

REGISTER NUMBER: 937
NOTIFICATION FOR PRIOR CHECKING
<p>Date of submission: 20/12/2012</p> <p>Case number: 2012-1090</p> <p>Institution: European Commission</p> <p>Legal basis:</p> <p style="padding-left: 40px;">Article 27.2.(a) Processing of data relating to health and to suspected offenses, offenses, criminal convictions or security measures</p> <p style="padding-left: 40px;">Article 27.2.(b) Processing operations intended to evaluate personal aspects relating to the data subject</p> <p style="padding-left: 40px;">Article 27.2.(c) Processing operations allowing linkages not provided for pursuant to national or Community legislation between data process for different purposes(1)</p> <p style="text-align: right;">(1) OJ L 8, 12.01.2001</p>

INFORMATION TO BE GIVEN⁽²⁾
(2) Please attach all necessary backup documents

<p>1/Name of the processing</p> <p>Security Trustworthiness Check</p>
<p>2/Description</p> <p>Any member of staff needing unescorted access to nuclear and related <input type="checkbox"/> sensitive areas or information within the Ispra site must undergo a <input type="checkbox"/> Security 'Trustworthiness Check'.<input type="checkbox"/></p> <p>The supporting documentation necessary for processing Security <input type="checkbox"/> 'Trustworthiness Checks' includes only a recent Curriculum Vitae or <input type="checkbox"/> Application Form, with the exception of External Staff, contracted under a <input type="checkbox"/> supply or service contract with the European Commission, where a police <input type="checkbox"/> criminal record is also necessary. <input type="checkbox"/></p> <p>Processing of information falls under Article 27 for what concerns:<input type="checkbox"/></p> <p>(a) criminal convictions or security measures;<input type="checkbox"/></p> <p>(b) processing operations intended to evaluate personal aspects relating to <input type="checkbox"/> the data subject mainly concerning conduct;<input type="checkbox"/></p> <p>(c) processing operations for the purpose of excluding individuals from a <input type="checkbox"/> right, benefit or contract.<input type="checkbox"/></p> <p>It should be noted that the information regarding presence on-site of <input type="checkbox"/> people to be able to apply the Commission Decision C(2004) 1597 on the <input type="checkbox"/> maximum duration for the recourse to non-permanent staff in the commission <input type="checkbox"/> services(http://www.cc.cec/guide/publications/infoadm/2004/ia04075_en.html) <input type="checkbox"/> is no longer processed or collected by Security Service.</p>

3/Processors <input type="checkbox"/> NA
4/Automated / Manual operations <input type="checkbox"/> Security 'Trustworthiness Check' procedure.
5/Storage <input type="checkbox"/> Documentation associated with the Security 'Trustworthiness Check' is <input type="checkbox"/> currently kept only in digital format and on Direct Access Storage of <input type="checkbox"/> Security Service Servers connected to the Security Service Internal <input type="checkbox"/> Network, physically disconnected and not accessible from the outside world, <input type="checkbox"/> as well as Removable Media used for backup purposes.
6/Comments Documentation associated with the Security 'Trustworthiness Check' is only <input type="checkbox"/> available to a very restricted user population i.e. vetted Security Service <input type="checkbox"/> Officers and within a physically separate network, fully controlled and <input type="checkbox"/> managed by Security Service. <input type="checkbox"/> The Security 'Trustworthiness Check' procedure replaces the abolished <input type="checkbox"/> "Nulla Osta" procedure and represents the practical solution for the <input type="checkbox"/> implementation of the EDPS recommendations, where such a process is no <input type="checkbox"/> longer associated to staff recruitment to all JRC sites with the exception <input type="checkbox"/> of Karlsruhe but to unescorted access to nuclear and related sensitive <input type="checkbox"/> areas within the Ispra site. This has greatly reduced the actual scope both <input type="checkbox"/> in terms of the number of people concerned as well as physical areas <input type="checkbox"/> involved (recommendations 3.3.2./1.1/1.2/1.3/2.1 described in the EDPS <input type="checkbox"/> Inspection Report of March 2011). <input type="checkbox"/> Following the new Security 'Trustworthiness Check', the application of <input type="checkbox"/> Article 28 (c) of the Staff Regulations of Officials of the European <input type="checkbox"/> Communities concerning recruitment, focusing on appropriate character <input type="checkbox"/> references as to suitability for the performance of specific duties is now <input type="checkbox"/> currently performed by Human Resources and Recruitment Units. Identical <input type="checkbox"/> articles are analogously applied for other types of temporary staff.
7/Purposes <input type="checkbox"/> The purpose of the processing of personal data is to ascertain and confirm <input type="checkbox"/> the trustworthiness of people needing unescorted access to the JRC Ispra <input type="checkbox"/> nuclear and related sensitive areas. <input type="checkbox"/> <input type="checkbox"/> .

8/Legal basis and Lawfulness

Italian Law 906/1960 (see attachment) regarding establishment of the ☐
Joint Research Centre - Ispra.☐

☐

- Physical Protection Plan approved in Italian Ministry of Industry decree ☐
(see attachment) that includes all additional measures on top of those ☐
referenced in the IAEA INFCIRC/225 ☐
(http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf) and ☐
considered as implicitly the basis of such a document.☐

☐

- Commission Decision C(2001)3031, also known as 2001/844/EC, and ☐
Commission Decision C(2007)513/Euratom☐

- Memorandum of Understanding between Directorate General "Human Resources ☐
and Security Directorate" and the "Joint Research Centre" regarding the ☐
tasks performed in the field of Security (an updated version will follow ☐
the adoption of the expected new EC Security Decision).☐

☐

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 information and monitoring of information ☐
system security.☐

☐

Processing necessary in order to comply with International and Italian ☐
Legislation concerning Nuclear Sites.

9/Data subjects

☐

Any staff needing to unescorted access to nuclear and related sensitive ☐
areas or information of the Ispra Site (i.e. needing to undergo a Security ☐
'Trustworthiness Check'). It should be noted that this does not concern ☐
daily visitors that enter the site on an occasional basis, they will have ☐
to be escorted at all times if visiting sensitive areas of the JRC Ispra, ☐
and such data is kept only within SECPAC (DPO-722).

10/Data fields / Category

Data fields are associated to presented documentation and fall mainly outside the scope of Article 10.

□

PEOPLE - first_name, real_first_name, last_name, real_last_name, presentation_name, sex, title, birth_date, birth_place, birth_country, nationality, alias, staff_number, source_id, source, email, phone, start_v_date, end_v_date, [universal_id]

□

DOCUMENTS - doc_type_id, doc_id, [universal_id], doc_name, doc_state_id, doc_content (*), doc_creation_date, doc_descr, doc_note, inserted_by

□

DOCUMENT_TYPES - Application Form or alternatively the Curriculum Vitae , recent Police Criminal Record (only for External Staff, contracted under a supply or service contract with the European Commission), copy of associated supply or service contract (reference number) (for External Staff), Contract Extension, End of Contract, Permesso di Soggiorno (for non-italian residents), Autocertification, Authorisation, Data Collection Form, Derogation

□

Certain documentation may eventually fall under Article 10 but exemption is provided within point 5 of the same article (i.e. processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards) due to the legal obligations associated with the implementation of the 'Physical Protection Plan' which the Joint Research Centre has the legal obligation to implement.

11/Mandatory Information

□

Staff upon recruitment is informed through Human Resources Managers that they have to supply certain documentation and are aware their data may be used for the application of staff regulations and by Security Service for performing a Security 'Trustworthiness Check' in case their job concerns access nuclear and related sensitive areas or information.

□

This particular issue along some others is further detailed and explained regularly during the bi-monthly 'Newcomer's Security Briefings'.

12/Procedure to grant rights

The JRC Ispra Security Service to ensure transparency has envisaged a procedure where data subjects may request and verify what data is registered and associated with them. The JRC SECURITY ISPRA single point of contact (jrc-security-ispra@ec.europa.eu <mailto:jrc-security-ispra@ec.europa.eu>) is responsible for providing access or correcting personal data.

A specific procedure for updating or returning an 'Original Police Record' has been put in place (see attachment in point 19). This currently only concerns External Staff.

13/Retention

Data must be kept as long as there is a contractual link with the concerned person. It should nevertheless be kept for an additional period of 2 years after the conclusion of that contractual link i.e. retirement, temporary contract duration limits, etc.

As a consequence all personal and documental data related to Trustworthiness Checks will be deleted or rendered anonymous after that time. Exceptionally such information could be kept longer if duly justified in support of allowing the investigation of security breaches or incidents related to the concerned a person after leaving the Ispra site.

For what concerns data collected for candidate's that give up their job application or are not recruited but have had a Security Trustworthiness Check processed for them, data is kept for a period of 1 year.

Currently a set of semi-automatic procedures are used for performing such an analysis of the retention period, due to the varied and multiple possible scenarios, but a manual intervention is needed for deleting ARDOS documental information, exclusively in digital format.

14/Time limit

Upon a justified request from the Data Subject data will be modified, frozen or eventually erased in a maximum period of 14 days.

15/Historical purposes

Security Service has eliminated and screened all its paper documentation that has been kept for more time than mentioned in 13) and that is no longer needed.

16/Recipients

☐ The supporting documentation necessary for processing Security ☐
'Trustworthiness Checks' stored in ARDOS is for internal use of Security ☐
Service. Actual data is never directly transferred or accessible from ☐
outside Security Service as such information system resides in a physically ☐
isolated network.☐

☐ Security 'Trustworthiness Checks' being an internal process to Security ☐
Service does not involve any kind of information provision to other people. ☐
Only security vetted core Security staff can access the data. The Ispra ☐
Site Director may ask for extra information in case of an emergency or ☐
security investigations.

17/Transfer out of UE/EEA

Not applicable.

19/Complementary information

Further attached document: ARDOS_OriginalPoliceRecordUpdateReturnForm.pdf ☐
for updating or requesting original Police/Criminal record.☐

☐ This notification has been implemented following the enclosed EDPS final ☐
opinion (2007-380) of December 2008, the EDPS Inspection Report of March ☐
2011 (2010-834 D-494) and the recent EDPS follow-up report (2010-0834 ☐
D-2417) based on the complementary report of the 4th Quarterly Progress ☐
Report (Sept. 2012) addressing the main conclusions to be drawn for Chapter ☐
3 of the JRC Action Plan following the EDPS Inspection. See also the ☐
Decision of the JRC Director General about Security Clearances of July ☐
2012. ☐

Finally, enclosed a 'Note to the File' replying to EDPS recommendations and ☐
describing the decision taken by the JRC Director General regarding the ☐
abolishment of the Security "Nulla Osta" and the actions taken to implement ☐
new procedures and to define the corresponding legal basis. Note that an ☐
updated version of the Memorandum of Understanding between Directorate ☐
General "Human Resources and Security Directorate" and the "Joint Research ☐
Centre" regarding the tasks performed in the field of Security will follow ☐
the adoption of the expected new EC Security Decision.

PLACE AND DATE:20/12/2012

DATA PROTECTION OFFICER: PACKER Frida

INSTITUTION OR BODY:European Commission