To be filled out in the EDPS' office

REGISTER NUMBER: 242

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 05/06/2007

Case number: 2007-375

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:RUBIRALTA CASAS Maria Asuncion

3) Title:Head of Unit

4) Directorate, Unit or Service to which the Controller is attached:J.01

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

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:

JRC.J.01

3/ Name of the processing

Access Control at JRC-IPTS in Sevilla

4/ Purpose or purposes of the processing

Access control in the IPTS is a collection of sub-processes, which main purpose is to secure the IPTS building and its staff by:

? encoding of data into personal and visitor's service cards
? storing access and personal data necessary for the application of the local security policy
? organising access schemas according to the local security policy
? automatically combining stored data with access schemas in order to grant or deny access to the IPTS to service card holders
? collecting and recording access data
? recording people's images at the internal entry points (no possibility to take images from public spaces)
? adapting, blocking or altering the stored personal data (i.e. in case of errors detected or similar issues or if so requested by the data subjects in execution of their rights)
? retrieving access and personal data for consultation and/or transmission if so required in the context of a legal enquiry (i.e. requested by the hierarchy)
? alignment or combination with equivalent personal data from other legal sources of information, such as SYSPER2 or the Active Directory
? erasure or destruction as foreseen in this notification (i.e. retention time exceeded)

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

All IPTS staff
All Commission staff
External visitors.

16) Category(ies) of Data Subjects:

All IPTS staff
All Commission staff
External visitors.

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

For IPTS staff
==========
Printed in the service card there is
-a picture
-the personnel number
-the staff's first and last name
-their contractual status (type of contract: statutory or not)
-an acronym of the site
Currently, the following data are stored in the magnetic band of the service card.

It is foreseen that those data are encoded in the chip integrated in the card:
-unique identifier of the card
-a pin code
-a hash produced by a mathematical algorithm representing a scan of DIFFERENT PARTS of their fingerprint, which is IRREVERSIBLE, namely, a fingerprint cannot be rebuilt out of the mentioned algorithm
-the personnel number
-the staff's first and last name
-their contractual status (type of contract: statutory or not)
-an acronym of the site

Recorded by the card readers and thus in the supporting processing units of the access and intrusion control
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

Identity data
Access data
Access profile (schemas)

This processing of personal data is subject to art.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'

Daily visitors will be informed by a privacy statement (see attachement) publicly available at the Reception.

IPTS staff will be informed by delivery of a privacy statement (see attachment) together with their service card. Additionally they will be informed by a privacy statement published in the IPTS intranet (as in DS site).

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' :

For staff, as this processing takes data coming from other systems (i.e. Sysper2), corrections should be done in the source systems where the data are managed (at the level of the Human Resources services).

For external visitors, they may address themselves to the IPTS Reception requesting to exert such rights.

In general, the data subjects can use the functional mailbox : jrc-ipts-secretariat@ec.europa.eu, (see also privacy statement).

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 JRC Institute for Prospective Technological Studies (IPTS) controls everybody's access to its premises by recording who and when enters and leaves the building. Such control is applied differently and with different purposes depending on the category of the data subject. Thus, for IPTS staff, the processing of data includes automatic authentication and authorisation to access the IPTS premises. External visitors must register themselves in the visitor's book. Finally, there is a visual control of the service cards for other Commission staff.

Every access event triggers the recording of images internally to the IPTS only.

The use of biometrics (fingerprints) or key codes is foreseen.

This treatment falls under article 27 (2a) in relation to security measures.

8) Automated Processing operation(s):

The access control relies on an access and intrusion control system that automates a number of operations, such as:
? encoding of data in service cards from a database (including the possibility of manual encoding)
? recording of access times
? storing of access schemas
? recording of images with video cameras at all the four entry points

Currently, the access control system is based on the use of service cards with magnetic bands, where personal data is encoded.

The IPTS is upgrading such system by:
? authentication of card holders with fingerprint or key code against the personal data stored in the service cards
? authorisation to access to card holders based on the stored access schemas

In order to realise these functions, the access control system includes software, installed in a computer hosted in the IPTS data centre.

9) Manual Processing operation(s):

The IPTS Reception is the only access point for external visitors, including EC staff (non-IPTS).

External visitors register their own data in a book that is made available to them at the IPTS reception, mentioning who they are visiting. The visitors must sign in and out the list. The receptionist calls the visited person, who identifies the visitor and accompanies them inside.

When an organised event takes place, a visitors list is given to the receptionist (see also notification DPO-1528 on JRC EVENTS,...), who controls access.

The EC staff coming from other services (non-IPTS) must show their service cards or else register themselves as external visitors, in which case they also sign in and out in the book.

Other manual operations include regular operation of the access control system configuration and database.

10/ Storage media of data

The access control system autonomously records the data in a dedicated computer situated in the data centre of the IPTS, which access is restricted to authorised personnel only.
Paper records of external visitors are stored in the physical archive of the IPTS Administration, following the rules applicable to all other documents.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

- Regulation N° 3 in application of article 24 of EURATOM Treaty; Section II, Article 21

- COMMISSION DECISION C(94) 2129 of 8 September 1994 on the tasks of the Security Office Article 4

- 2001/844/EC,ECSC,Euratom: Commission Decision of 29 November 2001 amending its internal Rules of Procedure (notified under document number C(2001) 3031) art 7.3: "...Buildings housing EU classified information or secure communication and information systems shall be protected against unauthorised access ... protection afforded... automated access control systems ... alarm systems, intrusion detection systems..."

- Internal JRC directive regarding 72 Month Rule (see attachment)

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)"

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 or other legal instruments adopted on the basis thereof

and Art. 5 b) processing is necessary for compliance with a legal obligation to which the controller is subject (see reference to Decision 2001/844/EC,ECSC,Euratom above)

This processing of personal data is subject to art.27.

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

20) Recipient(s) of the Processing:

- The Head of the Management Support Unit (MSU) as responsible of the processing
- The Security Officer of the IPTS for operation (input and management of data) or delegated staff
- The Informatics Service (for maintenance and system administration purposes).
- The Security Directorate (DG ADMIN/DS) of the Commission for security reasons in accordance with the applicable provisions of Regulation (EC) No 45/2001 (Art 7).
- The MSU for contractual reasons looking at the real presence on site of staff working for external contractors could (Art 7).

21) Category(ies) of recipients:

Controller
- Head of MSU

Operator/s
- Security Officer and/or delegate
- Informatics staff

13/ retention policy of (categories of) personal data

For identity and access profile data of statutory staff: during the lifetime of the corresponding contract (i.e. associated with a valid staff pass).
For identity and access profile data of non-staturory staff who need to follow the 72 months rule, data must be kept for 12 years.
For access data: limited to the capacity of the hardware and with a maximum of 1 year.
For backup copies of the access data: 5 years, as foreseen in the IPTS IT business continuity plan (BCP)
For physical archives: 5 years
For visitors' book: it is active for 1 natural year and then archived in the general archive of the IPTS and following its rules (local CAD), thus for 5 years
For video surveillance: limited to the capacity of the hardware and with a maximum of 1 year.

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

Upon a justified request by the data subject to the contact foreseen in this procedure (i.e. functional mailbox) the personal data will be blocked/erased within 14 days.

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

Not applicable

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

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 JRC Institute for Prospective Technological Studies (IPTS) controls everybody's access to its premises by recording who and when enters and leaves the building. Such control is applied differently and with different purposes depending on the category of the data subject. Thus, for IPTS staff, the processing of data includes automatic authentication and authorisation to access the IPTS premises. External visitors must register themselves in the visitor's book. Finally, there is a visual control of the service cards for other Commission staff.

Every access event triggers the recording of images internally to the IPTS only.

The use of biometrics (fingerprints) or key codes is foreseen.

This treatment falls under article 27 (2a) in relation to security measures.

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)"

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 or other legal instruments adopted on the basis thereof

and Art. 5 b) processing is necessary for compliance with a legal obligation to which the controller is subject (see reference to Decision 2001/844/EC,ECSC,Euratom above)

This processing of personal data is subject to art.27.

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

n/a

Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject,

Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject

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:

This notification has similarities to DPO-508 of DG ADMIN

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.

no

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

For staff only: the personal data processed by this processing originates from the official sources of data of the Commission, namely Sysper2.

See also enclosed copy of the visitors' book (with cover sheet).

PLACE AND DATE:05/06/2007

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission