To be filled out in the EDPS' office

REGISTER NUMBER: 601

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 03/06/2010

Case number: 2010-0427

Institution: European Commission

Legal basis: article 27-5 of the regulation CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN(2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

2) Name and First Name of the Controller:HUTCHINS Stephen

3) Title:Director

4) Directorate, Unit or Service to which the Controller is attached:DS.

5) Directorate General to which the Controller is attached:HR

2/ Organisational parts of the institution or body entrusted with the processing of personal data

26) External Company or Directorate General to which the Processor is attached:
25) External Company or Directorate, Unit or Service to which the Processor is attached:

DIGIT.C
Securitas.Contract manager.Guard Services

3/ Name of the processing

Commission Physical Access Control System (PACS) :: PSG ? Projet de Sécurisation Globale

4/ Purpose or purposes of the processing

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 infractions or criminal offences (processing is strictly based on data collection and subsequent handover of such data to the competent Commission bodies).

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Every person having or requesting access to Commission premises.

16) Category(ies) of Data Subjects:

As stated on section 14), all data subjects having or requesting access to Commission premises are concerned. In general terms the following main categories can be 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. Other European Institutions or bodies staff,
5. Visitors,
6. Commission staff family members,
7. Commission retired staff,
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
Data subjects will received 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.)
Note: Access rights are assigned based on data subject categories and access needs as defined on the applicable Commission physical access security policies.

6/ Description of the data or categories of data (including, if applicable, special categories of data (article 10) and/or origin of data)*(including, if applicable, special categories of data (article 10) and/or origin of data)*

17) Data field(s) of Data Subjects:
Attention: Please indicate and describe in the answer to this question also data fields which fall under article 10
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
(*) Data source is Sysper2/Comref for Commission staff or equivalent, ORIANA for external personnel and e-Pass for visitors. All other data is generated or collected directly by the system.
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 (see "Physical Access Control Use Cases and Data Processing Scenarios" and "PSG IS and Applications" for details (both accessible from: https://intracomm.ec.europa.eu/security/psg_info/psg_intro.htm)
No data fields fall under article 10.

18) Category(ies) of data fields of Data Subjects:
Attention: Please indicate and describe in the answer to this question also categories of data fields which fall under article 10

The following main categories can be enumerated:

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, video files.
3. Equipments data ? mainly data related to security equipments deployed, including: system names, IP addresses, locations, 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.
No data fields fall under article 10.

7/ Information to be given to data subjects

15a) Which kind of communication(s) have you foreseen to inform the Data Subjects as described in articles 11 - 12 under 'Information to be given to the Data Subject'

- A specific information leaflet (or equivalent) addressed to new badge holders and made available at badge delivery time ? "Information for New Badge Holders" (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm),
- A specific information leaflet (or equivalent) addressed to visitors and made available at buildings receptions ? "Information to Visitors" (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm),
- Affixed notification panels at RFID reading zones, mainly building entrance zones, for awareness purposes ? information content as presented in Annex II of the "PSG Technological Options and Recommendations Report" (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm) is foreseen,
- Affixed notification panels at video recording zones, mainly building entrance zones,
- On 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 de inquiries and by the service in charge of the inquiry. Exceptions to this rule fall under article 20.1 of regulation 45/2001 (see notifications DPO-153 and DPO-914 already mentioned)

8/ Procedures to grant rights of data subjects (rights of access, to rectify, to block, to erase, to object) *(rights of access, to rectify, to block, to erase, to object)*

15b) Which procedure(s) did you put in place to enable Data Subjects to exert their rights: access, verify, correct, etc., their Personal Data as described in articles 13 - 19 under 'Rights of the Data Subject' :

- Data subject are informed of their rights, available contact points, communication channels and procedures in place as described on the document and information sources enumerated above.
- In what concerns 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. The Controller of the access control processing has no information on the reasons or duration of the exclusion of a data subject and acts as a mere processor when processing these data. Following the request of the Director of the Security Directorate the data processor updates the list and activates or deactivates the exclusions as requested.

9/ Automated / Manual processing operation

7) Description of Processing:
Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"
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. Particularly, physical access control automation and uniform enforcement of procedures and security policies. To that end the following objectives and technological solutions are considered for implementation:
? 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 and fully compliant with the ISO/IEC 14443A international standard,
- A contact chip (smartcard), made available for existing or new corporate IT projects and fully compliant with the ISO/IEC 7816 international standard (not used by the notified system),
- The badge may be used to store fingerprint minutiae.
? 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"
(both accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm)
Due to the use of RFID technology and biometrics this processing falls under article 27.

8) Automated Processing operation(s):

Processing done by the system is performed by a range of Information Systems (IS) and applications ? AEOS, ORIANA, e-Pass, fingerprint enrolment, electronic forms and the video surveillance/monitoring system (CCTV) ? and can be described as:

Centralized IT processing, in particular:
1.Badge generation ? processing of personal identification and authentication
2.Access control functions, events and alarms:
? date/time of badge crossing control points, intrusion detection,
? date/time of guards patrols operations ?presence at a specific checkpoints, equipments operations for compliance requirements (check period, appropriate skills, etc.) ? these operations entail a biometric verification
? video recording ? security incidents or video surveillance
3.Visitors management:
? pre-registration, using a central web application,
? personal identification and optical reading of ID documents
4.Parking accesses and authorizations:
? access date/time,
? vehicle identification registration and driver's identification
5.Barring data ? denial of access to Commission premises or refusal to deliver access badge based on a specific list of excluded persons. Reasons and denial considerations are not known to the system or even processed by the system (origin: HR.DS itself, HR.IDOC, and Medical Service).
Local IT processing:
1.Biometric data reading and processing of fingerprint minutiae,
2.Secure storage of the data on the owner's badge chip,
3.Video recording following predetermined security alerts and alarms, etc.
Note: Video processing is included and described in notification DPO-544 "Surveillance vidéo ? stockage analogique et numérique". This notification is linked with that notification.
The system's architecture is described in the "PSG Architecture Document" and the IS and applications with the processed data elements are described in the "PSG IS and Applications" at http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm)

9) Manual Processing operation(s):

Little or no manual data processing is planned. However, some manipulation of legal or ID documents by receptionists and operators, possible exceptions upon system unavailability and indispensable human interventions will impose some manual data processing, like:
- In case of system unavailability paper based registration forms for visitors in building receptions and paper based request forms for visits requests and authorizations,
- Local OCR of data subjects ID documents or invitation credentials,
- Scanning and archiving of official documents (paper or electronic) or equivalent due to legal requirements and compliance (e.g.: future investigations and chain of validation compliance, etc.),
- In case of badge malfunctioning or upon physical access control system unavailability a manual and visual check of the badges and data subject identity will be performed,
- Video checks by control room operators or visual/manual checks by guard patrol of data subject photographs and identification elements when outside working hours access is requested,
- Visual/manual checks by guard on building entrances of photographs and badge identification elements of data subjects in case the presented badge is not recognized by the physical access control system.

10/ Storage media of data

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 eventual 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 contain 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 systems. 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.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

1. Commission Communication concerning the new access-control and security system for Commission buildings ? C(2007)797 of 14 March 2007, (http://intracomm.cec.eu-admin.net/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_C_2007_0797_1_XX.pdf)

2. Commission Decision on Tasks and Responsibilities of the Security Office ? C (94)2129 of 08 September 1994, (http://intracomm.cec.eu-admin.net/security/docs/eu_legislation/decision_2129.pdf)

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, (http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_032/l_03220070206en01440160.pdf)

4. Commission provisions on security ? Commission Decision amending its internal Rules of Procedure ? 2001/844/EC, ECSC, Euratom of 29 November 2001 (http://intracomm.cec.eu-admin.net/security/docs/eu_legislation/commission_decision_844_en.pdf)

12) Lawfulness of Processing:
Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

In accordance with Art.5:
a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities ? namely, 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.

Data collected may be used in the context of investigations led by the Security Directorate on its own initiative or at the request of IDOC or OLAF (see notification DPO-914 "Enquêtes en matière de sécurité" and DPO-153 "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" already submitted to the EDPS) after agreement of the Director General of DG Personnel and Administration and consultation of the Data Protection Officer. Article 20 applies to these investigations.

Due to the use of RFID technology and biometrics this processing falls under article 27.

12/ The recipients or categories of recipient to whom the data might be disclosed

20) Recipient(s) of the Processing:

By default the system is a closed system ? there is no automated sharing, export or retrieval of data with other applications or information systems.

Interactive access to system processed data will be restricted based on approved needs ? i.e.: equivalent to need-to-know principle ? and limited to the data associated with the user population under the responsibility of the operator or user ? e.g.: Local Security Officer (LSO) will have exclusively access to his/her own DG data and functional role (security profiles).

The identified recipients and data groups planned to be given access to data are described in detail in the document "Recipients of the Processing" (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm). In general terms the recipients are:
? The Security Directorate units and sectors: for investigations needs (DS.RA, DS.2), access control and system administration (DS.4) and safety needs (DS.RA, DS.1, DS.6).
? Commission services or other equivalent bodies (e.g.: Agencies): view access list, times ranges, and access profiles to own zones and areas (LSO, LISO, IRM) and view or validate requests of badge delivery and related human resources requests (RRH) and authorise specific requests (e.g.: authorisation to film/photograph inside buildings ? DG COMM, authorisation to use fire when doing works inside buildings ? HR.DS.6)
? Commission subcontractors: security management and monitoring (Security guards, Control Room operators, DS.4 operational staff)
? IT applications: Sysper2 (currently only the personal photo, upon request of the data subject).
? Internal users: end users to manage own request and visitors (e.g.: Commission staff, other regular personnel, etc.) and validate specific requests (e.g.: visitor parking reservation ? Chefs d'immeuble)
? External users: end users to manage own request and visitors/visits (e.g.: request for visit, etc.).

21) Category(ies) of recipients:

The various recipients of the data processing can be grouped on the following main categories (full details on the document "Recipients of the Processing"):
? System administrators (HR.DS.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
? End-users (people using the system to access Commission premises)
? IT application(s) (currently SYSYPER: 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.)

13/ retention policy of (categories of) personal data

The following retention policy will be implemented for the defined data categories:
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. Includes video data, to allow the link with other transit data.
3. Security Profiles data ? data retention is indeterminate (data will be retained until required for the proper operations of the system). All personal data is automatically removed based on the retention policy of category 1.
4. System data ? data retention set to 1 year.
5. Barring data ? data retention is under the responsibility of the Commission responsible authority. 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.
Data retention periods and procedures apply to any data collected about any data subject accessing or registering to have access to Commission premises.
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.
3. Fingerprint minutiae (if used) are permanently stored on the data subject RFID chip embedded on badge, for the badge validity period (foreseen for 5 years).

13 a/ time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject) (Please, specify the time limits for every category, if applicable)
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

22 b) Time limit to block/erase data on justified legitimate request from the data subjects

The global data processing functions to be executed by the system have been analysed in the light of the foreseen data categories and the requirement to perform a specific blocking or erasure of the data in case of errors causing prejudice to the data subject or for probation requirements.

Based on that analysis a global policy to block/erase data on justified legitimate request from the data subjects will be implemented. This block/erase policy is detailed in the "Time Limit to Block Erase Data" (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm).

14/ Historical, statistical or scientific purposes
If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

22 c) Historical, statistical or scientific purposes - If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification

Statistical data will be stored for longer (undefined) periods in a data warehouse or equivalent system.

All data stored for statistical purposes will be rendered anonymous ? first step ? and aggregated ? second step ? in a manner that only global information is available (e.g.: total access control operations per period, total created badges per period, global number of transactions per site, etc). No individual records or other data linked, directly or indirectly, to the data subject will be kept online on the system for statistical purposes.

15/ Proposed transfers of data to third countries or international organisations

27) Legal foundation of transfer:

Only transfers to third party countries not subject to Directive 95/46/EC (Article 9) should be considered for this question. Please treat transfers to other community institutions and bodies and to member states under question 20.

Not applicable ? no transfers allowed to third party countries or other external parties.

28) Category(ies) of Personal Data or Personal Data to be transferred:

Not applicable.

16/ The processing operation presents specific risk which justifies prior checking (please describe): *(please describe)*):

7) Description of Processing:
Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

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. Particularly, physical access control automation and uniform enforcement of procedures and security policies. To that end the following objectives and technological solutions are considered for implementation:
? 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 and fully compliant with the ISO/IEC 14443A international standard,
- A contact chip (smartcard), made available for existing or new corporate IT projects and fully compliant with the ISO/IEC 7816 international standard (not used by the notified system),
- The badge may be used to store fingerprint minutiae.
? 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"
(both accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm)
Due to the use of RFID technology and biometrics this processing falls under article 27.

12) Lawfulness of Processing:
Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

In accordance with Art.5:
a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities ? namely, 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.

Data collected may be used in the context of investigations led by the Security Directorate on its own initiative or at the request of IDOC or OLAF (see notification DPO-914 "Enquêtes en matière de sécurité" and DPO-153 "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" already submitted to the EDPS) after agreement of the Director General of DG Personnel and Administration and consultation of the Data Protection Officer. Article 20 applies to these investigations.

Due to the use of RFID technology and biometrics this processing falls under article 27.

☐ Article 27.2.(a) Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Article 27.2.(a) Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,
□ Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject,
n/a
□ Article 27.2.(c) Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,
n/a
□ Article 27.2.(d) Processing operations for the purpose of excluding individuals from a right, benefit or contract,
n/a
□ Other (general concept in Article 27.1)
n/a
17/ Comments
1) Date of submission:
10) Comments if applicable: The system is exclusively aimed to be used or to provide services and related functions for the implementation of a physical access control to buildings, the protection and safety of staff and protect Commission assets and information. The content of this notification exposes the most accurate description of the data processing to be undertaken and, the technological solutions and implementation particulars planned for deployment. However, considering the long deployment period (some years) the full set of functionalities will not be available at the same time. During the full migration phase from the current system (notified with DPO-508 "Délivrance et contrôle des titres d'accès aux bâtiments de la Commission à Bruxelles et Luxembourg") to the new system (this notification) both systems will interact and exchange information. Corporate deployment is planned to start beginning of 2011 and a pre-production site to be completed during the second quarter of 2010. The system will be operated by unit HR.DS.4

36) Do you publish / distribute / give access to one or more printed and/or electronic directories?
Personal Data contained in printed and/or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
If Yes, please explain what is applicable.

yes
No data publishing outside the main systems is foreseen. In the event that very specific data repositories are temporarily required for data transfer to support identified data recipients needs they will be exclusively accessible to the target data recipient and all data will be fully wiped after transfer or encrypted before transfer.

37) Complementary information to the different questions if applicable, including attachments to this notification which should not be public :

Specific awareness, information and training sessions targeting specific user groups' needs and roles will be prepared and delivered.

System operators' skills and awareness will be regularly reviewed and improved, in particular on fingerprint minutiae enrolment stations operations.

Documents associated with this notification are available on the Commission intranet (accessible from: http://intracomm.cec.eu-admin.net/security/psg_info/psg_intro.htm):
1. 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

PLACE AND DATE:03/06/2010

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission