to certain exemptions, established in paragraphs 2 to 5 of the same Article. Article 10(2) sets out exemptions related to all special categories; Article 10(3) creates an exemption for the processing of health data by healthcare professionals - or other persons subject to an equivalent obligation of secrecy - for medical reasons; Article 10(4) allows for additional exemptions to be laid down in the Treaties or in legal instruments based thereon in case of a "*substantial public interest*" or by decision of the EDPS, all subject to the provision of

[21] See section 3.7.1 below.
[22] See section 3.8.3 below.

adequate safeguards. According to article 10(5), processing of data relating to offences, criminal convictions or security measures can only be carried out on a specific legal basis or if approved by the EDPS.

All three notified processing operations involve special categories of data; the categories concerned and the precise extent of this processing differ between the applications. They will each be discussed in turn.

3.5.1. V-OCU

V-OCU can be used to exchange information on suspected breaches of agricultural and customs legislation, i.e. data relating to (suspected) offences. The processing of such special data by OLAF is authorised by Article 1(2) of Regulation (EC) 1073/99 and the respective provisions in Regulation (EC) 515/97 and the conditions of Article 10(5) are therefore met.

3.5.2. MAB

Several special categories of data may be processed in the context of MAB. According to the information obtained from OLAF, the field for warnings can now include information on drug habits and suicidal tendencies, which relate to health data. These have not been included in the previous notification of mutual assistance exchanges (EDPS case file number 2007-0202). The MAB Case User Manual shows that, in addition to these warnings offered in a 'pick-list selection', there is a free text field for additional warnings. Furthermore, the field on physical characteristics could in principle also include data revealing the racial, ethnic, or religious origin or health data. Finally, the field on case involvement data is likely to include information on suspected offences.

Given the information received, there is no reason to believe that any of the exemptions under Article 10 of the Regulation apply to the new warnings available in the 'pick list selection'. The exemptions provided for in Article 10(2) of the Regulation do not seem to be applicable. Neither could they be subsumed under the exemption under Article 10(3). This exemption allows the processing of health data by health care professionals or other persons subject to an equivalent obligation of secrecy for medical care and treatment and certain other medicinal uses. Even if the secrecy obligations of OLAF and Member State officials were deemed equivalent to those in the medical profession, this would not entail the applicability of this exemption to processing by OLAF, as its officials would in no way be involved in providing this care. Article 10 (4) allows additional exemptions to be laid down in the Treaties, in acts adopted based on them or by decision of the EDPS if there is a substantial public interest and appropriate safeguards are provided for. Unlike the warnings on a person being violent, armed or escaping, the new warning fields are not mentioned in the legal basis. Therefore, the additional exemption for processing foreseen in the Treaties or legal instruments based on them under Article 10(4) of the Regulation does not apply either. According to the MAB Case User Manual, there is also a free text field for other warnings, which could possibly include special categories of data as well.

As regards the field on physical characteristics, users of this system receive training informing them that data permitting inferences to racial or ethnic background or other special categories of data should not be entered into it.[23] Documentation with this information is also available to users of the notified system. This helps to ensure that no data falling under Article 10(1) are processed. However, given the wide range of data fields which may be entered in MAB (see

[23] See also Guidelines for OLAF staff regarding practical implementation of data protection requirements, p. 8-9.

2.2.2 above), it is not clear whether this additional data field is necessary for the identification of persons. Taking into account the risks associated with the field (i.e. misinterpretation of what constitutes data relating to health or simple disobedience of the instructions received), the EDPS recommends OLAF to evaluate whether this field is necessary. To this end, OLAF should collect statistics on the use of this field and inform the EDPS of the outcome within 6 months.

As regards case involvement data, the processing of such special data by OLAF is authorised by Article 1(2) of Regulation (EC) 1073/99 and the respective provisions in Regulation (EC) 515/97, which satisfy the conditions set out in Article 10(5) of the Regulation.

OLAF should consider removing the fields "drug addict" and "suicidal tendencies" from the list of warnings. It should also provide reasons for the inclusion of the free text field for warnings and consider removing it, should the predefined warnings be judged sufficient.

3.5.3. CIS

The list of data which can be included in CIS, set out in Article 25(2) of Regulation 515/97, includes as item (g) "*particular objective and permanent physical characteristics*". Paragraph 5 of the same Article clarifies that "[...] *no personal data revealing racial or ethnic origin, political Opinions, religious or philosophical beliefs, trade union membership and data concerning the health or sex life of an individual shall be included*." OLAF explained that before being granted access to the system, users are reminded of these restrictions in training sessions. These restrictions are also reiterated in documentation accessible to users. This helps to ensure that no data falling under Article 10(1) of the Regulation are processed in this field. However, given the wide range of data fields which may be entered in CIS (see 2.2.3 above), it is not clear whether this additional data field is necessary for the identification of data subjects. Taking into account the risks associated with the field (i.e. misinterpretation of what constitutes data relating to health or simple disobedience of the instructions received), the EDPS recommends OLAF to evaluate whether this field is necessary. To this end, OLAF should collect statistics on the use of this field and inform the EDPS of the outcome within 6 months.

Item (i) of the list in Article 25(2) is "*reason for inclusion of data*". This provision provides an explicit legal basis for the processing of data related to suspected offences, making the exception under Article 10(5) of the Regulation applicable.

Article 4(2), indents (g) and (h) and 4(5) of Council Decision 2009/917/JHA contain provisions to the same effect, providing a legal basis for the processing of data relating to suspected offences in the part of CIS established under this Decision.

3.6. Data Quality

Article 4(1) of the Regulation contains the principle of data quality. In more detail, Article 4(1) (c) establishes that data must be "*adequate, relevant and non excessive in relation to the purposes for which they were collected and/or further processed*". Additionally, data must - where necessary- be kept up to date (Article 4(1) (d)).

3.6.1. V-OCU and MAB

The principle of data quality is respected in V-OCU and MAB in that (i) the list of data categories seems to be adequate for achieving the respective purposes, (ii) OLAF's internal Guidelines stipulate that details of individuals shall only be entered if they are "*are suspected of being concerned by the irregularity or fraud*" (Guidelines for OLAF staff regarding practical implementation of data protection requirements, p. 7) and (iii) the same guidelines also require OLAF staff to take "*every reasonable step* [...] *to ensure that the information coming from national authorities and used and kept by OLAF, and that the information collected by OLAF and forwarded to national authorities is accurate and up-to-date*" (p. 7), for example by ensuring swift transfers of updated information. For Member States officials adding data, OLAF provides guidance containing the same information.

This being said, the EDPS cannot rule *in abstracto* whether these categories of data should be included in all specific cases. The decision whether or not to include specific data categories must be made on a case-by-case basis. OLAF has issued guidance on how to meet these requirements for case handlers, including guidance on keeping data up-to-date (Guidelines for OLAF staff regarding the practical implementation of data protection requirements, Title 1.3).

The EDPS notes that the guidance contained in the Guidelines for OLAF staff regarding practical implementation of data protection requirements reflects the recommendations made in terms of data quality in the earlier prior checks referenced above.

3.6.2. CIS

The notification included a list of data categories that can be included in CIS (field 17). It is identical to the list set out in Article 25(2) of Regulation (EC) 515/97.

CIS respects the principle of data quality insofar as (i) the list of data categories to be processed seems appropriate for the intended purpose, (ii) data may only be included *"[...] if, in particular on the basis of prior illegal activities or of information provided by way of assistance, there is a real indication that the person in question has carried out, is carrying out or is about to carry out operations in breach of customs or agricultural legislation which are of particular relevance at Community level*" (Article 27(2) of Regulation (EC) 515/97), (iii) the same information on keeping data up-to-date that is supplied to V-OCU and MAB users is available for CIS user as well.

As for V-OCU and MAB, the EDPS cannot rule *in abstracto* whether these categories of data should be included in all specific cases. Again, decisions on a case-by-case basis are necessary. The same internal guidance referred to above also applies to CIS.

3.7. Conservation of data/ Data retention

Article 4(1)(e) of the Regulation establishes the principle that "*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*". Regulation 515/97 only specifies retention periods for CIS. OLAF informed the EDPS that, in practice, the procedures established for CIS are used for the other applications notified as well. For this reason, this section will start with a discussion of CIS before addressing the other systems. In the replies received on 26 May 2011, OLAF also announced that an

additional notification related to the processing of personal data in the AFIS logs will be notified to the EDPS in the future.

3.7.1. CIS

From a legal point of view, Article 33 of Regulation 515/97 establishes that data included in CIS shall only be kept for as long as is necessary to achieve the purpose for which they were included. The supplying partners have to review at least annually whether data are still needed. If there is no reply from the supplying partner within the review period for CIS, the data shall be transferred to a restricted part of CIS with limited access, both in terms of who can access it and what it can be used for (Article 33 (4)). Access shall be restricted to representatives of the committee assisting the Commission (Article 43), when this committee investigates the security of the system, the need to store data, or the confidentiality of stored information (Article 43 (4) indents 7, 8, 9) and the supervisory authorities as designated by the Member States (Article 37). Data stored in this part of the CIS may only be used to check their accuracy and the lawfulness of the processing and must be deleted after a year (Article 33(4)). If the partner decides that data are still necessary, they shall be retained until the next review.

For the practical implementation of these requirements, OLAF informed the EDPS that there is an annual review procedure in place. After 11 months, case owners are informed that the case is up for review and are requested to assess whether continued storage is necessary. If data is not flagged for an extension of the retention period during the review period (one month), it is deleted. The maximum retention period is 10 years, the minimum period equals one year. Additionally, the uploading CIS partner can delete cases at any time if continued storage is deemed unnecessary. This is only possible for CIS; the other systems do not contain a similar possibility.

In his Opinion on the first notification for CIS, the EDPS asked OLAF to provide more information on how the possibility to prolong retention is only used when necessary. OLAF informed the EDPS that there is no specific guidance in place to help case owners in making this decision.

The EDPS therefore encourages OLAF to issue guidance establishing a methodology for assessing whether continued storage of data is necessary.

3.7.2. V-OCU

As mentioned above, OLAF informed the EDPS that the basic procedures used for CIS are also applied to V-OCU. However, already at the end of the post-operational period, access is blocked and the data are no longer accessible. Additionally, no extension of the retention period is possible. This means that in practice, data are deleted after one year.

It would seem to be a better solution to delete data directly after the end of the post-operational period, as there seem to be no reason for prolonged storage: checks that establish a breach of customs or agricultural legislation would lead to the creation of a seizure report in one of the other systems; checks that do not yield positive results are no longer relevant. In both cases, continued storage in V-OCU does not seem to be necessary.

OLAF should provide reasons for this retention period, given that there seems to be no necessity for continued storage after the conclusion of a JCO and inform the EDPS about possibilities for reducing the period.

3.7.3. MAB

The rules for CIS are also applied to other MAB case types. As with V-OCU, there is no possibility to extend the retention period, in practice meaning a retention period of one year. The EDPS welcomes this significant change to the 10 year retention period in the old prior check notification on Mutual Assistance Exchanges.

3.8. Transfer of data

Transfers of personal data to other EU institutions, bodies and agencies, other Member States and third states and international organisations are governed by Articles 7, 8 and 9 of the Regulation, respectively.

3.8.1. Forwarding to other EU institutions, bodies or agencies

OLAF has general procedures in place for dealing with transfers to other EU institutions and Member States. If such transfers were to occur in the scope of the notified systems in the future, they would apply. These procedures oblige OLAF staff to check (i) whether the intended recipient has the appropriate competence and (ii) whether the transfer is necessary. These requirements must be fulfilled on a case-by-case basis for each and every transfer. Even if the transfer is foreseen in relevant legislation, this test must still be carried out (Guidelines for OLAF staff regarding the practical implementation of data protection requirements, p. 15). This procedure would also be applicable for transfers to other units within OLAF. It reflects the recommendations made in the prior check case 2007-0202.

In the notification, OLAF also mentioned that the DPOs of Eurojust and Europol have requested access to the log files for the AFIS portal, of which the systems subject of this Opinion form part. This has led OLAF to realise that personal data are processed in the logs. OLAF informed the EDPS that a procedure will be put in place for providing a monthly extract of the log files to the two DPOs who have requested access. The EDPS urges OLAF to ensure that these transfers comply with the conditions set out in the Regulation and to document it.

3.8.2. Forwarding to Member States

While the notifications mention the possibility of such transfers, OLAF pointed out that they do not take place in practice.

In the case of MAB and V-OCU, the privacy notices mention that data may be forwarded to "*competent administrative, legislative, and judicial authorities in Member States*". Article 1(1) of Regulation 515/97 clearly refers to the cooperation between administrative authorities in the Member States and the Commission as the aim of this Regulation. Similarly, the notifications refer to possible recipients in the Member States as "*competent authorities of the Member States* [...] *responsible for the application of Regulation (EC) 515/97*". The categories of authorities mentioned in the privacy statements are significantly wider than what is established under the legal basis. Contrary to this, the privacy notice for CIS mentions that data may be forwarded to "*competent administrative authorities in Member States*", which is in accordance with the legal basis.

According to Article 30(4) of Regulation (EC) 515/97, personal data stored in CIS may be transferred to other national authorities or third countries provided the CIS partner who included the data in the system has agreed to this and that any conditions he may have imposed on this transfer are adhered to. If in the future, OLAF were to upload data, the procedures as established in the Guidelines for OLAF staff regarding the practical implementation of data protection requirements (p. 14-17) would apply.

The list of authorities having access to CIS as established under Regulation 515/97 shall - according Article 29(2) of the same Regulation- be published in the OJ. So far, this did not happen. Apart from these official lists, there are internal lists established by OLAF for the management of users on a technical level, which have been referenced in the general part above (2.1, heading "Users and user management"). There is no formal connection between these lists.

OLAF should document the procedure for establishing the internal lists of authorities having access to CIS for the management of users on a technical level. These lists should be regularly updated. Moreover, OLAF should also, to the extent possible, be active in promoting the updating and publication of the official lists. The kinds of authorities specified in the MAB and V-OCU privacy notices should be updated to reflect the legal basis and the authorities having access.

3.8.3. Forwarding to third states and international organisations

The notifications or the accompanying documents indicate that transfers to third countries may occur in all three applications. In its replies of 26 May 2011, OLAF pointed out that in fact, such transfers do not occur for CIS. Transfers to third countries are governed by Article 9 of the Regulation.

For data included in the systems by Member States, transfers from CIS may occur "*with the prior authorization of, and subject to any conditions imposed by*" the Member State which uploaded the data, as established in Article 30(4) of Regulation (EC) 515/97. OLAF plays no role in this process. Thus, assessing the procedures in place would be outside the scope of this prior check Opinion. However, the second subparagraph of the mentioned provision establishes that this shall apply *mutatis mutandis* also where the Commission has included the data in the system. As mentioned above in the factual description, data are included by the Member States only. If this situation were to change, and OLAF were to start uploading information into the systems, which could then possibly be transferred to third countries, OLAF would also have to put appropriate measures in place to ensure that the requirements of Article 9 of the Regulation are complied with.

The question of data transfers to third countries and international organisations is dealt with on a horizontal basis in cases 2005-0154 and 2006-0493. This Opinion is not the place to elaborate further on this aspect.

3.9. Right of access and rectification

Articles 13 and 14 of the Regulation grant data subjects the right of access and rectification. This right is subject to certain exemptions and restrictions set out in Article 20 of the Regulation. As the relevant provisions in the privacy notices of the notified applications are almost identical, they can be considered together.

All three privacy notices contain almost identical provisions that data subjects "*may*" be granted access to their data, unless the exceptions of Article 20 of the Regulation apply. The only difference is that the notices for MAB and V-OCU refer to Article 20 in general, while the notice for CIS specifies that the exemptions under Article 20 (1) (a), (b) and (c) may apply.

The procedures OLAF has in place for dealing with such requests are elaborated in Title 1.5 of the Guidelines for OLAF staff regarding the practical implementation of data protection requirements. The instructions contained therein implement the recommendations given by the EDPS in his earlier Opinions on CIS and Mutual Assistance Exchanges (cases 2007-0177 and 2007-0202).

For V-OCU, OLAF mentioned in its replies submitted to the EDPS on 26 May 2011 that access would likely be denied during the operational phase of a JCO. Article 20(1) (a) of the Regulation allows such restrictions if they are necessary for "*the prevention, investigation, detection and prosecution of criminal offences*". More specifically, Article 36 (2) second subparagraph of Regulation 515/97 establishes that "*access may be denied to any person whose data are processed during the period in which actions are carried out for the purposes of sighting and reporting or discreet surveillance and during the period in which the operational analysis of the data or administrative enquiry or criminal investigation is ongoing*". Additionally, the authority which uploaded the information shall have the possibility to state its position before any data is disclosed to data subjects. Providing information to the data subject while the investigation is still ongoing could jeopardise the success of said investigation, which is why a deferral of access might be justified in these cases. However, any deferral must be decided on a case-by-case basis. These provisions may not be used to systematically deny access. Information has to be supplied to the data subject as soon as these exemptions no longer apply. Even if one of the exemptions under Article 20 (1) applies, Article 20 (3) obliges the controller to inform the data subject of the principal reasons for deferring access and the right to seek recourse to the EDPS. Article 20 (4) establishes that in these cases, when investigating complaints by data subjects, the EDPS shall only inform the data subject whether data have been processed correctly and if not, whether the necessary corrections have been made. According to Article 20(5), this information may be deferred as long as it would deprive the restriction imposed under Article 20 (1) of its effect.

OLAF should clarify that information shall be supplied to data subjects as soon as possible and that the exemptions provided for in Article 20 of the Regulation shall only be used on a case-by-case basis.

3.10. Information to the data subject

For category I data subjects, it can be assumed that information on their alleged wrongdoings is not collected from them but from other sources. Therefore, Article 12 of the Regulation is the relevant provision. This Article entitles data subjects to be informed of the identity of the controller, the purposes of the processing operation, the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him or her; the legal basis of the processing operation for which the data are intended, the time-limits for storing the data, the right to have recourse at any time to the European Data Protection Supervisor and the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy. Without

awareness that data about them are being collected, data subjects cannot exercise their rights to access and rectification, making adequate information crucial to safeguarding their rights.

Data subjects are informed about the possible processing of personal data relating to them via the privacy notices to be published on the OLAF website. These notices fulfil most of the requirements under Article 12. However, they contain some deficiencies:

- the MAB and V-OCU privacy notices do not contain a list of data categories that can be included in the systems;
- the reference to CIS in the MAB privacy notice refers to CIS as notified in DPO-17, i.e. not the version scrutinised in this prior check;
- while the CIS privacy notice contains a list of data categories, it is not accurate: identity documents and addresses are missing;
- in all notifications, the references to the legal bases could be more precise.

Regarding personalised information -i.e. not the general information that data may be processed, but information on the content of data processed on a specific data subject-, OLAF informed the EDPS that such information will only be provided "*if appropriate*" and with the prior agreement of the providing partner. Exemptions according to Article 20 of the Regulation may be applied on a case-by-case basis. Procedures for proactively informing data subjects are set out in Annex 5 to the OLAF manual, titles 1.5 and 2. If the exemptions in Article 20(1) are used, data subjects must still be informed of the principal reasons on which their use is based and their right to seek recourse to the EDPS. This information may be deferred as long as is necessary if its provision would deprive the restriction imposed according to paragraph 1 of its effect. These provisions cannot be used to defer access indefinitely; as soon as the reasons for the deferral are no longer valid, information has to be supplied.

As regards information uploaded by authorities in the Member States, this should be provided by the authorities, reflecting their duties as co-controllers.[24]

Regarding category II data subjects in Member States, OLAF informs the respective authorities in the Member States that they should supply appropriate information to their officials before they start using the systems. For category II data subjects who are officials in international organisations, it is not evident from the supplied information whether they receive similar information. Similarly, it is not clear how employees at OLAF working on these systems are informed of their rights and the processing related to their data, which is different than for category I data subjects.[25] They have access to the Guidelines for OLAF staff regarding practical implementation of data protection requirements which contain information on their rights, but from the information available to the EDPS, there seems to be no privacy statement provided to them informing them concisely about their rights and how to exercise them.

OLAF should therefore update the V-OCU and MAB privacy notices with exhaustive lists of data categories. It should also include an updated reference to the CIS notification in the MAB privacy notice, as well as correct the list of data categories in the CIS privacy notice. All three notices should be updated with more precise references to the legal bases. The updated notices should be published on OLAF's website immediately. OLAF should also ensure that appropriate information is provided to category II data subjects in its own staff and in international organisations.

[24] See section 3.4 above.

[25] The retention period of audit logs, e.g. is irrelevant for category I data subjects, but not for category II data subjects.

3.11. Security measures

[...]

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations expounded above are fully taken into account.

The recommendations of the EDPS can be summarised as follows:

Recommendations on V-OCU:

- Update the privacy notice with the exhaustive list of data categories and update the list of authorities in there in order to reflect the legal basis. Also include a more precise reference to the legal basis. Publish the updated privacy notice immediately on the OLAF website.
- Provide clear rules for retention periods and provide reasons for the retention period, given that JCOs usually take place during a short timeframe, and inform the EDPS of possibilities for reducing the period.
- Ensure that appropriate information is provided to category II data subjects in OLAF's staff and in international organisations.

Recommendations on MAB:

- Consider removing "drug addict" and "suicidal tendencies" from the list of warnings that can be introduced in MAB cases to reflect the legal basis. Also include a more precise reference to the legal basis. Publish the updated privacy notice immediately on the OLAF website.
- Provide reasons for the inclusion of the free text field for "other warnings" and, if the predefined warnings are judged to be sufficient, consider removing the field. Evaluate whether the field on physical characteristics is necessary. To this end, OLAF should collect information on the use of this field and inform the EDPS of the outcome within 6 months.
- Update the privacy notice with the exhaustive list of data categories and include an updated reference to the CIS notification. Additionally, update the list of authorities specified in the privacy notice in order to reflect the legal basis.
- Ensure that appropriate information is provided to category II data subjects in OLAF's staff and in international organisations.

Recommendations on CIS:

- Correct the list of data categories in the privacy notice. Also include a more precise reference to the legal basis. Publish the updated privacy notice immediately on the OLAF website. Provide appropriate information to OLAF staff working in the system as well.
- Evaluate whether the field on physical characteristics is necessary. To this end, OLAF should collect information on the use of this field and inform the EDPS of the outcome within 6 months.
- Consider issuing guidance for officers making the decision on whether to extend the retention period of data.

- The procedure for establishing the internal lists of authorities having access to CIS for the management of users on a technical level should be documented. These lists should be regularly updated.
- Regarding the procedure for establishing the lists of authorities having access to CIS according to Article 29(2) of Regulation 515/97, OLAF should, to the extent possible, be active in promoting the publication of the official lists. These lists should also be regularly updated.

Recommendations regarding the security of the AFIS related systems:

- [...]

Done at Brussels, 17 October 2011

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor