**Opinion on a notification for Prior Checking received from the Data Protection Officer of European Anti - Fraud Office on Identity and Access Control System**

Brussels, 7 April 2008 (Case 2007-0635)

## 1. Proceedings

On 17 October 2007, the European Data Protection Supervisor ("*EDPS*") received from the Data Protection Officer of the European Anti-Fraud Office ("*OLAF*") a notification for prior checking ("*the Notification*") regarding the data processing operations relating to the operation of an Identity and Access Control System.

On 6 December 2007, the EDPS made a request for additional information, which the OLAF Data Protection Officer ("*DPO*") answered on 17 March 2008.

On 27 March 2008, the EDPS sent the draft Opinion to the DPO of OLAF for comments which were received on 4 April 2008.

## 2. Examination of the matter

### 2.1. The facts

Context

The Identity and Access Control System is part of the security infrastructure that protects OLAF premises and IT systems which in turn support OLAF investigations and all other activities to protect the financial interests of the European Union.

OLAF's operational data is subject to the security requirements specified in Regulation (EC) N° 45/2001. Moreover, in some cases these data can be classified and corresponding additional EUCI security provisions must be applied. OLAF wants to handle EUCI up to SECRET UE. Very stringent confidentiality and security requirements apply to processing such data in this context.

The OLAF Information Security Policy (ISP), which has been developed in order to implement these security requirements within OLAF, requires a strong implementation of the Need-To-Know principle. This implies unequivocal identification, i.e. strong authentication, of any user of OLAF's operations data processing systems.

Three authentication factors are defined by the Commission's Information Systems SECurity POLicy (SECPOL): Authentication by Knowledge, by Ownership and by Characteristic. OLAF decided to implement a two-factor authentication scheme based on "Ownership" and "Characteristic". According to the document provided to the EDPS, OLAF adopted

fingerprints as the "Characteristic" authentication factor because it constitutes the best available compromise in terms of user-friendliness, reliability and cost. Other systems as hand-geometry, iris and retina characteristics were deemed more intrusive and/or more expensive. As "Ownership", OLAF uses a smartcard. Users' biometrics data are stored only on the smartcard and it cannot be used for any other purpose.

Purpose
The purpose of the Identity and Access Control System data processing is to ensure that only authorised persons have access to OLAF's premises.

Controller
The primary responsibility for the data processing lies within OLAF, in particular within the Information Services division which provides all data processing systems.

Processing
This system is designed to control the identity and permit or deny access of persons entering and exiting from OLAF's premises outside working hours and special secure zones. The system grants or denies access at all entrances into and exits from the OLAF physical security perimeter within the OLAF building, as well as the special protected zones such as the IT technical rooms and the OLAF Document Management Centre where operational information is handled, stored and archived.

Access to OLAF through the PNG's (i.e. the automated personal access gates located in the guarded lobby) will not require biometric authentication. The use of fingerprint authentication will be required at unguarded access points to OLAF and outside normal working hours, i.e., from 20.00 to 07.00 and during weekends. A glass door beyond the PNG's slides shut outside normal office hours, preventing unauthorised access to the OLAF lifts. Biometric access control is required to open that door, as well as all doors leading to OLAF from the stairwells.

The Access Control System consists of personal access cards issued to each member of OLAF staff, a number of card readers, access points, a central database server for storage of access rights and access logging, and a number of administrative workstations.

Visitors will be issued a generic badge and their personal data will therefore not be recorded in this system.

* The enrolment of a user consists of two independent processes:
a) The card's unique identification will be registered in the access control system and linked to a person in the database;
b) The person's fingerprints from three fingers will be scanned by the system and a digital template representing the fingerprints will be calculated by the system and stored on the card only, not in the database. OLAF does not plan using the card for any other purpose than Physical and IT access control.

* Technical specificities: The technology used in the personnel cards is Mifare with a passive component (the model used is the Mifare standard 4K, which was the standard currently recommended by the Commission Security Directorate when the OLAF security project started). The cards contain a unique identity number and three fingerprint templates for match on card biometric authentication. The reason for having three fingerprint templates is to allow the authentication through one of the three fingerprints templates stored on the card.

The biometric template is the data that represents an enrolled fingerprint. It consists of two parts; the biometric header, which contains data about type and version of the biometric algorithm used, and the reference data, which contains the actual fingerprint characteristics. The reference data are computed and stored on the card at user enrolment time. The biometric algorithm works only one-way, i.e. the scanned fingerprints can not be reconstructed from the reference data.

There are two types of card readers: the standard type, which reads the card number and has it verified by the access point controller, and the biometric reader type, which can scan a person's fingerprint and match it with one of those stored on the badge. If there is a match, the reader communicates the card ID to the access control system. Access will be granted or denied on the basis of authorisations programmed in the system for that badge.

The False Rejection Rate which is used in all parts of the building is set at 1:100. Moreover, ten tries per enrolled finger are possible before the system blocks the card.

The access point controllers hold a list of authorised card numbers for the zones defined in the system and will grant or deny access according to these lists. They also store and forward the access logs to the central database server.

The central database server is the administrative interface with the system. It stores information about the users and their access rights. It also stores any access attempts, granted or denied.

Data subjects
According to the notification form, the following individuals are data subjects: Each member of OLAF staff, including statutory staff, detached National Experts and intra-muros staff working for a continuous period of time in the OLAF premises.

Visitors and other Commission staff will be given a temporary pass - they will not be enrolled in the system.

Categories of data concerned
The following categories of personal data are concerned:

- Personal identification data (Name; Staff number; Picture)
- Card number
- Vetting information
- Finger prints (on personal identification card only)
- Access rights.

More specifically, the following data are logged by the Access Control System each time a badge is presented to a card reader. Where user (fingerprint) authentication is required, this information is logged only for successful attempts: Date; Time; Name; Access granted or denied; Access group name; Card reader number and description.

As concerns access rights, OLAF's security perimeter is divided in zones. The Access control system allows the definition of "Families". A family contains the list of protected zones and times where access is authorised by the system. Access rights to - and within - OLAF's secure premises is defined by users' membership to one family. Family membership is assigned by OLAF according to the function category of staff members.

Recipients of data

According to the notification and the privacy statement, the access control information is accessible to OLAF Security Managers only. In case of a security incident, this information might be shared with the Security Directorate of the Commission and/or IDOC.

Information given to data subjects

A privacy statement will be available on the OLAF intranet and the OLAF Europa site, and at the guard station at the entry of the OLAF premises, upon request.

The privacy statement contains the following elements: explanation of the OLAF Access Control System; the personal information collected, for what purpose and through which technical means; the recipients of the information and to whom it is disclosed; the protection and safeguards of the information; the retention period; the right of data subjects (access, modification, deletion) and finally the right to have recourse to the EDPS. The DPO included a draft of the privacy statement with the notification

Rights of data subjects

The rights of the data subject are explained in the privacy statement in the following terms: "*You have the right to access the personal data we hold regarding you and to correct and complete them. Any request for access, rectification, blocking and/or erasing your personal data should be directed to Mr [...], Head of Unit D.8 [e-mail]. You may also contact him in case of any difficulties, or for any question relating to the processing of your personal data. Exemptions under Article 20 (1)(a) and (b) of Regulation 45/2001 may apply*".

Moreover, the time limit to block data on justified legitimate request from the data subjects is established at 1 month.

Retention period

According to the notification and to the privacy statement, the recorded data (access control information) will be kept for no longer than 1 year. The specified retention period is necessary because not all security incidents are discovered immediately. OLAF believes that a one year total retention period is reasonable in the case of OLAF, given the sensitive nature of its operational business.

Automated/Manual processing

The automated processing operation consists of the reading of personal access card by standard/biometric card reader; the transmission of data from reader to access point controller; the controller's storage and forwarding of the access logs to a central database server and the storage of information by the central database server.

Regarding the manual processing, this will only happen in case of a security incident, in which case the security officer will log on to the access control database and retrieve the information as to who has entered or left OLAFs premises at a certain time.

Storage

The data is saved on a database on hard-disk and backup media. The storage of finger prints is made on personal identification cards.

Security measures

Security measures are implemented. In particular, finger prints are stored on personal identification card. (...).

In addition to the above, security measures are also taken in the enrolment phase which takes place within the Administration & Human Resources Unit. (...).

## 2.2. Legal aspects

### 2.2.1. Prior checking

This prior check Opinion relates to processing of personal information carried out by OLAF, in particular the Information Services Division to control the identity and permit or deny access of persons entering and exiting from OLAF's premises and special secure zones.

Regulation (EC) No 45/2001[1] applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*"[2]. For the reasons described below, all elements that trigger the application of the Regulation are present:

First, *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed. Second, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001, as well as manual data processing operations. Indeed, the personal data such as personal identification data, fingerprints are collected and undergo 'automatic processing', for example when the information service takes the templates of fingerprints. Finally, the processing is carried out by a Community body, in this case by the Anti - Fraud Office, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. The EDPS considers that the presence of some biometric data other than photographs alone, such as the case in point where biometric fingerprints are collected, presents specific risks to the rights and freedoms of data subjects. These views are mainly based on the nature of biometric data which are highly sensitive, due to some inherent characteristics of this type of data. For example, biometric data change irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. In addition to the highly sensitive nature of the data, the EDPS also notes that possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for data subjects. These risks justify the need for the data processing to be prior checked by the EDPS in order to verify that stringent safeguards have been implemented.

Since prior checking aims addressing situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. The current opinion constitutes a **true prior check**. Therefore, such processing should not be implemented until formal approval is granted by the EDPS

---

[1] Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data ("Regulation (EC) No 45/2001").

[2] See Article 3 of Regulation (EC) No 45/2001.

The notification was received on 17 October 2007. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 102 days to obtain additional information plus 8 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later 7 April 2008 (6 April being a Sunday).

### 2.2.2. Lawfulness of the processing

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

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking falls under Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed"*

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

* The **legal basis** for the processing is to be found in:

- Article 297 of the EC Treaty; Article 17 of the Staff Regulations;
- Regulation 1073/99 - Recitals 4, 17, 18; Articles 8, 11(1), 12(3);
- Commission Decision 1999/352: Recitals 4, 5; Article 3;
- Commission Decision 2001/844/EC, ECSC, Euratom (security provisions)
- Commission Decision 2006/3602/EC concerning security of information systems;
- Commission's IT security policy (PolSec);
- OLAF Information Security Policy (Section 4.5 of the OLAF Manual).

* Processing operations are carried out **in the legitimate exercise of official authority.** The EDPS notes that the Commission carries out the processing activities in the legitimate exercise of its official authority. Indeed, the processing operations are taking place in the framework of a mission carried out in the public interest on the basis of the Staff Regulations of the officials of the European Communities and the conditions of employment of other servants of the European Communities, as well as the OLAF Information Security Policy. The admissibility of the treatment is thus respected.

* As to the necessity of the processing **(necessity test),** according to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. In this respect, recital 27 states that: "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*".

OLAF's mission is the protection of the financial and other interests of the Community against fraud and irregular conduct liable to result in administrative or criminal proceedings.

Moreover, OLAF shall exercise the powers of the Commission in order to step up the fight against fraud, corruption and any other illegal activities detrimental to the Communities' financial interests[3].

Taking into account the relevance of these interests and in order to prevent the unauthorized access and disclosure of this sensitive information, OLAF could indeed find it necessary to adopt special security measures, including the setting up of stringent access control systems for specific areas of OLAF. Therefore, in the EDPS' view, the implementation of strong access control systems which entail the processing of personal data can in this case reasonably be considered as a necessary internal control measure towards the safeguard of financial information and other interests of the Community.

### 2.2.3. Processing of special categories of data

The notified data processing does not relate to data falling under the categories of data referred to in Article 10.1 of Regulation (EC) No 45/2001.

### 2.2.4. Data Quality

**Adequacy, relevance and proportionality**. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed. This is referred to as the data quality principle. In analysing whether the processing at issue here, which involves mainly the processing of biometric data, is in line with this principle, the EDPS notes the following:

As stated in the notification, each member of OLAF staff is considered a data subject. Further, the notification describes that the system is designed to control the identity and permit or deny access at all entrances into and exits from the OLAF physical security perimeter within the OLAF building outside working hours, as well as the special protected zones. As a consequence, each member of OLAF staff must carry an OLAF badge in order to be authorised to access the OLAF Secure Premises. The EDPS does not, however, see the need to enrol the fingerprints of each member of OLAF staff. Indeed, only those who may have to work outside working hours and those who need to access special protected areas of OLAF's building should have their fingerprints enrolled on the badge. Moreover, OLAF informed the EDPS of the reasons for using Biometrics in OLAF's specific security systems. The OLAF Information Security Policy (ISP), which has been developed in order to implement the security requirements within OLAF, requires a strong implementation of the Need-To-Know principle. This implies unequivocal identification, i.e. strong authentication, of any user of OLAF's operational data processing systems. In the context of OLAF's access control, the EDPS interprets this Need-To-Know principle as requesting that only the people who need special access should be enrolled in the system and therefore be fingerprinted. Therefore, based on the above elements, the EDPS recommends that OLAF reassesses and considers the possibility to restrain the list of people that will have to enrol their fingerprints, based on the real needs either to access OLAF outside normal office hours, or to access internal protected areas, or to use unguarded access points – staircases - to access the OLAF secure premises.

The type of data collected, mainly the fingerprint templates of three fingers and related identification information, corresponds to the data required to operate an access control system based on biometrics. From this point of view, the EDPS considers that the data collected are adequate and relevant for the purposes of the processing.

[3] OLAF Manual, p. 13.

OLAF adopted a combination of two out of the three[4] authentication factors of the Commission's SECPOL (authentication based on "Ownership" and on "Characteristic"). OLAF further explained that the security guarantees provided by combining Ownership and Characteristic were deemed sufficient to cover the OLAF Information Security Policy requirements.

The EDPS welcomes this practice and reasoning of OLAF. Indeed, taking into account the highly sensitive nature of the biometric data in order to properly assess the adequacy of the use of such data for access control purposes, it is necessary to carry out a ***targeted impact assessment,*** evaluating the reasons that justified the use of such technique and whether other, less privacy intrusive alternatives, were envisaged. However, vis-à-vis the future and particularly concerning possible updates of the system, OLAF, besides technical and security aspects, should also take privacy/data protection considerations into account while carrying out an impact assessment.

**Fairness and lawfulness**. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects, which is further addressed in Section 2.2.8.

**Accuracy**. According to Article 4(1)(d) of the Regulation, personal data must be "accurate and, where necessary, kept up to date", and "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified".

In this case, the personal data at stake include mainly biometric data, used for access control purposes. Some key features of biometric systems have a direct impact on the level of accuracy of the data generated either in the enrolment or identification phases inherent to this type of system. Depending on whether biometric system is set up in a way that integrates these key elements, the accuracy of the data will be (or not) at stake. Next we describe these key elements and analyse the extent to which they have been taken into account in the biometric system concerned.

Firstly, any enrolment phase must foresee alternative ways to identify individuals who are not eligible, even temporarily, for enrolment, for example because of damaged fingerprints. This is usually referred to as ***"fall back procedures"***[5]. According to the additional information provided, OLAF has not foreseen any Failure to Enrol Rate (FER), as it anticipates that all staff will be able to enrol. Moreover, should there be any staff members who for some reason are not able or willing to enrol, either temporarily or permanently, the procedure foreseen by OLAF is that they will be obliged only to access OLAF within the core working hours and only through the PNG (i.e. the automated personal access gates in a guarded lobby), which regulate access to the OLAF lifts. They will not be able to use staircases in order to access the OLAF security perimeter.

After analysis, the EDPS concludes that although OLAF is anticipating that all staff will be able to enrol, it has implemented a fallback procedure in the sense that three fingerprint

---

[4] The third authentication factor "Knowledge (either a password or a PIN code) was deemed inappropriate for OLAF's operational security requirements because it is too user-dependent.

[5] For a description of the data protection principles applicable in relation to fall back procedures, see Opinion of 13 October 2006 on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions, OJ C 313, 20.12.2006, p. 36.

templates, and not only one, are taken during the enrolment phase. During the biometrics authentication process, the user will place one of the three fingers that he/she had chosen at enrolment time. Although this solution diminishes the risk of failure to enrol, it is still possible that some people may temporarily not arrive to enrol through the fingerprint system. In this case, the EDPS suggests that OLAF could implement an alternative solution to the one proposed. This alternative solution could ensure that the person who access secured areas of the OLAF building is accompanied during his/her movements by a mandated person. Besides, if a case of permanent impossibility to enrol would occur, OLAF should develop a workable alternative solution.

Second, similar types of measures must be foreseen for those individuals who are properly enrolled but who are wrongly identified (usually referred to as "***false rejection***"). If these measures are not embedded in the architecture of the system, the accuracy of the information produced by the system may be compromised. In particular, in the case of false rejection, the system will produce a record that a given individual without proper access rights intended to access a secured area, when in fact the individual did have such rights. At the same time, because the individual will be misidentified, he/she will be denied a right (the right to access specific areas of OLAF or to access at specific times) to which he/she is entitled.

Regarding OLAF's access control system, the False Rejection Rate which is used in all parts of the building is set at 1:100, determined by the level of security expected within OLAF buildings. Moreover, ten tries per enrolled finger are possible before the system blocks the card. The EDPS considers that this solution should mitigate the risk of rejections However, in the case of a false rejection, the EDPS suggests OLAF developing a similar alternative measure to the one relating to the failure to enrol. Such procedure should address the problem in a way that does not put too much burden upon individuals. In other words, the alternative procedures should provide sufficiently simple solutions to the problem of misidentification and rejection.

Third, OLAF physical access control system is based on fingerprints templates stored in cards and which are combined with the use of readers. The OLAF physical access control system does not implement a 100% "match-on-card" authentication scheme. OLAF has implemented the use of "one to one" search mode whereby the biometric data are only compared to one template rather than being compared to a larger number of templates. The EDPS welcomes this system, which avoids further unlawful uses and phishing expeditions which often appear with the use of databases[6].

Finally, the EDPS wants to underline a last element about data quality. Biometrics, especially fingerprints may evolve with the life of a data subject. In order to ensure a high level of accuracy of the data, the EDPS suggests OLAF introducing a procedure through which OLAF's staff members will have to renew their enrolment at fixed times. The determination of an appropriate period shall be based on the type of population (i.e. the quality of the specificities of the data provided by the data subject) who has to renew his/her enrolment and on the frequency of use of the system.

### 2.2.5. Conservation of data/ Data retention

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that "*personal data must be kept in a form which permits identification of data subjects for no longer that is*

[6] See Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank related to the extension of a pre-existing access control system by an iris scan technology for high secure business areas, 14 February 2008 (2007-501).

*necessary for the purposes for which the data were collected or for which they were further processed". "The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted."*

According to the notification, recorded data (or access control information) will be kept for no longer than 1 year. The data are needed for investigating security incidents. As justification, OLAF mentions that the specified retention period is necessary because not all security incidents are discovered immediately. For example, some security investigations were triggered 2-3 years after the leak of a sensitive OLAF operational document. Therefore OLAF believes that a one year total retention period is reasonable in the case of OLAF, given the sensitive nature of its operational business.

The EDPS considers that timing is a key element in the discovery of security incidents. Indeed, the more sensitive a system is, the earlier the detection of security incidents has to take place. The EDPS understands that it may be necessary to keep an audit trail of the registering data for a period of time which allows reconstructing events during security related incidents and that in the case of OLAF, it may not be practical to have a very short period. The EDPS assumes that OLAF has in place or, if not, should develop a process of identifying and responding to incidents so that they are detected and reported as soon as possible after they have occurred. Presumably OLAF aims at discovering incidents immediately after they take place and in any case no later than several months after they occurred. Based on the foregoing, the EDPS feels that the period of one year is a little long and invites OLAF to reconsider the setting of its conservation period by reassessing the need to shorten this time by using the statistics of incidents. Therefore, the storage period should be determined by the time it usually takes for OLAF to discover a security incident from the moment that it took place. The EDPS understands that OLAF does not have such statistics on incidents but that it will be able to re-evaluate the initial retention period after one year of operation of its new system. Therefore, the EDPS agrees that OLAF proposes a new retention period on the basis of statistics available by then.

As regards the time limit to block/erase data on justified legitimate request from the data subjects, it is set at one month. The EDPS considers that this retention period complies with the requirements set in Article 4(1)(e) of the Regulation

The EDPS understands from the notification that no statistics on personal data are allowed after the retention period. Nevertheless, the EDPS would emphasise that where such data are used beyond the retention period, they must be made anonymous (Article 4(1)(e) of the Regulation).

### 2.2.6. Transfer of data

According to the notification, the access control information is accessible to OLAF Security Managers only. In case of a security incident, this information might be shared with the Security Directorate of the Commission and/or IDOC. Therefore, information may be transferred within the Commission in case of a security enquiry, but in no circumstances will the data be transferred outside the Commission. Article 7 of Regulation (EC) No 45/2001, which sets forth certain obligations applying when data controllers transfer personal data to Community institutions or bodies, will therefore apply.

The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data be transferred if it is "*necessary for the legitimate performance of tasks covered by the*

*competence of the recipient"*. In order to comply with this provision, in sending personal data, OLAF must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. Whether a given transfer meets such requirements will have to be assessed on a case by case basis. In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted.

### 2.2.7. Processing of personal number or unique identifier

Article 10(6) of the Regulation provides that "*the European Data Protection Supervisor shall determine the conditions under which a personal number of other identifier of general application may be processed by the Community institution or body"*. The present opinion will not establish the general conditions of such a use of a personal number, but consider the specific measures necessary in the context of an "Access Control" system.

The EDPS already clarified, in a previous prior-checking opinion[7], the status of an embedded RFID chip number in a card. The identification number associated to the RFID chip is personal data covered by Regulation 45/2001. Indeed, this identification number when used to record a staff member's behaviour and linked to the personnel number (which means linked to the name of a person, as is the case here), makes this a processing of personal data, which requires compliance with the data protection principles.

The use of the personal number is necessary because the card ID is communicated to the access control system. The access point controllers hold a list of authorised card numbers for the zones defined in the system and will grant or deny access according to these lists. They also store and forward the access logs to the central database server.

For the case in hand, the use of the staff personnel number for the purpose of verifying the access right data in the system is reasonable considering that this number is used to identify the person in the system and thus helps ensure that the data are accurate.

### 2.2.8. Right of access and rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

The prior checking notification and the supplementary information submitted by the controller describe the possibility of access to and mention the possibility of rectification of personal data by a staff member.

According to the prior checking notification and the supplementary information notice submitted by the controller, the rights of access and rectification are recognized. The privacy statement which was submitted to the EDPS for review provides the name of the person responsible for the execution of these rights. The EDPS recalls that these rights apply not only to the information provided by the individual (identification information and fingerprint

[7] See Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "the implementation of flexitime - specific to DG INFSO", 19 October 2007 (2007-218).

templates) but also to the information generated every time an individual accesses a highly secured zone.

The EDPS notes that, according to the notification, Article 20 of Regulation 45/2001 is not to be applied, in principle, in the context of this data processing operation.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met.

### 2.2.9. Information to the data subject

Articles 11 and 12 of Regulation (EC) 45/2001 list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information.

The latter are applicable insofar as, taking into account the particular circumstances of the treatment in question, they are necessary in order to ensure a fair data processing with regard to the data subject. In this case, part of the data is collected directly from the data subject and another part from other people.

Article 11 (*Information to be supplied where the data have been obtained from the data subject)* should be observed in the present case. Staff members will personally click in and out in the system, thus data subjects provide the data themselves.

Article 12 (*Information to be supplied where the data have not been obtained from the data subject)* should also be observed as the list of identification information is retrieved from SYSPER2 about OLAF staff members.

Data subjects are informed by a "*privacy statement for access control at OLAF*". In order to show compliance with these articles, a copy of the privacy statement was provided to the EDPS.

The privacy statement contains information on the purposes of the processing and how the data are processed, the conditions for the exercise of the right of access and rectification, the time limits for storing the data and the possibility to have recourse to the EDPS. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation. However, he considers that some amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

- Mention the legal basis of the processing operation for which the data are intended;
- Mention whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply (for instance, the consequences of failure to enrol). By analogy with a questionnaire, the staff should be informed of the practical consequences to enrol and of failure to do so;

Besides, the privacy statement is supposed to be provided to individuals who undergo an enrolment phase in order to access OLAF physical security perimeter. In another prior-checking analysis[8], the EDPS acknowledged the procedure implemented at the ECB (i.e. "*the privacy statement will be provided in paper and individuals will be asked to sign it stating that they have read and understood the statement*"). The EDPS considers that this is an

[8] See Opinion on the European Central Band access control (2007-501).

appropriate method of providing the information and suggests that a copy of the privacy statement be given to individuals so that they can go back to the privacy statement in case, for example, they want to know how to exercise their rights or how the data processing takes place.

### 2.2.10. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing. The technical and organizational measures appear to be suitable in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected.

The system developed by OLAF bases its technology choice on the Security Directorate's recommendations. This implies that a technological choice on the combination cards/readers had to be made for the system which was developed. The EDPS has not been invited to participate in the discussions and choices leading to the selection of the technology[9].

The EDPS regrets it, as he estimates that other solutions could have been explored in terms of security and encryption, which would have further reinforced the level of data protection and security present in the cards and readers. To that effect, the EDPS recommends that OLAF reconsiders its decision taken in terms of technological choices through a new assessment, including a viable timetable to implement the change of technology, taking into consideration the choice of the best available techniques[10] and the context of current discussions on future security systems.

**Conclusion:**

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, OLAF should:

- Reassess and consider the possibility to restrain the list of people that will have to enrol their fingerprints onto the badge;
- Take, besides security aspects, privacy/data protection considerations into account while carrying future impact assessments;
- Develop fallback procedures which take into account the temporary impossibility of staff to be fingerprinted at the enrolment phase and develop alternative measures to deal with false rejections;
- Introduce a procedure through which OLAF's staff members will have to renew their enrolment at fixed time;

[9] The EDPS made the same remark in the Flexitime for DG INFSO in case 2008-0218.

[10] This concept of Best Available Techniques has been promoted by the EDPS in his annual report 2006. Moreover, the EDPS remains available to provide guidance on possible alternate technological choices in the future.

- Reconsider the setting of the conservation period of data after the first year of operation of the new system;
- In the case of future data transfers, ensure that notices are sent to Community institutions receiving data processed in the context of the fingerprint system informing that the personal data can only be processed for the purposes for which they were transmitted;
- Amend the privacy statement as recommended in this Opinion and ensure that a copy of the privacy statement is given to individuals or that it is made available to them in a way that allows them to consult it;
- Reconsider its decision taken in terms of technological choices through a new assessment taking into consideration the choice of the best available techniques and discussions on future security systems.

Done at Brussels, 7 April 2008

(signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor