To be filled out in the EDPS' office

REGISTER NUMBER: 287

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 03/09/2007

Case number: 2007-507

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:PETER Georg

3) Title:Official

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

SECURITY INVESTIGATIONS AT JRC ISPRA

4/ Purpose or purposes of the processing

Collect and report truthful facts regarding accidents or incidents; identify and eliminate security breaches; identify perpetrators of thefts, acts of vandalism, intrusion and unauthorised access with the overall objective to determine and quantify any endured damages as well as identify the authors of such infractions.

Provide technical support to the various administrative services of the Joint Research Centre e.g. Human Resources, Social Servies, Medical Service or Informatic Services, etc. in collecting information or any other probatory elements lawfully requested by such services.

Data can be handed over to OLAF, IDOC, Judicial Authorities or National Law Enforcement agencies upon written request and duly authorised by the controller in case of investigations regarding threats to the security of the Joint Research Centre sites or the European Commission.

5/ Description of the category or categories of data subjects

14) Data Subject(s) concerned:

All staff in active employment (including officials or other temporary or contractual agents) retired officials, external staff working under contract, visitors or any other person that addresses itself to the Joint Research Centre or its staff, notably by mail, e-mail, telephone, fax, etc., or that are victims, witnesses or authors of an infraction, a felony or damaging event to the institution or its staff as well as any staff member towards whom the Commission has to exercise its duty of solicitude.

16) Category(ies) of Data Subjects:

- Staff in active employment (including officials or other temporary or contractual agents);
- Retired officials;
- External staff working under contract;
- Visitors;
- Any other person that addresses itself to the Joint Research Centre.

See point (14) for further details.

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

As all details are included in a written detailed Security Investigation Report it is difficult to determine exactly which data may be considered. Usually information concerns:

People - surname, first name, date and place of birth, nationality, gender, full private address, contact telephone, contract type (official, temporary agent, contractual agent, etc.), internal address, internal telephone number, daily or long term permit start and ending dates.

Incident - Date, Time, Location, Detailed Description, Supporting documentation to the Description (Photogrpahs, Video Surveillance footage, etc.).

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

Please refer to ARDOS (DPO-725) for categorisation of possible fields.

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'

Data subjects will be informed by a Privacy Statement (see attachment). Such a Privacy Statement will be published on the intranet website of the Security Service of the Ispra site.

The person signalling a fact or incident, either personally, by telephone or e-mail is automatically aware of the information being collected and provided. All witnesses or authors of a fact or incident during an investigation are interviewed in the same way being aware of what is being discussed.

In all cases verbal or written declarations, always performed in agreement and in presence of the concerned person or people, are transcribed to a written statement that is immediately signed by the involved Security Service staff and always countersigned for approval by the person or people concerned. Data subjects are provided with a copy of their declaration.

In case people cannot be reached personally for an investigation all efforts are made to find an eventual contact through other Commission services e.g. ADMIN/DS. In order to achieve this an eventual follow-up with Judicial Authorities or Law Enforcement agencies may be made until the need for performing the investigation is deemed necessary.

For what concerns the particular case concerning the "Acceptable use of Commission?s ICT Services (i.e. PC equipment, e-mail and Internet Access Systems, Telephone, Fax and Mobile Phones, etc.)" all the control measures are described in the Administrative Notice 45/2006 (http://www.cc.cec/guide/publications/infoadm/2006/ia06045_en.html)

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' :

People concerned with an investigation are always invited to contact Security Service and in particular the Security Officer handling the investigations in case of need i.e. access, verify, correct or perform an integration of their own declarations or statements.

Data subjects may always contact Security Service through the use of the JRC-SECURITY-ISPRA@ec.europa.eu functional mailbox (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)"

Investigations related to security related incidents such as accidents, security breaches, thefts, vandalism, intrusions and unauthorised accesses.

See point (9) for further details.

Personal Data handled falls under article 27.

8) Automated Processing operation(s):

Not Applicable.

9) Manual Processing operation(s):

A Security Investigation usually concerns the following processing operations:

i) Constitution of a so called 'paper dossier' where complaints, testimonies or declarations of any intervenients are collected along with any probatory elements, like photographs etc. are included.

ii) Consultation of local databases like SECPAC (DPO-722) and ARDOS (DPO-725), video-surveillance footages and when necessary any other information deemed useful for the investigation and usually requested to Ispra local key services like the Human Resources, Social Service, Medical Services,Informatics Unit, etc.

iii) Transmission to anyone working for the Commission with the 'need to know' and within the framework of their professional activity of the results of an investigation.

iv) Production of an Investigation Report written with main conclusions of investigation that may be stored within ARDOS (DPO-725) if deemed necessary for future consultation purposes.

10/ Storage media of data

Paper and eventually electronic media.

11/ Legal basis and lawfulness of the processing operation

11) Legal basis of Processing:

i) Commission Decision C(94)2129 of 8 September 1994 (see attachment), where certain tasks and responsibilities have been delegated to the Security Service - Ispra.

ii) Decision 844 of 29/11/2001 and Euratom Regulation n° 3 of 31/07/1958 (see attachments)

iii) Administrative Information n° 45/2006 of 5/09/2006 (http://www.cc.cec/guide/publications/infoadm/2006/ia06045_en.html)

iv) Mission Statement of Security Service JRC Ispra (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)"

Lawfulness falls under Art. 5a , 5b, 5d, 5e.
Exceptions and Restrictions fall under Art. 20.1, 20.3, 20.4, 20.5.
Processing falls under article 27 - Priori checking by the EDPS.

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

20) Recipient(s) of the Processing:

Final Investigation Reports summarising all declarations, approbatory elements, etc. are delivered to involved services on a 'need to know' basis and may also be transmitted for information to ADMIN/DS, OLAF or any Judicial Authorities or National Law Enforcement agencies for eventual follow-up.

Data can be handed over to OLAF, IDOC, Judicial Authorities or National Law Enforcement agencies upon written request and duly authorised by the controller in case of investigations regarding threats to the security of the Joint Research Centre sites or the European Commission.

Transfer of data following Art. 7 and 8.

21) Category(ies) of recipients:

Authorised Commission Officials or any Judicial Authorities or National Law Enforcement agencies.

13/ retention policy of (categories of) personal data

Data of Security Investigations resulting in an effective applicable measure (e.g. interdiction in accessing the site or a particular area) needs to be kept until that applicable measure has to be enforced or tracked. Maximum retention period to be considered is of 5 years.

Security Investigations resulting in a dossier that may need to be handled under penal law are kept for a maximum of 10 years, starting from the conclusion date of the investigation, time period that usually corresponds to their legal prescription.

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

Justified legitimate requests addressed to Security Service will be considered with immediate effect.

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)"

Investigations related to security related incidents such as accidents, security breaches, thefts, vandalism, intrusions and unauthorised accesses.

See point (9) for further details.

Personal Data handled 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)"

Lawfulness falls under Art. 5a , 5b, 5d, 5e.
Exceptions and Restrictions fall under Art. 20.1, 20.3, 20.4, 20.5.
Processing falls under article 27 - Priori checking by the EDPS.

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

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:

No database is used for managing or tracking status of Security Investigations.

Final Investigation Reports are sometimes archived in ARDOS, the Security Service Archive, as a document.

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 :

Please also refer to DPO-914 as Security Service sometimes collaborates and explictily asks for the collboration of ADMIN/DS i.e. when extra support and resources are needed or eventually when an escalation is deemed necessary.

PLACE AND DATE:31/08/2007

DATA PROTECTION OFFICER: RENAUDIERE Philippe

INSTITUTION OR BODY:European Commission