To be filled out in the EDPS' office

REGISTER NUMBER: 634

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 15/11/2010

Case number: 2010-902

Institution: 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:PETER Georg

3) Title:Head of Unit

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

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:

3/ Name of the processing

Access Control System at JRC Ispra Site

4/ Purpose or purposes of the processing

Security Service aims at providing:

i) Security measures to protect the persons and premises of the site.
ii) Authorisation of access to site (registration of staff, visitors and vehicles),
iii) Physical protection of the site (guards, alarms, video surveillance, etc.)
iv) Protection of Commission assets, information and monitoring of information system security.

Processing necessary in order to comply with Italian Law concerning Nuclear Sites and both Commission and JRC internal regulations concerning On-Site Presences.

The access to facilities and sensitive areas for non-authorised individuals is restricted for security and safety reasons.

The Access Control System is one element of the Physical Protection Systems installed on site. It is essentially comprised of end point technical components (card readers and alarm points) installed throughout the campus, the sites entrances as well as its perimeter fence. Such installations use databases as information sources and repositories in order to implement and enforce the requested and needed staff access controls.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Anyone needing to access, enter or visit the Joint Research Centre - Ispra Site.

16) Category(ies) of Data Subjects:

Anyone needing to access, enter or visit the Joint Research Centre - Ispra Site.

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

Refer to SECPAC (DPO-722) and ARDOS (DPO-725) for Staff Pass or Special Authorisation Data Fields.

PHYSICAL BADGE - Badge Num, PIN Code, Version (augmented when badge lost or stolen), Validity Dates

CARD READER - Reader ID, Description, Physical Location, Location Co-ordinates, Parent Reader or Area

SPECIAL AUTHORISATION - Badge Num, Validity Dates (Max. 14 months), Time Range Validity (Working hours up to 24h/24h and Working Days up to 365 days/year), Accessible Areas (Buildings, Offices, Specific Reader IDs)

Furthermore data from card readers and licence plate recognition system, related to Transactions and Anomalies is collected:

BADGE TRANSACTION - Badge Num., Reader ID, Date, Time, Direction (Entry/Exit)

BADGE ANOMALIES - Badge Num., Reader ID, Date, Time, Error Code and Error Message

VEHICLE TRANSACTION (AUTOMATED RECOGNITION) ? Plate Number, Data Reliability, Plate Nationality (indicative), Time, Direction (Entry/Exit), Anomaly Flag with eventual corrected Plate Number

Processing and data fields fall mainly 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

Processing and data fields fall mainly under Article 10.

See point 17.

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'

The Access Control System is the end point system receiving data from SECPAC and ARDOS.

It should be noted that the data of the Access Control System that ends up in the ARDOS database for what concerns card reader transactions is by definition not used for presence control or flexitime accounting.

Privacy Statement is available to the data subjects in a clear visible way, among others on the JRC intranet.

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' :

This is performed through SECPAC (DPO-722) and ARDOS (DPO-725) as described above.

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 purpose of this notification is to describe the Access Control System at JRC Ispra, one element of the Physical Protection Systems installed on site to protect the European Commission premises in Ispra against unauthorised access and external as well as internal threats. It is essentially comprised by end point technical components (card readers and alarm points) installed throughout the campus, the sites entrances as well as its perimeter fence. Such installations use databases as information sources and repositories in order to implement and enforce the requested and needed access controls.

In entrances to the site where it is possible to enter with vehicles, a vehicle licence plate recognition system, is/will be in place to verify that vehicles entering the site are effectively registered in Vehicle Registration module of SECPAC (DPO-722) and are thus authorised to enter the site.

The Access Control System covers not only the entrances to the site, including the main entrance, the east ent

Such readers may be in control and integrated with other equipment like unipersonal SAS or electrical locks th

It should be noted, independently of the technology used, that no other information apart from the physical bad

Data fields to consider are mainly related to transactions and anomalies associated with a physical badge num

The processing doesn't falls ...
===> Could you replace by:
"The processing falls under art. 27 as Biometric Fingerprint Readers are used in this processing".

8) Automated Processing operation(s):

The programming of all existing card readers is usually performed automatically on a daily basis but may be performed manually in case of need if urgent updates to the binary data stored on readers are needed. Such a processing involves the reading of all active 'staff pass' and 'special authorisation' request data from SECPAC (DPO-722) and transformation of such data to a binary format understood by the card readers.

Similarly for what concerns automated vehicle access control, dedicated cameras read the licence plate - by taking several image snapshots uses OCR technology to interpret it - and confront the result with the records regarding registered and thus authorised vehicles. Furthermore a wider image of the entrance or entrance lane is visible and captured in order to verify the number of occupants of a vehicle corresponds to the number of badges identified and also present an overview of what is happening. It should be noted that such a system does not have as an aim the identification of people transiting.

9) Manual Processing operation(s):

Any troubleshooting or corrections to the automatic processes described above are handled and analysed by core Security Staff in charge of managing the Access Control System by performing manual corrections if necessary.

The definition of Card Readers and their relationship in micro or macro 'Virtual Areas' is also performed manually following 'in the field' logic.

10/ Storage media of data

Data is currently kept on Direct Access Storage of Security Service Servers connected to the Security Service Internal Network, physically disconnected and not accessible from the outside world, as well as on Removable Media used for backup purposes.

See also point 17.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

International Legislation
- IAEA INFCIRC/255 Prescription
(http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html)
- EURATOM Regulation n. 3 (O.J. 406/58 of 06.10.58)
- Law n. 906 of 1st August 1960 establishing formal agreement between EC and Italy
- Ministry of Industry Decree of 21.07.87 with technical specifications (confidential n. 42)

Internal Rules and Regulations
- 72 month On-site Presence rule (C(2004) 1597) along with JRC specific rules.
- Security Provisions C(2001) 3031 of 29.11.2001
- Industrial Security C(2006) 548 of 02.08.2006
- IT Security C(2006) 3602 0f 16.08.2006
- Mission Statement of Security Service

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)"

The processing is necessary according to art. 5a) & 5b) of regulation 45/2001.
It falls under articles 20 ===> and 27.

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

20) Recipient(s) of the Processing:

Mainly for internal use of Security Service. Information provided always with a very good justification on the basis of the 'need to know' principle.

This processing of personnel data is under the responsibility of the Head of Unit for Safety and Security, acting as Controller for this processing. This HoU reports directly to the Ispra Site Director.

21) Category(ies) of recipients:

Vetted core Security Service Staff.

13/ retention policy of (categories of) personal data

Access Control System transaction and anomaly data has only been kept since 2002 in its present format. Being complimentary to daily permit, staff pass and special authorisation related information it should be kept for at least 12 years.

For what concerns the data of access to nuclear areas, see point 22c) and privacy statement.

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 justified request from the Data Subject data will be modified, frozen or eventually erased in a maximum period of one month.

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

After the standard retention period motioned above, data related to general access control transactions will be anonymised in order to be able to produce statistics.

For what concerns the registration of controlled zones or nuclear areas entry/exit, the duration of the retention period is 30 years due to legal requirements e.g. to store Dosimeter assignments for health reasons.

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 data transfers occur.

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

Not applicable. No data transfers occur.

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 purpose of this notification is to describe the Access Control System at JRC Ispra, one element of the Physical Protection Systems installed on site to protect the European Commission premises in Ispra against unauthorised access and external as well as internal threats. It is essentially comprised by end point technical components (card readers and alarm points) installed throughout the campus, the sites entrances as well as its perimeter fence. Such installations use databases as information sources and repositories in order to implement and enforce the requested and needed access controls.

In entrances to the site where it is possible to enter with vehicles, a vehicle licence plate recognition system, is/will be in place to verify that vehicles entering the site are effectively registered in Vehicle Registration module of SECPAC (DPO-722) and are thus authorised to enter the site.

The Access Control System covers not only the entrances to the site, including the main entrance, the east ent

Such readers may be in control and integrated with other equipment like unipersonal SAS or electrical locks th

It should be noted, independently of the technology used, that no other information apart from the physical bad

Data fields to consider are mainly related to transactions and anomalies associated with a physical badge num

The processing doesn't falls ...
===> Could you replace by:
"The processing falls under art. 27 as Biometric Fingerprint Readers are used in this processing".

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)"

The processing is necessary according to art. 5a) & 5b) of regulation 45/2001.
It falls under articles 20 ===> and 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:

Card Readers support the following technologies:
- HICO Magnetic Stripe currently used by the majority of readers;
- RFID based MIFARE ISO 14443 that will substitute the majority of magnetic stripe readers in the future;
- A limited number (currently a total of 4) Biometric Fingerprint Readers, strictly based on fingerprint minutiae and a pattern based algorithm (see http://en.wikipedia.org/wiki/Fingerprint_authentication for greater details) and not actual fingerprint images, where data is stored and memorised only on the reader itself, are in use. It should be underlined that no database is used to store this kind of information and users enrol for using such readers on a voluntary basis.

This notification is related with both the SECPAC (DPO-722) and ARDOS (DPO-725) notifications. The personal data collected in such systems is used for practical implementation of what is called in such databases as the Access Control System.

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 :

In order to better understand the relationship between Security Service Information Systems and the Access Control System please refer to the attached SESAPPSSchema.pdf.

PLACE AND DATE:15/11/2010

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission