Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Commission Physical Access Control System (PACS): PSG Projet de Sécurisation Globale"

Brussels, 8 September 2011 (Case 2010-0427)

1. Proceedings

On 3 June 2010, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data in the context of the Commission Physical Access Control (PACs) from the Data Protection Officer (**DPO**) of the European Commission.

The EDPS also received relevant documents associated with this notification, which were made available on the intranet of the Commission, namely:

1. "Projet de Sécurisation Globale" (PSG) Vision Document
2. PSG Architecture Document
3. PSG Technological Options and Recommendations Report
4. PSG Physical Access Control Use Cases and Data Processing Scenarios
5. PSG IS and Applications
6. Recipients of the Processing
7. Time Limit to Block/ Erase Data
8. Information to Visitors
9. Information for New Badge Holders.

In the framework of the PSG, the setting-up of a pre-production site was considered required for the correct validation and fine-tuning of the various proposed technological options, systems and measures envisaged for the implementation of the new Physical Access Control System (PACS) within the European Commission. In accordance with his practice of prior-checking of pilot projects, the EDPS has established a procedure for pilot project/pre-production relating to new technological processing operations and this procedure was followed by the Commission.

In this latter procedure, the EDPS had requested the European Commission to provide specific information about the pre-production phase and he analysed the processing operations. In a letter dated 21 October 2010, before the launch of the pre-production phase, the EDPS provided recommendations that were specific to the pilot project. The EDPS also provided recommendations to be taken into account for the full launch of the system, in order to avoid any contradiction between the two phases (pilot phase and full launch of the system) that could have an impact on the protection of personal data.

This pre-production phase was conducted from November 2010 until May 2011 and the results were provided by the data controller to the EDPS on 1 July 2011.

At this time, the DPO provided the EDPS with two additional documents:

-a pre-production site evaluation report;
-the modified PSG-physical access control use cases (scenarios) and data processing scenarios, which reflects the adopted modifications following the end of the pre-production phase.

The conclusions of the pre-production phase were summarized in the report by the data controller who states that "*globally all the foreseen options and technologies have been validated and considered adequate for the intended purpose and delivering the required functionalities, as it was planned and designed. Mainly the major adaptations that had to be or will be made are placed at operations or operational procedure level*".

After the end of the pre-production phase, the PACS continued to be operational in the building which was used as pre-production site (L-56), respecting the conditions set for its implementation (information, conservation, etc).

The current prior-check Opinion concludes the legal analysis of the PACS. The aim is to go for full deployment of the PACS at the beginning of 2012 in the European Commission services in Brussels.

The EDPS notes that the European Commission has developed a privacy friendly approach to the implementation of the processing operations at stake by involving the EDPS at a very early stage of the notification procedure, by developing a pilot project phase and by considering all relevant data protection aspects at an early stage of its work.

The draft Opinion was sent to the DPO for comments on 29 July 2011. The EDPS received a reply on 6 September 2011.

2. The facts

The system aims at the implementation of a unique and coherent physical access control for the whole Commission, by performing all the required physical security functions. The system is a distributed PACS exclusively operating for physical access control and related security functions.

More specifically, it aims at physical access control automation and uniform enforcement of procedures and security policies. To that end the following objectives and technological solutions are implemented:

-a central IT access control system to operate and manage all physical access control functions and access rights definitions, allowing in particular:

- uniform and common production of badges and access rights definitions;
- central access control definition, monitoring and intrusion detection;
- central monitoring of assets based on standard technologies and common policies;
- central management and configuration of access control terminal equipments;

-a common badge or ID card supplying efficient and standardized technologies, based on:

- a contactless proximity chip, exploiting a Radio Frequency IDentification (RFID) technology fully compliant with the ISO/IEC 14443 Type A international standard;
- a biometric verification based on fingerprint minutiae, stored exclusively on the chip internal memory;
- a distributed set of physical security equipments (e.g.: door and gates controllers, intrusion detection and prevention systems, monitoring devices, CCTV, etc.).

The system's functions and operations are described in the "PSG Vision Document" and a detailed description of the system's use cases and data processing scenarios is given in the document "Physical Access Control Use Cases and Data Processing Scenarios", which was updated at the end of the pre-production site.

As described in the notification, the **purposes** of the processing operations are the following:

1. control and protection of Commission premises, information and assets;
2. security and protection of persons present inside Commission premises;
3. compliance with safety requirements. Knowledge of the most accurate number of persons still present inside premises is required for evacuation and other emergency situations;
4. compliance with legal requirements. The prevention, investigation, detection and prosecution of disciplinary or administrative violations or criminal offences (processing is strictly based on data collection and subsequent handover of such data to the competent Commission bodies).

Little or no **manual** data processing is planned. However, some use of legal or ID documents by receptionists and operators, possible exceptions upon system unavailability and indispensable human interventions could lead to some manual data processing.

The legal basis of the processing operations is to be found, according to the notification, in the following legal acts:

1. Commission Communication concerning the new access-control and security system for Commission buildings C(2007)797 of 14 March 2007;
2. Commission Decision on tasks and responsibilities of the Security Office C (94)2129 of 08 September 1994;
3. Commission responsibility on protection of its staff (security and safety) and assets: Commission Decision on alert states and crisis management 2007/65/EC of 15 December 2006;
4. Commission provisions on security: Commission Decision amending its internal Rules of procedure 2001/844/EC, ECSC, Euratom of 29 November 2001.

In the light of the purposes described above, the **data subjects** concerned are every person[1] having or requesting access to Commission premises.

[1] The following main categories are enumerated:
1. Commission staff (officials or equivalent personnel);
2. staff of external organizations or companies with whom the Commission has specific contracts;
3. National Detached Experts (NDE/END; experts from Members States or other countries);
4. staff from other European Institutions or bodies;
5. visitors;
6. Commission staff family members;
7. Commission retired staff.

Data subjects will receive at least one badge of the two categories: personal badge giving access (access badge) and if applicable a role badge not giving access but identifying a specific role:

1. access badge (with different layouts based on data subject category)-badge permitting access based on the person's specific access rights,
2. function or role badges (with different layouts based on data subject role)-badge not allowing access but used to identify specific roles (e.g.: security staff, safety staff, etc.)[2].

According to the notification, the following **data fields** will be processed (if and when applicable):

full name*; birth date*; photograph; nationality*; personal number (unique identifier: personal number for Commission staff and internal DB number for other people)*; gender*; fingerprint minutiae; link type with the Commission: official, temporary agent, contractor, visitor, contractual agent, retired staff, staff family member, etc.*; current working status: active, detached, long term absence, etc.*; place of work*; DG attached to*; office and tel/fax number(s)*; e-mail*; contract number and contract end date*; identity document number and dates; access rights; roles associated with system privileges and tasks; employer contacts for subcontractors*; car plate number; specific data related with roles within the Commission: press, diplomatic representation, security officer, safety officer, etc.*; access point traversal information: badge number, date, time, direction, alarms and video captures if any, etc.; data related with guards and guard patrols tasks execution and operations: presence or inspection at specific control checkpoints, security equipments operations (e.g.: X-ray devices) conforming with requirements; video images taken by the associated video surveillance system [3].

Not all data fields are processed or retained for each data subject. Fields processed or recorded are directly related to the kind of link the data subject has with the Commission or the reason for presence in Commission premises.

All the above mentioned data fall within the following main categories of data: identification data; transit data; equipments data; security profile data; system data and barring data.

1. Identification data: mainly, data related to data subject identity and administrative situation (including name, personal number, photo, badge number, telephone number, office address, e-mail address, identity card/password number, fingerprint minutiae);
2. transit data: mainly, data related to access control checks and events/alarms generated by the use of the system by data subjects (including badge number, date/time of access control points traversal and checking, system alarms associated with usage incidents, badges present on a specific zone and video files);

---

8. accredited persons (press representatives and technicians, Member States representatives or other diplomatic representatives having received a formal accreditation from the appropriate Commission services);
9. Commission trainees;
10. others- any other person not covered in any of the above mentioned categories and requiring or requesting access to Commission premises.

[2] Access rights are assigned based on data subject categories and access needs as defined on the applicable Commission physical access security policies.

[3] Data with (*): the data source is Sysper2/Comref for Commission staff or equivalent, ORIANA for external personnel and e-Pass for visitors. All other data are generated or collected directly by the system.

3. equipments data: mainly, data related to security equipments deployed (including system names, IP addresses, locations and software versions);
4. security profiles data: mainly, data related to security groups definition and membership, generic and specific access rights, standard and non standard access times, allowed access times, security roles;
5. system data: mainly, data related to systems management (including defined system user and roles, system logs, audit trail, access time for interactive users, if applicable);
6. barring data: data identifying data subjects to whom physical access to some or all Commission premises has been barred for some period of time. This list contains only the following data fields: data subject full name, identification number (internal ID number, identity card number or any other available), barred premises, barring starting and ending date.

The **biometric enrolment** is made on voluntary basis and mainly used to facilitate access to premises outside of normal working hours and for restricted or sensitive zones access (e.g.: computer rooms, communications configuration rooms). In some very specify circumstances based on particular security conditions (e.g.: high alert states, classified zones access, etc.), biometric verification may be made mandatory and will be evaluated and implemented on a case by case assessment.

For resilience and user comfort reasons two fingers are always enrolled, preferably one from each hand. The two indexes or middle fingers are proposed for enrolment, but the user can decide on the fingers to enrol.

The verification procedure mainly consists of a 1:1 (one to one) verification process – minutiae stored in the holder's card matched (verified) with the minutiae scanned, on the spot, by the biometric reader/scanner. The verification comparison is performed locally by the biometric reader device– *match on reader*.

The various **recipients** of the data processing can be grouped on the following main categories:
- system administrators (HR.DS.4[4]);
- system operators (HR.DS.4);
- security & safety operators (HR.DS.RA, HR.DS.1, HR.DS.2, HR.DS.4, HR.DS.6);
- internal or external investigation agents (Official investigators: HR.DS.RA, HR.DS.1, HR.IDOC, OLAF, EDPS, ECJ);
- access rights and profiles managers;
- validators (people using the system to access Commission premises)[5];
- IT application(s) (currently SYSPER: data subject photography can be transferred if request by the data subject);
- request validation officers (HR.DS.4, HR.DS.6, DG COMM, Chefs d'immeuble);
- local operators (LSO, etc.).

As to the **conservation regime**, the notification states that the following retention policy will be implemented for the defined data categories:

[4] Directorate General for Human Resources and Security, Security Directorate, Physical Security.

[5] The first version of the notification mentioned "end-users" as recipients. As further clarified by the data controller, in the context of the notification, these end-users are to be considered as users that use or interact with the system IT interfaces as normal IT end-users. This is the case when validating or visualising visits requests by internal users. These users have access to data inserted by the visitors about themselves and their visits, hence the name was changed to validators.

1. identification data: data retention set to be until termination of the link between the data subject and the Commission plus 6 months and will vary based on the type of link (e.g.: staff member: end of contract plus 6 months, visitor: end of visit plus 6 months, etc.);
2. transit data: data retention set to 6 months (it includes video data, to allow the link with other transit data);
3. security profiles data: data retention is indefinite (data will be retained until required for the proper operations of the system)[6];
4. system data: data retention set to 1 year;
5. barring data (persons on an exclusion list): data retention is under the responsibility of the Commission responsible authority (i.e. the authority which decided on the exclusion). Data in this category is completely removed from the system following appropriate authorisation from the Commission responsible authority.

Data older than the defined retention periods will be:
1. copied to an alternate system to be made anonymous and aggregated for statistical purposed, if considered useful: data warehouse, or
2. fully wiped from the IT operational systems.

Regarding the anonymisation of the data, mainly the anonymization is embedded in the process according to the following procedure:

a. every month the data warehouse system connects to the operational data base;
b. the running process selects the various data sets (e.g.: badge production, passing controls, persons known, etc.) older than the retention period;
c. performs the required calculations for aggregation (e.g.: how many passes, how many passes per day/hour/month, how many access denials, how many badge refusals, how many printed badges, etc.) on the selected data sets;
d. inserts the calculated values on the data warehouse data base;
e. after this processing all selected data (older than retention period) are deleted from the operational data base.

Data retention periods and procedures apply to any data collected about any data subject accessing or registering to have access to Commission premises covered by the system.

Particular cases:
1. data retained in the local door controllers are stored for less than one week until transferred to the central system or overwritten in a round-robin mode;
2. on enrolment stations, fingerprint images and minutiae are temporarily stored on memory or swap space. Temporary storage space will be cleaned at start-up.

[6] Security profiles data seem not to be personal data. They are described as mainly group sets of entrances, access periods or access permissions required by the system to manage access permissions and time schedules. This can be compared to access groups and associated permissions defined on IT systems to allow access to files and resources. Typical groups are:

a. ALL-BXL-BUILDINGS-Entrances–a group containing all main entrances existing in Brussels buildings;
b. ACCESS-24h-7d–a group allowing access at any time;
c. ACCESS-08-20-WeekDays–a group allowing access only during normal working hours;
d. Specific-Zone-ClassII–a group containing all main entry points (entrances) allowing access to the specific zone;
e. etc.

This is permanent system data and this is why there is no retention period defined beforehand. These groups are kept as long as required (almost forever) after creation. When badges (identifiers) are associated with these groups the normal retention period applies to the associate badge data and the data subject data, if no badges are associated (empty group) then no link with personal data exists.

3. Fingerprint minutiae (if used) are stored on the data subject RFID chip embedded on badge, for the entire badge validity period (foreseen for 10 years).

As to the **rights** of the data subjects, the notification states that data subjects are informed of their rights, available contact points, communication channels and procedures in place as described on the document and information sources enumerated above.

Regarding persons included on the exclusion list (barring data), they are informed by the Commission authority (Security Directorate, IDOC or Medical Service) responsible for the exclusion. On this aspect, the controller of the access control processing has no information on the reasons or duration of the exclusion of a data subject and acts on behalf of the Commission authority when processing these data. Following the request of the Director of the Security Directorate it updates the list and activates or deactivates the exclusions as requested. The EDPS underlines that this exclusion procedure is not part of the currently analysed notification.

As to the **information** which is provided, the following documents are provided:
- a specific information leaflet (or equivalent) is addressed to new badge holders and made available at badge delivery time ("Information for New Badge Holders");
- a specific information leaflet (or equivalent) is addressed to visitors and made available at buildings receptions ("Information to Visitors");
- affixed notification panels at RFID reading zones, mainly building entrance zones, for awareness purposes (the information content as presented in Annex II of the "PSG Technological Options and Recommendations Report" is foreseen);
- affixed notification panels at video recording zones, mainly building entrance zones;
- on the Security Directorate Intranet web pages, information equivalent to the leaflet for new staff as described above;
- on Europa web pages and when global Internet registration forms will be made available, information equivalent to the leaflet for visitors as described above;
- appropriate information and advice on personal data processing requirements available on the front page or relevant web pages of the user/operators web interfaces of the specific system under deployment;
- in case of inquiry requiring access to the physical access control systems data, the person is always informed in accordance with the rules which govern the inquiries and by the service in charge of the inquiry.

As regards the **storage of data,** the notification describes the following rules.

All operational or active data will be stored on dedicated clustered servers with dedicated data storage (disks). The systems will be hosted in the Commission Data Centres.

Personal data when moved outside the main systems (e.g. backups) will be encrypted before transfer. Backups will be made to central tape systems in the Commission Data Centres.

For BCP (Business Continuity Planning) reasons and to cope with possible central servers' unavailability an encrypted data set will be copied to dedicated servers hosted in the Security Directorate computer room.

Transitional storage of data by infrastructure servers is foreseen for transmission or temporary processing requirements. Mainly e-mail transmission (servers hopping), collected data from external websites before transmissions, data typed by data subject on automated registration and badge delivery kiosk machines, optical ID document reading, etc.

Each local security equipment (door controller, key boxes, IP cameras, monitoring or reception desk PCs, etc.) enforcing access control or used for monitoring contains a copy of the required access permissions stored on its local storage. These equipments are physically isolated and protected from public access. Only authorized personal can manipulate the stored data.

Fingerprint minutiae will be stored exclusively on the data subject badge chip after enrolment and enrolment will be made on a dedicated system. When fingerprint is used for access control, verification (1:1) is made at badge reader level by comparing the contents of the badge and the fingerprint which has just been read, no local or central storage is performed.

Various **security measures** are foreseen in the notification:

[...]

3. Legal analysis

3.1. Prior checking

Applicability of Regulation No 45/2001 ("the Regulation"): This prior check Opinion relates to processing of personal information carried out by the European Commission, in particular the Security Directorate.

Regulation (EC) No 45/2001 applies to the *"processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system*" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*"[7]. 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 including 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 an institution, in this case, the European Commission, in the exercise of activities which fall within the scope of EU law (Article 3(1) of the Regulation).

Grounds for prior checking*:* 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[8] that the presence and processing 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

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

[8] See also cases 2007-635 of 7 April 2008 and 2008-223 of 30 June 2008, available on the EDPS website.

subject to further use. 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.

Besides, the EDPS considers that in some specific cases, the inclusion of the RFID technology (the RFID chip embedded in the badge) into an access control system creates specific risks. Therefore, the current prior checking falls under Article 27(1) of the Regulation.

Moreover, as already mentioned above, the EDPS considers that the procedure relating to investigations as well as exclusions is not part of the scope of this prior-checking notification.

Deadlines*:* 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 qualifies for **prior check**. Therefore, such processing should not be implemented until formal approval is granted by the EDPS.

The notification was received on 3 June 2010. 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 355 days to obtain additional information and during the period of the pre-production site, plus 39 days to allow comments on the draft Opinion. The Opinion must therefore be adopted no later 13 September 2011.

3.2. Lawfulness of the processing

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

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 [...]"*. In interpreting Article 5(a), 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*".

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). The three requirements are closely related.

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

- Commission Communication concerning the new access-control and security system for Commission buildings C (2007)797 of 14 March 2007;
- Commission Decision on tasks and responsibilities of the Security Office C (94)2129 of 08 September 1994;
- Commission responsibility on protection of its staff (security and safety) and assets Commission Decision on alert states and crisis management 2007/65/EC of 15 December 2006;

- Commission provisions on security Commission Decision amending its internal Rules of procedure 2001/844/EC, ECSC, Euratom of 29 November 2001.

* 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 on the basis of the above mentioned legal acts taken on the basis of the staff Regulations.

* 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 of Regulation (EC) No 45/2001 states that the "*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*".

In this respect, the processing operations aim at the physical protection of Commission staff, information and assets, safety conditions for working personnel (including evacuation and emergency situations), visitors and access control to Commission property.

Taking into account the relevance of these interests, the European Commission could indeed find it necessary to adopt special security measures, including the setting up of stringent access control systems and to allow investigation of security incidents by IDOC or 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 information and other interests of the EU.

3.3. 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.

The EDPS analysed the data fields which will be processed (if and when applicable) and concludes that the current list of data fields complies with Regulation (EC) No 45/2001. It is also specified that not all data fields are processed or retained for each data subject. Fields processed or recorded are directly related to the kind of link the data subject has with the Commission or the reason for presence.

As regards biometric data, the EDPS notes that only the people who need special access will be enrolled in the system and therefore be fingerprinted. Moreover, for resilience and user comfort reasons two fingers are always enrolled, preferably one from each hand. The two indexes or middle fingers are proposed for enrolment, but the user can decide on the fingers to enrol. The type of data collected, mainly the fingerprint templates of two 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 notes that the data collected could be considered adequate and relevant for the purposes of the processing.

The use of fingerprint minutiae verification as biometric validation method could be considered adequate.

The verification procedure mainly consists of a 1:1 (one to one) verification process – minutiae stored in the holder's card matched (verified) with the minutiae scanned, on the spot, by the biometric reader/scanner. The verification comparison is performed locally by the biometric reader device– *match on reader*. The EDPS considers this verification more privacy friendly than when the comparison is performed against references in a database.

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 2.2.9.

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 the case at hand, the personal data at stake include 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 the biometric system is set up in a way that integrates these key elements, the accuracy of the data will (or not) be at stake. The EDPS has analysed in previous opinions relating to access control the rules to be followed when implementing biometric systems[9]. The following analysis describes these key elements and analyse the extent to which they have been taken into account in the biometric IT access control system concerned.

First, 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"***[10].

Regarding the enrolment phase itself, following the pre-production phase, the data controller decided to include in the enrolment procedure a verification of each of the enrolled fingerprints before finalisation and badge delivery, to minimize the probability of later refusal–*false rejection.* According to the Commission, this verification step associated with the finger scanning quality metrics, that any professional enrolment software provides, creates the conditions to minimize any later refusal.

Furthermore, following the pre-production phase, if biometric data is not available or biometric verification is not possible, at a specific verification time, the following *fallback solution(s)* will be made available based on the particular case and on the specific access control verification conditions:

1. facial recognition of the badge holder by a trusted individual (e.g.: control room operator, security personnel, zone/area responsible person, etc.) done remotely or locally and able to allow access;
2. gor access to less sensitive zones the use of a specific secret PIN code can be proposed instead of biometric fingerprint minutiae verification.

[9] See for instance cases 2007-0635 and 2008-0223 on OLAF access control (Physical and Logical).

[10]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.

The EDPS considers that these fallback procedures are satisfactory but he reminds the Commission that these measures have to take into account the level of security risk of the building and should also preserve the rights of the data subject(s) concerned.

Moreover, in the case of a false rejection, the EDPS suggests that the Commission develops a procedure which should address the problem in a way that does not put too much burden upon individuals. In other words, the alternative procedure should provide sufficiently simple solutions to the problem of misidentification and rejection. In this respect, the EDPS would like that the Commission establishes a periodical renewal of enrolment in order to maintain a high level of data quality. The establishment of a renewal period is justified, for instance, because biometrics, especially fingerprints may evolve with the life of a data subject. It is also justified by the possible change in the skin condition of relevant finger of the user over the time, as well as by the quality of the enrolled fingerprint template. This renewal period could be defined and implemented after 2 years of operation of the new system, on the basis of the experience faced by the Commission with the system.

Finally, the minutiae will be stored in the chip internal memory only, as initially announced, and the verification process –minutiae match, 1:1 verification– will be performed locally by the biometric reader. The EDPS welcomes this system, which avoids further unlawful uses and phishing expeditions which often appear with the use of databases[11].

3.4. Conservation of data/ Data retention

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed. This is usually referred to as 'conservation principle'.

The Commission states that the retention period foreseen about the identification data is 6 months and that the retention for system data is foreseen for one year:

- regarding identification data, the EDPS notes that the duration period established in the light of Article 4 of Regulation (EC) No 45/2001 as long as the retention periods for the different categories of data could be considered justified.

- regarding the conservation of system data, the EDPS understands that these data represent the access logs. On this aspect, the EDPS considers that the European Commission should evaluate after one year of use of the system the necessity of keeping the data for this period and adapt the period if needed. In other cases analysed[12], the EDPS considered that a conservation of three months could be considered as reasonable.

Moreover, the fingerprint minutiae (if used) are permanently stored on the data subject RFID chip embedded on badge, for the badge validity period (foreseen for 10 years). The EDPS agree with this conservation period.

3.5. Transfer of data

[11] 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) available on the EDPS website.
[12] See above OLAF cases.

According to the notification and the document "Recipients of the Processing", various recipients within DG HR DS may have access to the data. Also investigators, either internal or external to DG HR DS may also have access to the data in the course of their investigations (IDOC, OLAF, EDPS, ECJ).

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, HR DS must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. The EDPS considers that this is the case for reporting security incidents in this instance. However, 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.

No further transfers of data according to articles 8 or 9 are foreseen. However, it is possible that disclosure to national law enforcement agencies shall take place, in case of crime prevention or investigations. In such case, the EDPS underlines that Article 8 of Regulation (EC) No 45/2001 requires that personal data shall only be transferred if *"(a) the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or (b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"*.

The EDPS reminds the Commission that such analysis should be conducted on a case by case basis.

Finally, according to the information provided, there is no transfer to third countries.

3.6. 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 or 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 the PACS.

The EDPS has already clarified, in a previous prior-checking Opinion[13], 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 (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. 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

[13] 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).

number is used to identify the person in the system and thus helps ensure that the data are accurate.

3.7. 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 notification states that data subjects are informed of their rights, available contact points, communication channels and procedures in place as described on the documents and information sources enumerated above (see point 2 the Facts). Furthermore, on the basis of the information provided, the European Commission seems to correctly implement the rights of the data subjects, in the light of Regulation (EC) No 45/2001.

The data controller also provided the EDPS with the PSG time limit to block/erase data and defined data categories document. This document presents the foreseen data categories and details the global block/erase policy on justified legitimate requests from the data subjects.

Should Article 20 be applied (as is foreseen in the case of investigations), the EDPS reminds the Commission that it should be applied restrictively and on a case by case basis.

In conclusion, the EDPS considers that the conditions of Articles 13 and 14 of the Regulation are met subject to practical implementation on a case by case basis.

3.8. Information to the data subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The European Commission provided the EDPS with the privacy statement to data subjects who will use the PACS. This privacy statement is made available on the intranet and will be distributed to the holders of the new badges.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001.

The EDPS concludes that the privacy statement contains the elements foreseen by article 11 and 12 of Regulation (EC) 45/2001.

3.9. Security measures

According to Article 22 of the Regulation, the controller must implement the appropriate technical and organisational 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 to prevent all other forms of unlawful processing.

[...]

The notification also foresees that a full IT risk assessment will be performed and appropriate security controls and mitigation measures implemented. It also foresees that any residual risk will be documented and formally accepted by the data controller and data processor. The EDPS expects to have access to the results of the risk assessment conducted.

On the basis of the available information, the EDPS does not see any indication to believe that the European Commission has not applied the security measures required in Article 22 of the Regulation, but invites it to provide the EDPS with the above mentioned documents.

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the European Commission:

- evaluates the conservation period of system data and provides after one year of use of the PACS an adapted conservation period;

- allows the EDPS access to the results of the IT risk assessment conducted and the list of security controls and mitigation measures implemented;

- provides the EDPS with the documentation relating to the procedure established in case of security incidents.

Done at Brussels, 8 September 2011

(**signed**)

GIOVANNI BUTTARELLI
Assistant European Data Protection Supervisor