Opinion on the notification for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the Investigative Data Consultation Platform

Brussels, 18 July 2013 (case 2012-0280)

1. PROCEEDINGS

On 23 March 2012, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer ("DPO") of the European Anti-Fraud Office ("OLAF") a notification for prior-checking relating to the Investigative Data Consultation Platform (the "IDCP"). Together with the notification the DPO also filed:

- a note containing a description of the processing (the "Note") and
- an annex containing a list of entity types and data fields which will be used to create the database (the "Annex").

During the procedure, the EDPS requested OLAF to provide some complementary information both in writing and in meetings on various occasions. Given the complexity of the case, the EDPS extended the time-limit for issuing the Opinion by two months under Article 27(4).

On 13 May 2013, OLAF withdrew the initial notification and replaced it with a new one.

2. FACTS

The new notification deals with the design, development and use of a platform for the reciprocal exchange of investigative information between OLAF and its international partners. It raises complex issues of great importance for both anti-fraud investigations and data protection policy.

OLAF considers that fraud and corruption are global phenomena which must be addressed at an international level with flexible, swift and efficient instruments and with reinforced cooperation and exchange of information between investigative services. Cooperation with third countries and international organisations is thus considered as a crucial element of OLAF's activities. When carrying out its mission to protect EU financial resources, OLAF intends to rely on a network of investigative, administrative and judicial partners and equivalent partners in international organisations. OLAF notes that these partners often have a key role in exercising main control responsibilities in various projects financed by the EU and which are taking place outside the EU territory. According to OLAF, in these cases, the success of an investigation depends to a large extent on its ability to gather the necessary information from its international counterparts.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

From a data protection perspective, this case has also wide policy implications. Regulation (EC) No 45/2001 ("the Regulation") subjects data transfers to third countries or international organisations to strict conditions. Regular transfers of data to third countries or international organisations not ensuring an adequate level of protection is in principle prohibited. In these cases, authorisations may be granted by the EDPS, but only subject to adequate safeguards being put in place. To assess the adequacy of the safeguards, it is necessary to consider not only the content of the rules applicable to data transferred to third countries or international organisations but also the mechanisms in place to ensure the effectiveness of such rules.

The EDPS considers that an efficient anti-fraud investigation is in principle compatible with a high level of protection of personal data, provided that all the necessary data protection safeguards are put in place. We acknowledge that the fight against transnational crime cannot work without a certain degree of information exchange. In the same way, the reinforced exchange of useful information should take place with due respect of fundamental right to data protection and therefore on the basis of the strict conditions established by law. Data protection considerations should be seen as facilitating trust on the fight against fraud by promoting fair, proportionate and effective processing of personal data.

The EDPS will analyse the notified processing in the light of the above considerations, with a view to finding the appropriate balance in conformity with the Regulation between the protection of personal data and the public interests involved in the investigation and detection of fraud and corruption activities. In particular, the EDPS will focus the analysis on data processing modalities and safeguards allowing necessary and proportionate exchanges and ensuring the accountability of the actors involved.

2.1. Purpose of the processing

The following analysis builds on the description of the processing made by OLAF.

The IDCP is described as a database developed with the iBase technology. It will contain a subset of data from the investigative files of OLAF and its selected international partners ("IDCP partners"). The purpose of the tool is to allow IDCP users to exchange in efficient manner investigative information on ongoing cases. The functioning of the database is described in more detail in Section 2.2. OLAF mentioned that IDCP practical arrangements would be entered first with one donor international organisation. It is envisaged in the future that a limited number of other similarly important international organisations and possibly competent authorities of Member States and third countries will become partners.

In the framework of its activity, OLAF is negotiating and concluding with some selected partners the so called Administrative Cooperation Arrangements ("ACAs"). The ACAs set out a framework for practical cooperation between OLAF and its third country and international organisation partners, including rules and safeguards for the exchange of information. They also lay down in an annex data protection clauses and principles to be respected by ACA parties when exchanging personal data. The conclusion of an ACA with OLAF is a prerequisite for becoming a partner of the IDCP. The draft-model ACA and the Model Data Protection Contractual clauses were submitted to the EDPS for prior consultation under Article 46(d) on 26 January 2012. The EDPS provided his position on 3 April and 16 July 2012.[1]

[1] See EDPS Opinions of 3 April and 16 July 2012 on Model Data Protection Clauses to be included in Administrative Cooperation Agreements (ACAs) concluded with third country authorities or international organisations, available on EDPS website.

2.2. Description of the processing

The IDCP will contain a subset of data extracted from the IDCP partners' investigative files. The subset of data corresponds to the main characteristics of the investigation, which are regrouped into the following "data entities": 1) investigation, 2) person, 3) organisation/company, 4) location, 5) address, and 6) communication. Each data entity has a number of "data fields". For instance the fields for the investigation data entity are the following:

- name of the case,
- number of the case,
- case type (e.g. investigation, coordination),
- brief description of the case (e.g. "alleged fraud within network of companies in relation to EU funds in Country X"),
- principal allegation (e.g. misappropriation of funds, fraud and embezzlement, altered submission of tenders before the evaluation exercise began),
- method of fraud (e.g. non-eligible claims and expenditures, failure to comply with contract conditions, conflict of interest, irregularity in tendering procedure),
- geographic zone,
- date of opening,
- date of closing,
- stage of the case.

The full list of data fields is contained in Section 2.4 below.

For each of their investigative files, IDCP partners will extract the data fields corresponding to the six data entities. With regard to OLAF files, the data will be extracted, in particular, from case files relating to external aid and direct expenditure sectors but can also include other expenditure sectors. The extraction will be limited to documents from 2003 onwards.

In addition, all entities include the following data fields for maintenance purposes: source hyperlink, creation date, creation user, last update date, last update user and record ID.
OLAF's partners will electronically send to OLAF identical data sets relating to the above data entities. OLAF will introduce the data into the database and carry out all the operations necessary for the functioning thereof. This transfer will occur on a regular basis and via a specific “secured e-mail protocol”.

The IDCP will allow the IDCP partners to carry out searches using search terms. No particular limitation or rules are foreseen with regard to the selection of the search terms: the system will list all data entities from the IDCP database that match the search term used. For instance the search on the name of a person will list all data entities whose data fields contain this name, including the related investigation entity for all cases stored in the database. In addition, the database will show the *links* between that entity and other correlated investigation, communication, address and organisation/company entities. A search on the name of a person could thus give rise to results in the *Person* data entity if the name corresponds to that of a person concerned by an investigation and the *Organisation/company* entity if the name is included in the name(s) of the organisation (including the relevant address). In addition, the database will show the *links* between that person entity and related investigation, communication address and organisation company entities. It is technically possible to limit the number of results returned to the users for any search. The user will thus only see results up to a certain predefined threshold (i.e. if the threshold is set to 200, the user will see the first 200 results and not more).

The partner (or OLAF) will be entitled to ask for a schematic graphical display of the links. If the partner then clicks on one of the matching entities within the schematic display, any further entities linked to the selected entity will then be displayed. The partner will be also empowered to ask for display of the data fields for each entity. This expansion of related entities will be limited to the predefined threshold.

The partner or OLAF, where interested to get additional information, should contact OLAF or the IDCP partner concerned and request to be provided access to such information in accordance with the applicable ACA. This potential follow-on exchange of personal data (which also has to comply with the requirements for data transfers set forth in Article 9 of the Regulation), is not covered by the present prior-check.

2.3. Data subjects

The data subjects concerned by the present processing activity fall within the following categories:

- natural persons who are or were the subject of OLAF's external investigations;
- natural persons who have provided information to OLAF or its operational partners as witnesses;
- natural persons whose name appears in the information provided by OLAF's IDCP partners.

In further exchanges with the EDPS, OLAF specified that informants and whistleblowers and witnesses will be specifically excluded from the IDCP.

2.4. Categories of data

In the notification, OLAF indicates that the following data entities and corresponding data fields will be processed in the IDCP database:

- Identification data: full name, last name, first name, alias, data of birth, age, place of birth and country of birth (Person table);
- Contact data: address, telephone, e-mail, website and fax (Communication and Mailing Address table);
- Professional data: role in company, address, telephone, e-mail, website and fax (Organisation, Company table);
- Case involvement data: case name, brief case description, principal allegation. The nature of involvement of a person/economic operator is not provided.

The iBase design report attached as an Annex to the notification contains a more detailed configuration of the entity types and data fields which will be used for the purpose of the database. The list of data fields has been modified and further updated in the course of the procedures. According to the information received, the complete list appears as follows:

The data fields displayed for the *Investigation* entity will be the following:

- name of the case,
- number of the case,
- case type (e.g. investigation, coordination),
- brief description of the case (e.g. "alleged fraud within network of companies in relation to EU funds in Country X"),

- principal allegation (e.g. misappropriation of funds, fraud and embezzlement, altered submission of tenders before the evaluation exercise began),
- method of fraud (e.g. non-eligible claims and expenditures, failure to comply with contract conditions, conflict of interest, irregularity in tendering procedure),
- geographic zone,
- date of opening,
- date of closing,
- stage of the case.

The data fields displayed for the *Person* entity will be the following:

- full name,
- icon,
- surname,
- first name,
- alias,
- date of birth,
- age,
- incomplete date of birth,
- place of birth,
- country of birth.

The data fields displayed for the *Organisation/company* entity will be the following:

- icon,
- organisation name,
- name tradestyle,
- type,
- nationality,
- activity.

The data fields displayed for the *Address* entity will be the following:

- street name,
- house number,
- floor,
- post/zip code,
- city, region,
- country,
- location name

The data fields displayed for the *Communication* entity will be the following:

- icon,
- device number,
- region,
- country code,
- city.

OLAF states that no special categories of data will be transferred via the IDCP.

2.5. Information rights

According to the notification, the data subjects will be normally informed of the processing taking place in the context of such investigations by means of the privacy statements and other means foreseen in the context of these investigations. If a derogation pursuant to Article 20 of the Regulation applies, such information will be provided when the conditions of the derogation no longer apply.

OLAF will make available to data subjects, upon request, a copy of the relevant ACA and its annex. The relevant procedures can be found in the notifications concerning external investigations and have been analysed in the context of the EDPS Opinion on OLAF new investigative procedures.[2]

2.6. Categories of recipients to whom data might be disclosed

Access to the platform is reserved to a small number of OLAF's designated staff in charge of case selection and operational analysts, and designated staff of the relevant OLAF partner. These recipients will have direct access to the platform and to the relevant personal data.

The notification also mentions possible recipients in relation to follow-on manual exchanges of personal data. These exchanges, however, do not form part of the present prior-check.

2.7. Conservation of data

The personal data concerned by the present processing will be stored for 10 years. Data are subject to annual reviews using automated and manual checks after three years in order to ensure that data are held in accordance with the agreed retention period. OLAF could retain relevant personal data in its investigation case files for a maximum of 15 years in accordance with the rules applicable to such investigations.[3] Data received from IDCP partners will be retained by OLAF according to the transmitting partner's requested time limit. The ultimate retention period in these cases will be 10 years.

2.8. Right of access

As regards right of access, OLAF refers to the privacy statements for the external investigations. The applicable procedures can be found in OLAF's notification concerning external investigations and have been analysed in the context of the related EDPS Opinions.[4]

2.9. Security measures

The notification provides background information on the security controls implemented within OLAF (baseline security controls), regardless of the system specific needs. These security controls contribute to the overall assurance in the level of security implemented on all OLAF systems.

An additional description of the IDCP-specific security controls was provided as a follow-up and in the answers to the EDPS's questions. [...]

---

[2] EDPS Opinion on OLAF new investigative procedures of 3 February 2012, available on EDPS website under the section Supervision/Prior checks/Opinions.

[3] *Ibidem*.

[4] Cited above. See also EDPS Opinion on OLAF external investigations of 4 October 2007 (cases 2007-0047, and others), available on EDPS website.

3. LEGAL ASPECTS

3.1. Prior checking

The IDCP will be a platform for the reciprocal exchange of investigative information between OLAF and its IDCP partners, i.e. international organisations and possibly Member State and third country national authorities. The information exchanged will contain personal data of the persons who are the subject of an investigation. The platform therefore will imply the processing of personal data. The processing activity will be carried out by a European institution, in the exercise of activities which fall within the scope of EU law (Article 3.1 of the Regulation). The processing of personal data will be done by automatic means (Article 3.2 of the Regulation). As a consequence, the Regulation is applicable.

Article 27.1 of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks. Under Article 27(2)(a) of the Regulation, processing operations relating to "suspected offences, offences, criminal convictions or security measures" shall be subject to prior checking by the EDPS. In the case in point, the processing operation could be related to the processing of these types of data.

The notification of the DPO was received on 23 March 2012. According to Article 27(4) the present Opinion must be delivered within a period of two months. In view of the complexity of the case, the EDPS extended the time limit to provide his Opinion by two additional months in conformity with Article 27(4). The procedure has been suspended during a total of 273 days in order for the EDPS to obtain necessary additional information.

On 23 April 2013, OLAF withdrew its original notification and replaced it with a new one. A new time limit started to run from that date. The procedure has been suspended for a total of 3 days in order for the EDPS to obtain necessary additional information.

The procedure was further suspended for 16 days to allow for provision of comments on the draft Opinion. Therefore, the present Opinion must be delivered no later than 22 July 2013.

3.2. Lawfulness of the processing

Processing of personal data must be based on one of the grounds listed in Article 5 of the Regulation.

3.2.1. Article 5(b)

In the notification, OLAF indicates that the legal basis for the present processing is Article 5(b) of the Regulation concerning the processing which is necessary for the purpose of a legal obligation. In the EDPS view, only an obligation which is sufficiently clear and specific may legitimise the processing of personal data pursuant to Article 5(b). For Article 5(b), it has to be established that the controller (which is OLAF in the present case) is subject to a legal obligation to collect and process data which leaves him no space for discretion.[5]

[5] Article 5(b) authorises processing that is "*necessary for compliance with a legal obligation to which the controller is subject*".

The notification mentions specifically the following provisions: Article 3 of Regulation 1073/2001 and Article 2 of Commission Decision 1999/352, horizontal legislation (in particular Council Regulation 2185/96[6] and 2988/95[7]) as well as sector specific legislation or other legal provisions where applicable (e.g. Regulations 1080/00[8], 2666/00[9]; LOME Conventions and Cotonou agreements). The EDPS considers that the link to the above legal provisions is not sufficiently precise in the present case to justify the application of Article 5(b). While the above provisions establish OLAF investigative powers in the field of external investigations, they do not oblige OLAF to set up the IDCP or a similar instrument. The fact that OLAF has been conducting external investigations in the past without such instrument further supports the conclusion that OLAF is not "legally obliged" to establish the IDCP.
In view of the above, the EDPS will analyse whether the processing can be covered by Article 5(a) of the Regulation.

3.2.2. Article 5(a)

Article 5(a) of the Regulation allows processing of personal data that is *"necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*". Article 5(a) contains three elements, all of which must be complied with: 1) the processing must be performed in view of a task carried out in the public interest; 2) the task must be based on law (either the Treaties or another act based on them) or in the legitimate exercise of official authority vested in the EU institutions or body or in a third party to whom the data are disclosed, 3) it must be necessary for the performance of such task.

3.2.2.1. Performance of a task in the public interest

On the basis of the information provided and mentioned in Section 2.1, it appears that the IDCP will be part of a task carried out in the public interest, i.e. the conduct of external investigations in order to combat fraud, corruption, and other illegal activities affecting the financial interests of the EU.

3.2.2.2. Legal basis

The specific legal bases for administrative external investigations have been already outlined in the EDPS prior check Opinion on OLAF external investigations to which reference is made.[10] The legal bases cited by OLAF in the notification are also relevant. All the above provisions entrust OLAF with the task of carrying out external administrative investigations for the purpose of strengthening the fight against fraud.

---

[6] Council Regulation (EURATOM, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities, OJ L 292, 15.11.1996, p. 2–5.

[7] Council Regulation (EC, EURATOM) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests, OJ L 312, 23.12.1995, p. 1–4.

[8] Council Regulation (EC) No 1080/2000 of 22 May 2000 on support for the United Nations Interim Mission in Kosovo (UNMIK) and the Office of the High Representative in Bosnia and Herzegovina (OHR), *OJ L 122,* 24.5.2000, p. 27–28.

[9] Council Regulation (EC) No 2666/2000 of 5 December 2000 on assistance for Albania, Bosnia and Herzegovina, Croatia, the Federal Republic of Yugoslavia and the Former Yugoslav Republic of Macedonia, repealing Regulation (EC) No 1628/96 and amending Regulations (EEC) No 3906/89 and (EEC) No 1360/90 and Decisions 97/256/EC and 1999/311/EC, OJ L 306, 7.12.2000, p. 1–6.

[10] EDPS Opinion on OLAF external investigations of 4 October 2007 (cases 2007-0047, and others), available on EDPS website.

Pursuant to Article 2(5)(a) of Commission Decision 352/1999 "*[t]he Office shall be responsible for any other operational activity of the Commission in relation to the fight against fraud as referred to in paragraph 1, and in particular: (a) developing the necessary infrastructure; (b) ensuring the collection and analysis of information; [...]. The Office shall be in direct contact with the police and judicial authorities*".[11]

The IDCP will be used by OLAF for the purpose of exchanging information and cooperating with its international partners in the framework of external investigations. It can thus be considered as justified by the above legal provision, as an infrastructure developed in relation to the fight against fraud and ensuring the collection and analysis of information.

Nevertheless, for the sake of legal certainty, the EDPS recommends that the legal basis be reinforced and that for this purpose OLAF enter specific arrangements with the IDCP partners by exchange of letters as specified in the ACA's based on the Model ACA approved by the EDPS, setting out the main elements of the processing and its external limits. This would be a necessary safeguard, not only for data subjects but also for OLAF itself, as it would give the IDCP a more solid legal basis.

3.2.2.3. Necessity

OLAF put forward various arguments to justify the necessity of the new platform both in writing and orally in the course of the operational meeting at the EDPS.

OLAF stressed that cooperation with Member States, third country authorities and international organisations is a crucial element of its activities. When carrying out its mission to protect the EU budget OLAF intends to rely on a network of investigative, administrative and judicial partner services and organisations. OLAF notes that these partners often have concurring responsibilities in exercising control in various projects financed by the EU and which are taking place outside the EU territory. OLAF declares that it may not have sufficient investigation or information gathering powers in respect of such projects and need therefore to rely on its partners' cooperation. Information sharing with regard to the implementation of such projects is therefore considered by OLAF as an essential element for its investigative tasks.

OLAF stressed that in order to be able to effectively share investigative data with its partners, it must know whether relevant information exists and which partner has it. OLAF emphasised in particular the need to gather information about cases of undeclared double funding for the same project and parallel investigations running on the same project. It explained that the lack of coordination between donors leads to cases in which funds for the same project are paid twice or even several times by different donors, due to a general lack of coordination. OLAF maintains that these shortcomings would significantly be reduced if a system were in place allowing the exchange of information on parallel investigations. OLAF argues that the IDCP would fill this lack of intelligence, because it will allow OLAF to verify that a partner has investigated or is investigating on a parallel or related case or anyway may possesses relevant information on a specific case.

The EDPS has carefully taken note of these arguments. OLAF provided sufficient elements justifying the need for more structured cooperation in the fight against fraud in the external expenditure sector. Cooperation and exchange of information are indeed essential to effectively

[11] Commission Decision 352/1999, cited above.

tackle fraud taking place at the international level. Double funding cases may provide an appropriate example of the need for greater coordination, as their financial impact is considerable. Especially in times of economic crisis, funds have to be administered effectively.

Cooperation could be more effective where it is not unilateral but takes place on a reciprocal basis. OLAF provided sufficient arguments to establish that it can only get the information it needs from its partners if it also accepts to mutually share information with them. The necessity of the transfers should therefore be assessed in view of the reciprocity that is ensured. In this respect, OLAF's contribution to the IDCP could be seen as a precondition to its membership and to the partners' willingness to contribute to it.

As to the specific tool chosen, it falls within the margin of appreciation of the EU institution to consider which mechanisms are best suited to achieve the underlying aim, insofar as these means are not manifestly disproportionate. In the present case, it appears that a manual system for information sharing would not be an effective substitute for various reasons. First, the IDCP will allow OLAF to consult its partners in one shot instead of one by one. Second, the consultation will be carried out through automatic means, which means immediate and more precise replies.

The notified processing can therefore to be based on Article 5(a) of the Regulation. Having said this, the lawfulness of the IDCP depends on its compliance with all the requirements of the Regulation, including proportionality and data quality, which will be examined in the following Sections.

3.3. Identification of the controller

Under Article 2(d) of the Regulation the "controller" is defined as "*the [EU] 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*". Opposed to the notion of controller is the notion of "processor" defined by Article 2(e) as "*any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*" (emphasis supplied).

The identification of the controller in the context of data processing operations serves to determine the entity which shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which data protection law is applicable as well as jurisdictional issues. The clarification of roles and responsibilities becomes even more important when, as in the present case, several entities are potentially involved in the processing of personal data.

In the notification, OLAF states that it will process the data sets received from IDCP partners "on behalf of the partner". This does not make it clear whether OLAF regards itself as a processor, as opposed to a controller, in relation with the data sets transmitted by IDCP partners. However, on the basis of the description of tasks included in the new notification and the other documents provided, it appears that OLAF will play a crucial role in the database management. The database will be physically located in OLAF's premises and hosted on an OLAF's server. OLAF's analysts will be responsible for the management of the physical infrastructure. OLAF will manage authentication, user accounts, uploads, secure access and authenticated users with valid certificates from the partner organisation.

Given the extent and importance of its tasks as described in the notification, OLAF's role regarding the set of data transmitted by the IDCP partners cannot be that of a mere processor.

OLAF will have a paramount role in the management of the system. Depending on the degree of control exercised by the IDCP partners over the management of the database, OLAF can be qualified either as a sole controller or a joint controller with a primary responsibility, but not as a mere processor.

In view of the above, the EDPS recommends that OLAF clearly specifies the responsibilities of the various actors in the implementation of the IDCP in a specific User Manual. The EDPS recommends that OLAF foresees, inter alia, the following main points:

- Each IDCP partner and OLAF will be controllers with respect to their own data processing activities as partner of and contributor to the system. Each IDCP partner will be responsible for ensuring the data quality and lawfulness of the data they put into the system.
- OLAF will be the operator of the system, responsible, first and foremost, for the technical operation, maintenance and ensuring the overall security of the system.
- IDCP partners and OLAF will share responsibility with respect to notice provision, and provision of rights of access, objection, and rectification.

3.4. Data quality

Pursuant to Article 4(1)(a), (c) and (d) of Regulation 45/2001, personal data must be processed fairly and lawfully, be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed, as well as accurate. The lawfulness of the data processing has already been discussed (cf. point 3.2), whereas its fairness has to be assessed in the context of information provided to data subjects (cf. point 3.9).

The IDCP implementation will be based on a "pull" concept. IDCP partners will be able to access OLAF investigative information from the database directly without OLAF interaction. The pull access presents specific risks that data which is not relevant will be provided in response to a search. In order to minimise such risks, the data included in the IDCP should be limited to a strict minimum. By way of example, a search for a particular name may reveal information concerning several unconnected cases in different countries, whereas the investigating authority is only interested in one of these cases in one particular country. The risk of irrelevant collection or fishing expeditions would therefore increase when direct access is allowed. As a general rule, any exchange of personal data must respect the principles of necessity and proportionality. The exchange of data which are not relevant for the purpose of the investigation concerned must therefore be avoided or minimised.

In the course of the procedure, the EDPS considered whether a pure hit/no hit system, showing solely whether a particular entity (e.g. a name, a company, an address) linked to any investigation could be used in the present case. OLAF firmly replied that such a system would not serve the underlying purpose for a number of reasons:

- a hit-no-hit system is best conceived for those systems in which the information is fully described in terms of a positive or a negative answer and would therefore be comprehensively expressed in terms of a hit (or a limited number of hits) or a no hit. This is particularly the case for those systems which are based on a binary logic (hit-no hit). This is not the case for the information included in the current database;

- investigative data are linked by complex logical relationships and become intelligible only on the basis of the understanding of such links. This is due to the fact that investigators do not work on complete information on their case (as they are investigating it) and need to verify if any element in their case has a direct or indirect link with information collected in another case. Understanding the links between the different entities is one of the core analyses performed by investigators in their line of duty and this cannot be achieved solely on the basis of a hit-no-hit system. To obtain a meaningful result, investigators need to identify cases that have only limited similarities with the object of their investigation and confirm a possible direct or indirect relation with their case by looking at the known cases and how they relate to one another;
- names may be easily misspelled, certain terms or names may be too common and give rise to excessive matches or wrongly or inaccurately classified. To obtain a meaningful result, OLAF may thus need to make links with the other data at its disposal and put them in relation with the other partners' data;
- OLAF considers that this system would represent an administrative burden that would create a strong deterrent to using the system.

The EDPS takes note of the above arguments. Nonetheless it is important to introduce some appropriate safeguards as to the scope of access, to mitigate data quality concerns. In particular, he recommends that OLAF further specifies the modalities of access as follows:

1. each access to the IDCP shall be duly motivated and validated via an internal procedure set up by each partner, specified in the user guide, which each partner would have to agree to apply. This would allow a prior control of the necessity of the access to the data. The request and the motivation by the partner should be recorded and verifiable *ex post*. This procedure should also be reflected in the database functionalities. In particular, OLAF should include a mandatory field requesting the partner at each search session to indicate the investigation concerned (or the related case operational file) and briefly motivate necessity on this basis. If integrating this functionality into the database is not possible, OLAF should set up a separate database solely for the purpose of recording the justifications from the users. This database could be located in a separate environment under tight control by OLAF;
2. implement a two stages approach in which all partners will have access to a first layer of data and may then obtain access to the graphic expansions of the result (second layer) upon reasoned request to be electronically validated by OLAF as far as OLAF's data are concerned. As an alternative, OLAF may envisage a blended system with full access to non-personal data (e.g. data relating to companies that do not identify natural persons) and hit-no hit for names and other personal data;the system should set a threshold to the number of results it returns per search. If a search results in too many hits, the user should only be presented with the most relevant results (exact matches first) up until the threshold is met and the user should be informed of the fact that his search yielded too many results. This threshold should be determined based on business needs and with considerations for data protection;
3. OLAF should limit the recourse to open fields. In particular, OLAF should limit the content of open fields on the basis of specific criteria (for example by limiting the length of the text string);
4. OLAF should limit the scope of the data entity "Person" only to persons or entities subject to an investigation.

Having regard to data accuracy, data must be subject to frequent reviews by each partner (at least annual) with a view to verifying their accuracy and their being up to date. Data may also need to be updated due to the progress of the investigation, e.g. when people are cleared of

suspicions. OLAF should also recommend and verify that adequate policies and safeguards are put in place by its partners in this respect. Data which according to OLAF retention policy need to be deleted from its files must be removed also from the IDCP. In this respect, see also below Sections 3.6, 3.8 and 3.10.

3.5. Special categories of data

Article 10.5 stipulates the following: *"[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 by OLAF can be considered authorised by the relevant provisions in Regulation 1073/1999 and Article 2 of Commission Decision 1999/352 establishing OLAF competence to conduct anti-fraud investigations.

According to Article 10.1 of the Regulation, the processing of special categories of data (that is *"data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life"*) is prohibited. The Regulation foresees certain exceptions in Article 10(2). However, it seems most likely that, if any exception would apply, only that of sub-paragraph (d) would possibly be relevant. However, being an exception, this provision must be interpreted restrictively.
In the new notification, OLAF, as controller, states that no special category of data will be transferred via the IDCP. In the context of the ensuing exchange of personal data, it seems that the processing of special categories of data cannot be totally excluded but would be exceptional. In any event, OLAF staff in charge of the files must be aware of this rule and avoid the inclusion of special categories of data unless one of the circumstances foreseen in Article 10.2 (in a restricted sense, as mentioned above) is present in the particular case under investigation or if Article 10.4 can be applied.

3.6. Conservation of data

Personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes"* (Article 4(1)(e) of the Regulation).

According to the new notification, the personal data concerned by the present processing will be stored for 10 years. Data will be subject to annual reviews using automated and manual checks once data will be held for three years in order to ensure that data are held in accordance with the established retention period. OLAF declares that relevant personal data may be retained in its investigation case files for a maximum of 15 years in accordance with the rules applicable to such investigations.[12] Data received from international partners will be retained by OLAF according to the transmitting partner's requested time limit. In any event, the ultimate retention period also in these cases will be 10 years.

The EDPS has not received convincing justification as to the necessity of such a long retention period. *Prima facie*, there is no evidence that shows that a shorter retention period (e.g. 5 years)

[12] EDPS Opinion on OLAF new investigative procedures of 3 February 2012, available on EDPS website under the section Supervision/Prior checks/Opinions.

would not be sufficient. He therefore recommends that OLAF reduce its retention period for IDCP data. In addition, it is recommended that OLAF ensures deletion from the IDCP of all personal data that according to its retention policy need to be deleted from its files (e.g. data older than 15 years), irrespective of whether they are being kept in the IDCP for less than IDCP retention period.

3.7. Transfers of data

Pursuant to Article 9(1) of the Regulation, transfers of personal data to recipients other than EU institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, can only take place if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and data are transferred solely to allow tasks covered by the competence of the controller to be carried out.[13] This rule is of particular relevance to OLAF as most of the third countries or international organisations with respect to which transfers of personal data by OLAF would take place would not be recognised generally as ensuring an adequate level of protection.

By way of derogation to the general rule, an EU institution or body may transfer personal data to the above mentioned recipients if one of the exceptions laid down in Article 9(6) of the Regulation applies. Among the various exceptions stipulated in Article 9(6), subparagraph (d) concerning transfers necessary or legally required on important public interest grounds is of specific relevance to OLAF, as many of the international transfers it carries out are likely to fall within its scope. Nevertheless, a systematic use of the derogations is unacceptable from a data protection viewpoint. In principle, transfers based on the above mentioned exceptions should not be massive, systematic or structural.[14]

The IDCP introduces an information sharing tool which is permanent, structural and systematic. Therefore, it does not as a matter principle qualify for an exception based on Article 9(6)(d) of the Regulation. Consideration must therefore be given to Article 9(7) of the Regulation providing that the EDPS "*may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection [...] where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular results from appropriate contractual clauses*".

In order to establish whether the IDCP qualifies for the application of Article 9(7) of the Regulation, the EDPS has thus to verify whether it provides for adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

In this respect, the following elements should be considered:

- OLAF has defined a set of clauses for the exchange of information to be agreed with third countries and international organisations in the framework of an administrative cooperation arrangement (ACAs). OLAF will grant access to the IDCP only to international partners with whom it has concluded an ACA which includes an annex containing data protection clauses;

[13] In parallel with the present prior-check, the EDPS is developing a position paper on trans-border data transfers (TBDF), which will also cover the type of exchanges which are the subject of the present prior-check.

[14] See Article 29 Working Party Working Document, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24 June 1998, available on the Working Party website.

- the EDPS has analysed these safeguards[15] and considered them essentially in relation to exceptions pursuant to Article 9(6) of the Regulation. Given the limited number of transfers foreseen by OLAF, the EDPS invited OLAF to use such clauses in the context of transfers based on exceptions. Should the frequency and scope of exchanges significantly grow in the future, OLAF needs to request a specific authorisation pursuant to Article 9(7) of the Regulation;
- OLAF plans to conclude an IDCP partnership only with selected partners who are considered by OLAF to provide sufficient guarantees of reliability. In its advice concerning ACAs the EDPS recommended, among other issues, that "*OLAF should carefully select its partners, by making a preliminary assessment of their capacity and willingness to respect the clauses of the ACA and its annexes*".

Having been developed in relation to exceptional transfers, the general safeguards provided in the ACAs cannot automatically be used in the case of IDCP and must therefore be reinforced to qualify as adequate safeguards for the purpose of an Article 9(7) authorisation. The request for authorisation will be analysed by the EDPS in a separate procedure.

3.8. Rights of access and rectification

Article 13 of the Regulation provides for a right of access for data subjects, Article 14 grants the right to rectification of personal data.

The right of access gives individuals the possibility to learn whether and what type of information relating to them is being processed. The right of access often is a *prius* to the right of rectification. Once individuals have had the opportunity to access their data and verify the accuracy and lawfulness of the processing, the right to rectification enables them to require rectification of any inaccurate or incomplete information. Respect for the rights of access and rectification is directly connected to the data quality principle and, in the context of investigations, it overlaps to a great extent with the right of defence. Ensuring the right of access to the person concerned by the external investigation is therefore of the utmost importance.

The EDPS would note that as a manager of the IDCP and controller of the data, OLAF is bound to provide access to IDCP data, irrespective of whether such data originate from its files or from the files of a partner. OLAF will have to provide access, unless a restriction under Article 20 of the Regulation applies. In deciding whether a restriction applies to the personal data originating from a third party, the EDPS recognises that OLAF may need to consult its partners. The EDPS stresses in any event that these restrictions should be interpreted restrictively and cannot be applied systematically.

In the new notification, OLAF refers to the principles and procedures used in the framework of external investigations, which would also apply in the present case. Therefore, the guidance given by the EDPS in the Opinions on OLAF external investigations (see section 3.7 thereof) and OLAF's new investigative procedures applies by and large in this context[16]. The EDPS would refer OLAF to the observations and recommendations issued in those Opinions and the related ongoing follow up.

[15] The clauses are essentially inspired - with some adjustments - by the Commission's 2004 alternative contractual clauses. See Commission Decision of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ 29.12.2004, L 385/74.

[16] Cited above.

3.9. Information to the data subjects

The Regulation states that the data subject must be informed where his or her personal data are being collected and lists a number of mandatory points to be included in the information, in order to ensure the fairness of the processing of personal data. In the case at hand, the data processed by OLAF are either already in its possession (i.e. OLAF's data) or collected from other IDCP partners.

In the notification, OLAF refers to the principles and procedures used in the framework of external investigations. The EDPS points out that this approach is only acceptable in part. In particular, it only applies to the first category of personal data (data already stored in OLAF files). As these data are already recorded in the CMS in the framework of the respective external investigation, it is true that the data subjects have in principle already been informed of the processing of his/her personal data for the purposes of Articles 11 and 12 of the Regulation.[17] The EDPS would refer in this regard to the prior-check Opinions on OLAF external investigations and OLAF new investigative procedures.

The situation is different for those personal data which have been collected by OLAF from IDCP partners. In this case, there is no guarantee that the data subjects have been informed by the transferring authority. It should also be borne in mind that data may be collected from countries or organisations where there are no data protection rules. This implies that the information pursuant to Article 12 has in principle to be provided by OLAF, unless pursuant to Article 12(2) of the Regulation "*the provision of such information proves impossible or would involve disproportionate effort*".

In the present case, the EDPS recognises that the provision by OLAF of particularised information to each person whose name is provided by OLAF partners would involve a disproportionate effort. Alternative means should therefore be used in order to ensure, as a second best solution, the widest transparency of the processing. For example, OLAF could place a specific privacy statement concerning IDCP on its website and ask its partners to do the same. The ACAs and the Data Protection annex should also be adequately published.

3.10. Security measures

[...]

4. CONCLUSIONS

The proposed processing operation may be implemented in light of the provisions of Regulation (EC) No 45/2001 provided that full account is taken of the recommendations made above. In particular, OLAF should:

- make relevant arrangements with the IDCP partner organisations for the present processing, setting out the main elements of the processing and its external limits;
- clearly specify the allocation of responsibilities between OLAF and other IDCP partners concerning the respect of the requirements of the Regulation (see Section 3.3 above);
- limit modalities of access as specified in Section 3.4 above;
- ensure sufficiently frequent (at least annual) reviews of the accuracy, completeness and up-to date nature of the personal data included in the IDCP;

[17] Except in cases where an Article 20 exception applies.

- reduce the length of the retention period;
- ensure deletion from the IDCP of all personal data that according to its retention policy need to be deleted from its files (e.g. data older than 15 years), irrespective of whether they are being kept in the IDCP for less than 10 years;
- provide for additional guarantees in the context of the IDCP partnership in order to be eligible for an authorisation under Article 9(7) of the Regulation. Such additional guarantees will be dealt in the framework of the separate procedure for the granting of the authorisation pursuant to Article 9(7);
- provide an effective right of access to IDCP data (or ensure that the partner from which the data originates provides such access), irrespective of whether such data originate from OLAF files or from the files of a partner, unless a restriction under Article 20 of the Regulation applies;
- put in place adequate mechanisms with a view to enhancing the transparency of the processing vis-à-vis the data subjects of data transmitted by third countries according to Article 12 of the Regulation, as indicated in Section 3.9;
- perform a complete analysis of the risks and define in details the specific security controls that need to be implemented to reduce the risks to a level acceptable by OLAF's management; this includes a review of the existing security controls, taking into account Section 3.10 above.

The implementation of the IDCP is subject by law to a specific authorisation by the EDPS under Article 9(7) of the Regulation. The request for an authorisation will be analysed by the EDPS in a separate Opinion. OLAF should refrain from activating the IDCP until the EDPS grants such authorisation.

Done at Brussels, 18 July 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor