Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on the Security opinions on the Third Country Nationals accessing the Joint Research Centre sites

Brussels, 22 July 2014 (Case 2013-1020)

1. Proceedings

On 17 September 2013, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer ("DPO") of the European Commission (Commission) a notification for prior checking regarding the processing operations carried out in the context of Security opinions on Third Country Nationals (hereafter 'TCN") accessing the Joint Research Centre ("JRC") sites.

The JRC developed the TCN procedure in close cooperation with the Commission's Directorate of Security (unit HR.DS.2), in response to two events:

- the abolition of the JRC *nulla osta* procedure (clearance procedure) as of 1 September 2012[1], causing a lack of JRC security policy concerning, among other features, the screening of TCN accessing all the JRC sites but the *Karlsruhe* one;
- the instruction by DG HR to ensure, without delay, adequate screening of TCN accessing the Commission premises.

Following the abolition of the *nulla osta* procedure, the Commission submitted a JRC Security 'Trustworthiness Check' procedure (Case 2012-1090) that covers the processing of personal data for any staff needing unescorted access to nuclear and related sensitive areas or information of the *Ispra* site.

The TCN procedure was implemented as of 1 September 2013 and thus prior to its notification on 17 September 2013, making the analysis an ex-post control of a processing operation.

On 19 June 2014 the EDPS sent the draft Opinion to the DPO for comments. The feedback was received on 7 July 2014.

2. Facts

The ***purpose*** of the processing operation is to allow the JRC hierarchy to take a decision whether to grant or refuse TNC access to the JRC sites. The TCN procedure defines in which

[1] Decision of 11 July 2012 by the Director General of the JRC. This decision followed, among others, an inspection conducted at the JRC in 2010 (Case 2010-0832) where the EDPS questioned the lawfulness of the *nulla osta* procedure in place at the JRC.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

circumstances security screening is requested as well as preventive measures and countermeasures that can be introduced in that context. The JRC maintains working-level contacts with scientific establishments from different countries, which may imply presence at the JRC sites of staff seconded from those establishments and frequently requires admitting visitors taking part or assisting in JRC activities taking place on its sites. The specificity of JRC tasks may also require the presence on the different JRC sites of external contractors (or bidders – at the stage of contract preparation and negotiation) providing services commissioned by the JRC. Many of these are TCN. Some TNC are potential staff members invited for e.g. job interviews (such as grant-holders, visiting scientists, etc.).

The ***procedure*** involves the processing of personal data within the meaning of the Regulation (EC) No. 45/2001 (henceforth: the Regulation). Each JRC staff member requesting access for a TCN to a JRC site fills in an application form containing all personal data relevant for the exercise (see below). On the basis of the information provided, the security opinion is issued by the Local Security Service. Before issuing the opinion, 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.

Regarding the ***legal basis***, the JRC identified the following:

- Commission Decision of 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 regard to the JRC;
- Memorandum of Understanding (MoU) 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.

As noted in case 2012-1090, the Commission will adopt a new Security Decision on the basis of which a new MoU will be adopted between the DG HR/DS and the JRC. This Decision and this MoU will clarify the competences of the different services involved and form the legal basis of different processing operations, including the TCN procedure. Neither document has so far been adopted.

The ***controller*** is the Commission represented by the JRC Director of Resources. Subcontractors of Security Services attached to the Local Security Officers of each JRC site may process the data as ***processors*** on behalf of the controller.

The ***data subjects concerned*** are natural persons (not legal entities, associations, foundations, etc.) accessing the JRC sites who are TCN.

The ***processed data***, which are provided by the data subject and are accompanied by paper evidence, are:

- 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(s) and length of stay on those sites;
- Documents that contain personal data: CV, the extract of the criminal record and the opinion of the JRC sites Local Security Officer/HR Security Directorate.

Independent of the security service capabilities and tools used on the different JRC sites, the data are processed manually or by computer to prepare a file consisting of the application form and the TCN security opinion.

As to the ***conservation period***, the notification underlines that the JRC sites are subject to national legislation that requires different arrangements as to the retention of personal data of people accessing their premises, which also depends on the security level of the area accessed. According to the notification, the following arrangements apply:

- *Ispra*[2]: Access Control System transactions and anomaly data are kept for 24 months, regarding 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*[3]: Files are kept for 3 months. In case of an incident, the data will be kept for analysis for a longer period where necessary to establish, exercise or defend a right in a legal claim pending before a court.
- *Seville*[4]: The identity and access *profile* data of statutory staff is retained during the lifetime of the corresponding contract (i.e. associated with a valid staff pass); for non-statutory staff data is kept for 24 months. Access *profile* data of external contractors' staff is retained during the lifetime of the corresponding contract (i.e. associated with a valid staff pass). Access data is kept for 5 years. Personal data of participants in workshops/meetings (managed by Scientific Units) is linked to the project file and are kept according to the requirements of the project. A copy is kept by the Security Officer for a maximum of 6 months after the event.
- *Geel*[5]: The retention period is minimum 30 years for nuclear control areas and can be shortened to 5 years on request for persons not accessing nuclear control areas[6].
- *Karlsruhe*[7]: Personal data of staff and of contractors 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, according to the notification, the maximum retention period is 95 years after the date of birth of the data subject[8].

Regarding the ***recipients*** of the data, the JRC differentiates between internal and external recipients:

- *Internal recipients*: the JRC staff members who request the access for the TCN, their hierarchy, the Local Security Officers, the JRC Safety and 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

[2] DPO-2734.1 - JRC: Access Control System at JRC *Ispra* site.
[3] DPO-1534.3 - JRC: access management system at JRC-IE in *Petten.*
[4] DPO-1426.5 - JRC: Access Control at JRC-IPTS in *Seville.*
[5] DPO-1177.6 - JRC: access control at JRC-*Geel.*
[6] The notification refers to Article 30(1) of the Royal Decree of 20 July 2001 laying down the General Regulation for the protection of the public, workers and the environment against the hazards of ionizing radiation, as amended
[7] DPO-1460.2 - JRC: entrance permission and access control for physical protection (ZES+ZKS) at JRC-ITU in *Karlsruhe.*
[8] The notification refers to §42 of the German *Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung - StrlSchV*, which reads: "*Die Aufzeichnungen sind so lange aufzubewahren, bis die überwachte Person das 75. Lebensjahr vollendet hat oder vollendet hätte, mindestens jedoch 30 Jahre nach Beendigung der jeweiligen Beschäftigung. Sie sind spätestens 100 Jahre nach der Geburt der betroffenen Person zu löschen*".

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 is mentioned above) is not provided to the guards.

Regarding the ***right to information***, a Privacy Statement is provided to each data subject via e-mail by the staff member requesting the access for the TCN to the JRC site before the JRC starts collecting the information necessary to complete the form. It is also available upon request and published on the JRC internet website. The Privacy Statement contains information on the purpose of the processing operation (with a short description), the personal data collected, the identity of the controller, the information on the relevant legal basis, the recipients of the data, the security of the data storage as well as the time limits for storing the data (making reference to the fact that the retention of personal data depends on the national legislation for each JRC site, as well as the security level of the area accessed; it provides a link to the retention periods of all the sites). It also contains information on the rights of access and rectification. Finally, it also states the right to have recourse to the European Data Protection Supervisor.

As regards the ***rights of access and rectification***, the data subjects can exercise the following rights by sending an e-mail containing a justified request to a functional mailbox address:

- The right of access to 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);
- The right to rectify inaccurate or incomplete personal data held by the controller; the data will be rectified or modified in a maximum period of 14 days.

As regards ***security measures***,
...

3. Legal analysis

3.1. Prior checking

This Opinion relates to the processing of personal data in the context of the TCN procedure. The processing activity is carried out by a European institution, in the exercise of activities which fall within the scope of EU law (Article 3(1) of Regulation (EC) No. 45/2001, henceforth: "the Regulation"). The processing of personal data is done, at least partly, by automatic means (Article 3(2) of the Regulation). As a consequence, the Regulation is applicable.

Article 27(1) of the Regulation subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

The EDPS considers that such data processing operation falls under Article 27(2)(a) of the Regulation, which establishes that processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" shall be subject to prior checking by the EDPS. In the case at hand, by processing the abovementioned data, the security service may process information related to alleged offences or criminal convictions.

Although not referred to in the notification, the EDPS considers that the notification also falls under Article 27(2)(b) of the Regulation which stipulates that processing operations which *"evaluate personal aspects relating to the data subject, including his or her (...) conduct*" shall

be subject to prior checking by the EDPS. In the present case, the conduct of individuals will be evaluated in order to ascertain whether access can be granted to the JRC sites, thus triggering the application of Article 27(2)(b) of the Regulation as was the case for the Security 'Trustworthiness Check' procedure[9].

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operation by the Commission had already been established. The recommendations issued by the EDPS should however be fully implemented. As this is considered an ex-post notification, the two-month period within which the EDPS must deliver an Opinion pursuant to Article 27(4) of the Regulation does thus not apply to this notification, which has been treated on a best effort basis.

3.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation.

The EDPS considers that the processing operation falls both under Article 5(a) of the Regulation, pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof* (...)*"* and Article 5(b) of the Regulation, as the processing is necessary for compliance with a legal obligation to which the JRC is subject. Indeed, national legislation of different Member States requires different arrangements as regards security checks of individuals accessing the JRC sites located on their territory[10]. In particular, such specific national legislation foresees different retention periods for the personal data as described in the facts.

The EDPS takes note of the following EU legal instruments[11], which provide some legal ground for the processing operations that take place:

- 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 JRC;
- Memorandum of Understanding between DG HR/DS and JRC on tasks performed in the field of security, Ares (2010)884864 – 30/11/2010, **once updated;**
- 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;
- Furthermore, national legislation imposing specific measures contribute to the legal basis as they impose specific procedures to the JRC sites.

However, as already stated by the EDPS in the Security 'Trustworthiness Check' case (Case 2012-1090)[12], the future Commission's Security Decision on and the updated MoU between DG JRC and DG HR are of paramount importance to empower the JRC to carry out such security procedures. Both will also ensure the lawfulness and the legitimacy of the security

[9] See EDPS Opinion of 19 June 2013 on a notification for Prior Checking received from the Data Protection Officer of the Commission on the Security Trustworthiness Check at the Joint Research Centre Ispra (case 2012-1090).

[10] As noted in the Security 'Trustworthiness Check' case (2012-1090), there are for instance specific obligations for the JRC *Ispra* site as nuclear operator and holder of a nuclear licence under Italian law to implement different security measures.

[11] The Commission Decision C(2001)3031 (also 2001/844/EC) mentioned in the notification is not considered relevant in this case.

[12] At the time of the analysis of case 2012-1090, the EDPS already stressed the need to base such security related procedures on the new Security Decision and Memorandum of Understanding.

opinions on the TCN accessing the JRC sites' processing operation. Failing the adoption of this Decision and the MoU, the legal basis for the processing of personal data cannot be considered complete. **The EDPS consequently recommends adopting both, the Commission's new Security Decision and the updated MoU, as a matter of urgency.**

As to the necessity of the processing, the EDPS notes that the processing of personal data in the context of the TCN procedure is considered as necessary for compliance with EU and national provisions applicable to the JRC sites.

3.3. Processing of Special Categories of Data

Taking into account the purpose of the processing, certain documentation may fall under Article 10 of the Regulation. In this regard, the EDPS highlights the application of Article 10(5) of the Regulation, which establishes that *"[p]rocessing 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"*. In the present case, this exemption may apply due to the legal obligations to which the JRC sites are subject (see legal instruments mentioned in the facts and in point 3.2 above).

3.4. Data Quality

Pursuant to Article 4(1)(c) of the Regulation, personal data must be *"adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed"*. The personal data processed in the present case seems to be limited to what is necessary in order to comply with the purpose of the TCN procedure, hence complying with Article 4(1)(c) of the Regulation.
According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and where necessary kept up to date"*, and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified".* As regards extracts of criminal records, it should be noted that such documents have a very limited period during which they can be considered accurate. Therefore, the EDPS invites the JRC to assess the necessity to keep such extract beyond a certain period (see also point 3.5 below).

3.5. Conservation of Data/Data Retention

Pursuant to Article 4(1)(e) of the Regulation, personal data may be kept in a form which permits the identification of data subjects for *"no longer than is necessary for the purposes for which the data were collected and/or further processed"*. The processing operation foresees different retention periods depending on the national legislation applicable for each JRC site, as well as the security level of the area accessed, as described in the facts. In the light of the information provided on the national legislation applicable for each JRC site, the EDPS sees no reason for concern as regards the necessity and proportionality of the retention periods applied in the light of the objective pursued by the TCN procedure.
However, as stated above, the personal data contained in an extract of criminal records have a very limited period during which they can be considered accurate. Therefore, the EDPS considers that the retention period of the extract of criminal record should be limited to a maximum of two years after it has been provided. Indeed, this corresponds to the period during which the European Court of Auditors would check such document (for further processing). As formally accepted by the European Court of Auditors in case 2011-0482, records that have

been checked before this deadline can be destroyed earlier. The EDPS recommends modifying the retention period applicable to extracts of criminal records in order to reflect this.

3.6. Processing on behalf of the controller

The procedure specifically foresees that processors may process data on behalf of the controller, as subcontractors of security services attached to the Local Security Officers of each JRC site may process the data on behalf of the controller.
The EDPS recalls that processing of personal data on behalf of the controller must be secured by a contract or legal act binding the processor to the controller and must meet the following minimum requirements stipulated in Article 23 of the Regulation: the contract must stipulate that the processor shall act only on instructions from the controller and the processor must provide sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out as well as ensure compliance with such measures.
The EDPS therefore recommends that JRC ensure that the requirements under Article 23 are met and invites the JRC to provide the EDPS with the respective documents.

3.7. Rights of Access and Rectification

Article 13 of the Regulation establishes a right of access and the arrangements for exercising it upon request by the data subject. It encompasses the right to be informed that information relating to him/her is processed by the controller and to obtain the communication of such data in an intelligible form. Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data without delay. The Privacy Statement gives a functional mailbox as a dedicated contact point to exercise these rights and foresees that upon a justified request submitted to the functional mailbox, the data will be rectified or modified in a maximum period of 14 days. The EDPS has no reason for concern as regards compliance with the requirements under Articles 13 and 14 of the Regulation.

3.8. Information to the Data Subject

The obligation to inform data subjects is enshrined in Articles 11 and 12 of the Regulation. As part of the TCN procedure, a Privacy Statement is provided before collecting the information necessary to complete the TCN form.
The EDPS would like to note that the Privacy Statement refers to links or internal documents of the Commission or of the JRC that may not be available to the data subjects who may not have a direct access to these resources. For instance, the Privacy Statement provides for information on the national legislations applicable to each JRC site and the respective retention periods by means of a mere link to the register of the DPO of the Commission. The EDPS considers that providing such a link to the register of the DPO is not sufficient to ensure correct information of the data subjects, as they may not have access to this register.
Therefore, the EDPS invites the Commission to ensure that information on the national legislations applicable to each JRC site and the respective retention periods is provided in an easier accessible way to the data subjects. Furthermore, the references to the Commission's new Security Decision and the updated MoU will have to be introduced, once these Decisions are adopted.
As to the other elements of information provided in the Privacy Statement, the EDPS considers that it contains the information required under Articles 11 and 12 of the Regulation.

3.9. Security Measures

...

4. Conclusion

The EDPS is concerned that the Commission's announced new Security Decision and the MoU relevant for this processing operation and the one in case 2012-1090 have not been adopted yet. Both are of great importance as legal basis for several processing operations. Therefore, the EDPS specifically highlights that all efforts must be made to adopt such a Decision and MoU as a matter of urgency, in order to avoid any gap in the lawfulness of the processing operations concerned. **The EDPS consequently urges the Commission to adopt the new Security Decision and the MoU as soon as possible.**

The following recommendations must be taken into account by the Commission. The Commission must:

- ensure that the Commission's new Security Decision and the updated MoU are adopted as a matter of urgency and provide these to the EDPS as soon as they become available;
- modify the retention period applicable to extracts of criminal records;
- ensure that the Privacy Statement itself contains comprehensive information;

...

Done at Brussels, 22 July 2014

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor