(To be filled out in the EDPS' office)
REGISTER NUMBER: 1158

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 17/09/2013

CASE NUMBER: 2013-1020

INSTITUTION: EC

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

CONTROLLER : MICHEL JEAN-PIERRE
E-MAIL: Jean-Pierre.MICHEL@ec.europa.eu

DELEGATE : D'ALBERTI FRANCESCO
E-MAIL: Francesco.D'ALBERTI@ec.europa.eu

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

THE EUROPEAN COMMISSION
DG JRC - DIRECTORATE B

3/ NAME AND DESCRIPTION OF THE PROCESSING

NAME: Security opinions on the Third Country Nationals accessing the JRC Sites

DESCRIPTION:
Within the limits of its mission, the JRC maintains the working-level contacts with scientific establishments from different countries. This may imply presence in the JRC Sites of the staff seconded from those establishments, or frequently requires admitting visitors taking part or assisting in the JRC activities taking place on its Sites. The specificity of the JRC tasks may also require the

[1] OJ L 8, 12.01.2001.

presence on the Site of external contractors (or bidders – at the stage of contract preparation and negotiation) providing services commissioned by the JRC. Often among the above persons, as well as the potential staff members invited for e.g. job interviews within the limits of the staff selection procedures (such as grant-holders, visiting scientists, etc.), there are nationals of countries not being part of the EU Member States (hereafter 'TNC' – Third Country Nationals). In line with the relevant legal requirements (see the chapter 8 "Legal basis"), the JRC has developed a procedure providing for the rules according to which the access of the TNC to the JRC Sites is granted. The procedure defines in which circumstances the security screening is requested and preventive measures and countermeasures are introduced in the context of the TCN accessing the JRC sites. The application of the procedure involves the processing of personal data within the meaning of the Regulation 45/2001.In practical terms, each time a JRC staff member requests the access for a TCN to a JRC Site, he/she is required to fill in the APPLICATION FORM by providing certain general information about the TCN together with the details of the length of the TNC stay on the Site, modalities of access (unaccompanied, accompanied) and the type of the JRC premises that are to be made accessible to the TNC (public, restricted, nuclear, etc.). On the basis of the information provided, the security OPINION is issued by the Local Security Service. Before the opinion is issued the Local Security Service may consult the Commission's Directorate of Security (unit HR.DS.2). On the basis of the opinion, the decision to grant/refuse the access will be taken by the JRC hierarchy. The same procedure and form are used in all JRC Sites. Personal Data handled falls under article 27.

4/ PURPOSE OR PURPOSES OF THE PROCESSING, AND PROCESSORS

The data are collected and processed in order to allow the JRC hierarchy to take a decision whether to grant (or refuse) the TNC the access to the JRC Sites.

PROCESSORS:
Subcontractors of Security Services attached to the Local Security Officers of each JRC site may process the data on behalf of the controller.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

The natural persons (not legal entities, associations, foundations, etc.) accessing the JRC Sites.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA *(including, if applicable, special categories of data (Article 10) and/or origin of data).*

The collected data, to be provided by the data subject and to be accompanied by paper evidence, are:

- Data: first name, family name, nationality, passport number and date of issue; list of countries visited in the 12 months prior to the application to access the JRC sites, reasons of visit and length of stay in those countries; list of JRC sites already visited prior to the application to access again the JRC site(s), reasons of visit and length of stay in those sites.
- Documents: CV, the extract of the criminal record and the opinion of the JRC Sites Local Security Officer/HR Security Directorate.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Data subjects will be informed by a Privacy Statement (see attachment). Such a Privacy Statement will be provided to the data subject before the JRC starts collecting the information necessary to complete the form. It will be provided to the data subject directly by e-mail by the staff member requesting the access for the TCN to the JRC Site. It is also available upon request and published on the JRC internet website.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

The Data Subjects have the rights to: access their data held by the controller (at any time within three months from the receipt of the request and free of charge from the controller), rectify the data held by the controller (without delay of inaccurate or incomplete personal data).By written request to be sent solely via email to: JRC-SAFETY-SECURITY-COORD@ec.europa.eu

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Depending on the JRC Site security service capabilities and tools, the data are processed automatically (by a computer machine) or manually (hard copy or excel sheet or database) where the data is introduced, updated, deleted manually without computer intervention. The procedure of granting access to the JRC Sites to the TCN involves preparation of a dossier consisting of the APPLICATION FORM and the TNC SECURITY OPINION.

10/ STORAGE MEDIA OF DATA

The collected personal data and all information related to the above mentioned process is stored on electronic media and/or on paper copies, and is stored in security containers and/or on the servers of the Sites Local Security Officers services.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

- Commission decision 29 November 2001 - 2001/844/EC/ECSC/EURATOM

- Commission Decision on Alert States and Crisis Management Commission Decision 2007/65/EC of 15 December 2006 , in particular section 4 of the annex with regards to the Joint Research Centre

- Memorandum of Understanding between DG HR/DS and JRC on tasks performed in the field of security, Ares(2010)884864 – 30/11/2010

- Mesures de sécurité liées à la présence de ressortissants de pays-tiers sans lien statutaire au sein de la Commission, Ares(2012)251857), 16/11/2012.

The JRC sites are subject also to national legislations that require different arrangements for what concerns security checks of people accessing their premises. As per the DPO notifications already existing for the JRC sites access control systems, also the following legislations apply:

ISPRA (DPO-2734.1 - JRC: Access Control System at JRC Ispra Site)

- JRC Ispra site nuclear physical protection plan, Decreto del Ministro dell'Industria, del Commercio e dell'Artigianato, nr. VII-260, 21/07/1987; with technical specifications (confidential n. 42)
- 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)
- Italian Law n. 906 of 1st August 1960 establishing formal agreement between EC and Italy
- 72 month On-site Presence rule (C(2004) 1597) along with JRC specific rules.
- Industrial Security C(2006) 548 of 02.08.2006
- IT Security C(2006) 3602 0f 16.08.2006

PETTEN (DPO-1534.3 - JRC: access management system at JRC-IE in Petten)

- Commission decision 29 November 2001 - 2001/844/EC/ECSC/EURATOM
- Commission Decision on Alert States and Crisis Management Commission Decision 2007/65/EC of 15 December 2006, in particular section 4 of the annex with regards to the Joint Research Center

SEVILLE (DPO-1426.5 - JRC: Access Control at JRC-IPTS in Sevilla)

- COMMISSION DECISION C(94) 2129 of 8 September 1994 on the tasks of the Security Office Article 4.
- Commission decision 29 November 2001 - 2001/844/EC/ECSC/EURATOM

GEEL (DPO-1177.6 - JRC: access control at JRC-Geel)

- Euratom Treaty Art.3: security requirements for nuclear installations.
- Belgian Regulation (Royal Decree 20.7.01, Art 30.1, see: http://fanc.fgov.be/nl/page/koninklijk-besluit-20-07-2001-samenvatting/30.aspx).

KARLSRUHE (DPO-1460.2 - JRC: entrance permission and access control for physical protection (ZES+ZKS) at JRC-ITU in Karlsruhe)

- Atomgesetz (AtG) §9+§12b+§12c as of 15.07.1985 http://www.gesetze-im-internet.de/atg/index.html
- Atomrechtliche Zuverlässigkeitsüberprüfungsverordnung (AtZüV) as of 01.07.1999 http://www.gesetze-im-internet.de/atz_v/index.html
- Strahlenschutzverordnung (StrlSchV) §42 as of 20.07.2001 http://www.gesetze-im-internet.de/strlschv_2001/index.html
- Euratom Treaty as of 25.03.1957 http://europa.eu/scadplus/treaties/euratom_en.htm , http://eur-lex.europa.eu/en/treaties/dat/12006A/12006A.html

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

- Internal recipients: the JRC staff members who request the access for the TCN, their hierarchy, Local Security Officers JRC Safety & Security Coordinator DG HR Security Directorate

- External recipients: Contractors charged to implement and monitor the implementation of Security provisions (Site guards) – the information provided to the guards is limited to the name surname, passport number and the "access ok" decision. The text of the security opinion and the information included in the APPLICATION FORM (except for what mentioned above) is not provided to the guards.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

The JRC sites are subject also to national legislations that require different arrangements for what concerns the retention of personal data of people accessing their premises. The following arrangements apply:

ISPRA (DPO-2734.1 - JRC: Access Control System at JRC Ispra Site):

- Access Control System transactions and anomaly data are kept for 24 months.
- Access to Controlled Zones or Nuclear Areas, the retention period is 30 years due to legal requirements (e.g. to store personal radiation dosimetry data for health reasons).

PETTEN (DPO-1534.3 - JRC: access management system at JRC-IE in Petten):

- Recorded files are kept for 3 months. In case of incident the data will be kept for analysing for a longer period to establish, exercise or defend a right in a legal claim pending before a court.

SEVILLE (DPO-1426.5 - JRC: Access Control at JRC-IPTS in Seville)

- Identity and access profile data of IPTS statutory staff: retention is during the lifetime of the corresponding contract (i.e. associated with a valid staff pass).
- Access profile data of IPTS non-statutory staff who need to follow the 72 months rule: data must be kept for the last 24 months.
- Access profile data of external contractors' staff: retention is during the lifetime of the corresponding contract (i.e. associated with a valid staff pass).
- For access data: 5 years.
- Data of participants to workshops/meetings (managed by Scientific Units) are linked to the project file and are kept according to the requirements of the project. A copy is kept by Security Officer for a maximum of 6 months after the event.

GEEL (DPO-1177.6 - JRC: access control at JRC-Geel):

- Retention: minimum 30 years for nuclear control areas (regulatory requirement according Belgian Royal Decree of 20.07.2001). Retention period can be shortened to 5 years on request for persons not accessing nuclear controlled areas.

KARLSRUHE (DPO-1460.2 - JRC: entrance permission and access control for physical protection (ZES+ZKS) at JRC-ITU in Karlsruhe):

- Personal data of ITU-Staff and contractors staff will be deleted 5 years after expiration date of the security clearance.
- For visitors who have no access to nuclear areas the maximum retention period is 5 years after the last visit.
- For persons with access to nuclear areas and registered with dosimeter data the maximum retention period is 95 years after the date of birth of the data subject following Art. §42 of the German nuclear legislation (StrlSchV).

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

The data subject may access their data by submitting a request to the functional mailbox JRC-SAFETY-SECURITY-COORD@ec.europa.eu . Upon a justified request submitted by the data subject data to JRC-SAFETY-SECURITY-COORD@ec.europa.eu , the data will be rectified, 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.

After the expiry of the declared retention period, data could be kept for historical, statistical or scientific purposes in anonymous form or, if that is not possible, the identity of the data subject shall be encrypted.

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

The data are not transferred outside of the EU or EEA by the JRC staff.

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING

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

17/ COMMENTS

The process, somehow existing in the past although not in the form as proposed now, is a consequence of the review of the JRC security policy ("elimination of the Nulla Osta procedure") and of the new security measures introduced at Commission level (see the chapter 8 "Legal Basis"). [Mesures de sécurité liées à la présence de ressortissants de pays-tiers sans lien statutaire au sein de la Commission, Ares(2012)251857), 16/11/2012].

PLACE AND DATE: BRUXELLES, 16.09.2013

DATA PROTECTION OFFICER: RENAUDIERE PHILIPPE

INSTITUTION OR BODY: THE EUROPEAN COMMISSION