To be filled out in the EDPS' office

REGISTER NUMBER: 247

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 06/06/2007

Case number: 2007-381

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:KOLETSOS Antonios

3) Title:Head of Unit

4) Directorate, Unit or Service to which the Controller is attached:C.07

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

SECPAC

4/ Purpose or purposes of the processing

Authorise and register entry on-site of people, internal or external, and respective vehicles and material, with their various profiles in accessing controlled areas or accessing the site outside working hours.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

Anyone with the intention, wanting or needing to enter or visit the Ispra Site.

16) Category(ies) of Data Subjects:

Anyone with the intention, wanting or needing to enter or visit the 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

Data fields to consider are mainly related to personal identification data, that for visitors includes date of birth, nationality, personal address and details of an identification document among others.

In summary the following 'personal data' is collected:

VISITORS ? Surname, Firstname, Company, Date and Place of Birth, Nationality, Full Private Address, Contact Telephone,
Identity Document Details [Document Type (Passport, Identity Documents, Driver's licence, etc.), Document Number, Issuer, Issue Date], Permit Start and End Date/Time, Visit Start and End Date/Time, eventually also with dosimeter number between 1983 and 2002, Visited Area(s) and People.

STAFF ? Personnel Number, Surname, Firstname, Date and Place of Birth, Nationality, Gender, Full Private Address, Contact Telephone, Contract Type (official, temporary agent, contractual agent, etc.), Internal
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.

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'

Please see Privacy Statements.

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' :

In case a user has questions related to SECPAC or concerning any information processed in this context, he/she can contact the Ispra Site Director acting as Controller for this processing as defined in Regulation (EC) n° 45/2001 on personal data protection under the following functional mailbox: jrc-secpac-support@ec.europa.eu (see attachment JRCSECPACSupport.pdf).

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)"

Management of the full workflow of access requests to Security Service that may involve unit secretariats, authorising officers, responsible people for access controlled areas or nuclear zones as well as security service.

SECPAC is the application used to process and manage the following type of requests:
a) Daily permits for entering the Ispra site (both for Visitors or staff with special requirements associated with a daily Special Authorisation) delivered by the Reception Desk (see attachment RulesandUsefulInformationforVisitors.pdf);
b) Long term access permits (i.e. staff passes) and associated Special Authorisations(related to outside normal working hours or access controlled areas or nuclear zones);
c) Vehicle Registrations (VCARP);
d) Registration of material for off-site use (REGMAT).
e) Tracking of presences regarding staff working on-site for external contractors.
8) Automated Processing operation(s):

Management of the full workflow of requests to Security Service that may involve unit secretariats, authorising officers, responsible people for access controlled areas or nuclear zones, Human Resources as the only entity that may request Long Term Permits for Statutory and Non-Statutory staff, as well as security service.

9) Manual Processing operation(s):

Data insertion for all types of requests.

Issue of 'On-Site Presences', to authorised people, and application of internal '72 month Rule' (see attachment Point 11).

10/ Storage media of data

Direct Access Storage on Security Service Servers connected to the Commission Internal Network and Removable Tape Media.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

- Euratom Treaty and Directives (see attachment) regarding the need to maintain certain types of information (e.g. dosimeter assignment)
- Italian Law 906/1966 (see attachment) regarding establishment of the Joint Research Centre.
- Physical Protection Plan included in decree of Italian Ministry of Industry (see attachment)
- Internal JRC directive regarding 72 Month Rule (see attachment)
- Financial Regulations
- Italian Safety Regulations 626/1994

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 and lawfull under art. 5(a) of Regulation (EC)45/2001

Security Service within the Logistics unit 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 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.

Data processing falling under article 27.

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

20) Recipient(s) of the Processing:

SECPAC Users, including 'Secretaries' and 'Authorising Officers', have access to a well-defined subset of request processed by them or delegates. Security Service staff that has access to all information and uses it mainly for internal use.

For visitors coming from non-EU Member States a copy of a valid identification document is transferred to ADMIN/DS for further authorisation following article 7. For this reason such daily permit requests if being done for the first time have to be inserted in SECPAC 30 days before the visit.

Database View accessible to the JRC DATAPOOL for registration of external staff with a valid staff pass, i.e. long term authorisation, needing access to Commission Computing Resources i.e. people working for the JRC and with 'name.surname@ext.ec.europa.eu' e-mail address.

Manual processing of 'On-Site Presence' requests sent to list of authorised people from Management Support Units and Human Resources involved in staff recruitment in support to the application of the '72

21) Category(ies) of recipients:

Authorised SECPAC users are statutory staff only. The directory of data subjects is nevertheless visible to all authorised SECPAC users.

Visibility of data, excluding personal details directory, is filtered always by unit unless someone works for Security Service.

Vehicle registrations visible only to owner of vehicle and Security Service.

The 'On-site Presence' data is only fully visible to Security Service.

13/ retention policy of (categories of) personal data

As declared In the Privacy Statements, included in attachment to this notification, the following retention periods depending on which information is concerned are defined:

i) SECPAC Visitor Data and Vistor 'Daily Permit' Pass
Personal data is kept as long as follow-up actions to visits and linked to the 72 months rule are necessary. As a consequence all personal data related to your visit will be deleted 12 years after the visit.
Visitor 'Daily Permit' Passes are physically destroyed 3 months after the date of the visit.

ii) SECPAC Long Term Permit & Special Authorisation Data
Data must be kept as long as there is a contractual link with the data subject. Additionally it is kept as long as follow-up actions linked to the 72 months rule are necessary. As a consequence all personal data related to long term access permits will be deleted after 12 years.

iii) Vehicle Registrations (VCARP) Data
Data is kept as long as there is a contractual link with the data subject. It is kept for an additional period of 12

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

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

At least for the last 12 years.

Registration of entry into controlled zones or nuclear areas, the duration of the retention period is longer e.g. when Dosimeter assignments are concerned where by law it is obligatory to store them at least for 30 years (see attached Euratom Treaty and Directives, in particular, Article 90 in point 11).

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)"

Management of the full workflow of access requests to Security Service that may involve unit secretariats, authorising officers, responsible people for access controlled areas or nuclear zones as well as security service.

SECPAC is the application used to process and manage the following type of requests:
a) Daily permits for entering the Ispra site (both for Visitors or staff with special requirements associated with a daily Special Authorisation) delivered by the Reception Desk (see attachment RulesandUsefulInformationforVisitors.pdf);
b) Long term access permits (i.e. staff passes) and associated Special Authorisations(related to outside normal working hours or access controlled areas or nuclear zones);
c) Vehicle Registrations (VCARP);
d) Registration of material for off-site use (REGMAT).
e) Tracking of presences regarding staff working on-site for external contractors.
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 and lawfull under art. 5(a) of Regulation (EC)45/2001

Security Service within the Logistics unit 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 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.

Data processing falling under article 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:

The search function within the People's Directory allows all SECPAC users to have access to the data of visitors containing: Surname, Name, Company, Nationality, Date and place of birth and Type of Visitor.

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
The electronic directory of people that have at least had the intention to enter the Ispra site is available to all SECPAC users for forwarding requests to Security Service and thus abides to the strictly necessary and specific usage rule.

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

SECPAC application reference manuals (SECPAC, VCARP, REGMAT) in attachment.

'On-Site Presence' document template issued by Security Service to Management Support Units and Human Resources.

Please find attached also the Legal Clauses for Data Transfer under Article 7 concerning SECPAC.

In the specific case of the JRC Open Day Event, regularly held annually, a list of registered visitors is elaborated and transferred by the Public Relations to Security Service but due to the high number of visitors, the data is not inserted or processed within SECPAC.

** Historical Dosimeter Data ***
The SECPAC Visitor database was designed to include the possibility to associate a dosimeter number with a particular visitor. Before the entry into production and use of SECPAC this information was handled on paper and by an internal information system that recorded exactly the same data. With the itrodcution of SECPAC it became much easier and quicker to trace a particular dosimeter to a particular person when deem important to note that no other radiological information was ever recorded or kept for what concerns dosimete

PLACE AND DATE:06/06/2007

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission