GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Ms Laraine LAUDATI
Data Protection Officer
European Commission
European Anti-Fraud Office
(OLAF)
1049 Brussels

Brussels, 10 August 2012
Our ref: D(2012)1681 **C 2012-0279**
Please use edps@edps.europa.eu for all correspondence

Subject: notification for prior checking from the Data Protection Officer of the European Anti-Fraud Office (OLAF) regarding the processing of personal data in relation to the Search Facility

Dear Ms Laudati,

I am writing about the prior check notification concerning the Search Facility submitted by you on 23 March 2012. The notification was triggered by a recommendation made by the EDPS in the framework of his prior-check Opinion regarding OLAF new investigative procedures of 3 February 2012. The Search Facility was indeed originally notified in the context of this prior-check procedure. In his Opinion, the EDPS concluded that he did not dispose of sufficient information to carry out an analysis of the new Search Facility database and therefore asked OLAF to submit a separate notification.

In the accompanying letter to the present notification, you stressed that, upon further reflection in the preparation of the notification, OLAF was of the opinion that a prior-check for this processing was not necessary because it fell within the scope of the notification concerning OLAF Intelligence Databases (the "2007 Notifications") (see EDPS Opinion of 21 November 2007, Joined Cases 2007-0027 and 2007-0028, hereinafter: the "2007 Opinion").

The Search facility is a new iBase database whose main purpose is to enable the authorised staff in charge of the selection of cases in the Investigation Selection and Review Unit (Unit 0.1) to perform electronic searches of a subset of data in OLAF's Case Management System (CMS) case files in order to verify whether the new information relates to an already existing case and avoid the opening duplicative cases on identical matters. The facility will search for cross-matches in the following data fields extracted from the "Organisation" and "Person" tabs of the CMS: name, involvement comment, organisation comment, address(es), contact(s), job(s), type of data subjects, alias, birthday, birth place, person comment, country, programme. The search results will point to documents where the searched data appears.

The database will contain the following documents: opinions on opening decision (initial assessment before 1 February 2012), 9 month reports, interim reports and final reports. The present facility is connected with the new investigative procedures, which have introduced a selection procedure for the evaluation of new information of potential investigative interest (see EDPS prior check Opinion of 3 February 2012 on cases 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132). Like other intelligence databases, the Search Facility may also be used by OLAF's analysts for the purposes and under the conditions set out in the 2007 Notifications and related Opinion. Unlike other intelligence databases, the access to the Search Facility database is granted also to members of the Unit 01 for case selection purposes.

The 2007 Notifications set out the conditions under which OLAF would process data for the purpose of intelligence/analysis and operational activity, and to support specific case requests, operations and investigations with a view to ensuring the optimum accuracy and relevance of information received, disseminated and otherwise processed for intelligence, financial, administrative, disciplinary and judicial use. The Intelligence Databases (iBase) were identified as one of the tools used by the Information and Intelligence Data Pool. Therefore, the IT tool used (iBase database) in the processing described in Joint cases 2007-0027 and 2007-0028, and the current notification, coincide. However, there are some differences. Joint cases 2007-0027 and 2007-0028 cover a broader scenario. The Search facility, on the contrary, is restricted essentially to verifying whether the new information relates to an already existing case and avoiding the opening duplicative cases on identical matters. Its content is specifically defined (opinions on opening decision (initial assessment before 1 February 2012), 9 month reports, interim reports and final reports).

Despite its more restricted scope and other differences (e.g. access granted to Unit 01), it nonetheless appears, on the basis of information available, that the Search Facility would indeed replicate the standard features of the intelligence databases, thereby falling within the scope of the corresponding notifications. The 2007 Notification described the standard structure, design, audit trail, management control and access rights of databases in the iBase environment rather than one individual database. As long as a new database corresponds to the characteristics enounced in that notification, the latter will be covered by the 2007 Notification, without a separate notification being necessary. In response to a specific request, OLAF has confirmed that the Search Facility complies with such standard features. Therefore, the observations and recommendations made in the EDPS 2007 Opinion are also applicable to this case, where appropriate.

In addition, it should be considered that the processing activity conducted with the help of the Search facility iBase database is part of the general processing activity described in case 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132 (more specifically, the "Selection phase"). This processing activity should therefore comply, as far as they are applicable, also with the observations and recommendations made in the context of the EDPS Opinion of 3 February 2012.

In view of the above, we consider that the present processing does not require a full prior-check, as it is already covered by the notifications regarding OLAF's Information and Intelligence Data Pool and Intelligence Databases, cases 2007-0027 and 2007-0028 and new OLAF's Investigative Procedures (internal investigations, external investigations, dismissed cases and incoming information of no investigative interest, coordination cases and implementation of OLAF recommendations), cases 2011-1127, 2011-1129, 2011-1130, 2011-1131, 2011-1132. We refer you to the recommendations issued in the final EDPS Opinions in these cases, which are applicable in general also to the present database. In particular, we recall the importance of ensuring data quality, necessity and proportionality in the use of the database on a case by case basis in relation with the specific needs of each inquiry.

As to the specific security measures applicable to the database, the EDPS would like to draw OLAF's attention on several elements:

- Security controls should be derived from an information risk analysis. Ideally, an Information Security Management System (ISMS) would pick up on the creation of a new system and would require a risk analysis to be performed, which in turn would help OLAF in defining all required technical and organisational security controls to implement.

- With regards to user management:
    - The EPDS understands that a directory service will be used to provide user authentication and that the user accounts will be reviewed once per year. Reviewing these user accounts is critical in ensuring that only authorised personnel has access to the system and thus these reviews must be planned and carefully managed.
    - Finally, the procedures for granting, modifying or removing access to this system should be clearly documented and communicated; reviews of these procedures should occur on a regular basis to ensure that sufficient security controls have been implemented and are effective.

- With regards to logging and monitoring:
    - Regular reviews of the directory service's logs should be carried out to detect attack attempts. Other security controls (such as Intrusion detection systems or Intrusion prevention systems (IDS/IPS)) could also be considered.
    - The iBase audit database and security database should be secured against loss of confidentiality and integrity, even from the administrators.
    - The iBase audit database should be managed in such a way that if its service is disrupted, no log information is lost.
    - A documented process should be implemented to ensure that the 3 year retention period for logs is enforced. Ideally, this should be implemented by automatic means (i.e. the system should automatically remove logs older than 3 years). Exceptions may occur for internal inquiry purposes and following a properly documented process.

- With regards to the initial historical extract of data necessary to create the iBase database mentioned in your notification, and subsequent imports of data in this iBase database:
    - Due care should be taken to ensure that any step, especially manual steps, is sufficiently controlled to detect errors (ensure data quality).
    - Any temporary copy of the data (even a partial copy) should be secured against loss of confidentiality and integrity, and should be destroyed as soon as it not useful any longer.

In case you need additional information in relation with the present processing, the EDPS staff is at your disposal to provide further assistance.

Yours sincerely,

(**signed**)

Giovanni BUTTARELLI