Opinion 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

Brussels, 19 June 2013 (Case 2012-1090)

1. Proceedings

On 20 December 2012, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer ("DPO") of the Commission a notification for prior checking regarding the processing operations carried out in the context of Security Trustworthiness Check at the DG Joint Research Centre in Ispra ("JRC Ispra").

The notification under analysis follows the decision of 11 July 2012 by the Director General of the JRC to abolish the *nulla osta* screening procedure in place for recruitments of selected candidates to the JRC Sites. The decision follows an inspection conducted at the JRC in 2010 (Case 2010-0832) where the EDPS questioned the lawfulness of the the *nulla osta* procedure in place at the JRC.

In re-placement, the JRC is submitting a draft procedure of security trustworthiness screening named Security 'Trustworthiness Check' procedure. Such a process is no longer associated to staff recruitment to all JRC sites[1] with the exception of Karlsruhe but to unescorted access to nuclear and related sensitive areas within the Ispra site. This has greatly reduced the scope both in terms of the number of people concerned as well as physical areas involved.

Ten annexes were sent with the notification. As one of the annexes, a note to the file provides information on the implementation of some specific recommendations made in the inspection report that lead to the development of the trustworthiness security check.

As explained in the note to the file, to safeguard the need to uphold specific security measures for high risk areas, Directors may implement necessary security related screenings. Such possibility is, however, very confined in nature as:
- may only be imposed for what concerns access to restricted areas, with an indication of nuclear (contrary to the abolished *nulla osta* procedure which applied to the recruitment of staff), and

[1] The JRC has ceased the *nulla osta* proedure for its sites in Petten, Sevilla, Geel and Brussels and this procedure has equally been lifted for the Ispra site, albeit maintaining a security related screening for accessing "sensitive areas" (including nuclear areas).

- where required by Commission standards and/or applicable local, regional and/or national security obligation, and
- in compliance with data protection rules.

In the exchanges with the JRC, it was clarified that the JRC has a specific mandate through a Memorandum of Understanding ("Memorandum") between the Directorate General Human Resources and Security/Security Directorate ("DG.HR.DS") and the Joint Research Centre to conduct certain types of security investigations.

After a first analysis of the notification, on 9 January 2013, the EDPS contacted both the DPO and the JRC as controller underlining that the notification was not in line with the EDPS third follow-up report to the JRC. In this letter, the EDPS stressed the need to base the procedure on the new Security Decision and Memorandum of Understanding. Indeed, as noted in the e-mail, at the time of analysis, the Commission Security Decision C(94)2129 which defines the general tasks of the Security Service was under revision. As it was explained in the note to the file, the draft of this new Decision includes an article on "*the security measure which the Commission may - under strict observation of fundamental rights and principles of legality, transparency, accountability, subsidiarity and proportionality - undertake. The description of such measures includes, inter alia, systematic a priori security cheks, in order to prevent and control threats to security, of persons accessing its premises*.". The draft equally contains a provision, providing for the possibility that certain security checks may -by means of the signature of an implementing act- be performed at local level, such as the JRC Ispra Security Service. This will lead to the adoption of a new Memorandum of Understanding (MoU).

At the time of drafting of this Opinion however, discussions between DG.HR.DS and the JRC were still ongoing.

At the same time, the JRC is in a position where it must implement mandatory security screenings for access to its nuclear restricted areas. The JRC is subject to the recommendation 4.26 of the document (INFCIRC/225/fifth) from the International Atomic Energy Agency (IAEA) which states that "persons authorized unescorted access to the protected area should be limited to those whose trustworthiness has been determined" and to the Physical Protection Plan approved in Italian Ministry of Industry decree.

Therefore the EDPS has decided to conduct his legal analysis on the basis of the information received even though the new Commission decision and MoU are not finalised in order to avoid a security loophole. The EDPS had access, through the JRC note, to relevant parts of the draft Decision and was told by the JRC that the new MoU will only slightly differ from the current one.

Therefore, this Opinion is without prejudice to additional comments which the EDPS may make when the new Security Decision and new MoU will be adopted.

On 31 May 2013 the EDPS sent the draft Opinion to the DPO for comments. The feedback was received on 14 June 2013.

2. Examination of the matter

2.1 The Facts

The ***purpose*** of the processing of personal data is to ascertain and confirm the trustworthiness of people needing unescorted access to the JRC Ispra nuclear and related sensitive areas.

The supporting documentation necessary for processing Security 'Trustworthiness Checks' includes a recent Curriculum Vitae or Application Form, with the exception of External Staff, contracted under a supply or service contract with the European Commission, where a police criminal record is also necessary. A "Permesso di soggiorno" for non-italian residents is also necessary.

Following the new Security 'Trustworthiness Check', the application of Article 28 (c) of the Staff Regulations of Officials of the European Communities concerning recruitment, focusing on appropriate character references as to suitability for the performance of specific duties is now currently performed by Human Resources and Recruitment Units. Identical articles are analogously applied for other types of temporary staff.

The notification stresses that the information regarding presence on-site of people to be able to apply the Commission Decision C(2004) 1597 on the maximum duration for the recourse to non-permanent staff in the commission services is no longer processed or collected by the Security Service.

As to the ***data subjects concerned***, it applies to any staff needing 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 (2007-0381).

The ***processed data*** are classified in the following categories: people, documents and document types.

- 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 and end v date, [universal id]

- 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 and Derogation.

According to the notification, data fields are associated to presented documentation and fall mainly outside the scope of Article 10 of the Regulation. It is also stated that certain documentation may eventually fall under Article 10.

As to the mandatory aspect of this information, the notification foresees that staff upon recruitment is informed through Human Resources Managers that they have to supply certain documentation and are made aware that 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'.

The ***primary responsibility for the data processing*** lies with the Unit for Safety and Security of JRC Ispra. He reports directly to the Director of the Ispra Site Management.

As to the ***conservation period***, the notification foresees that data must be kept as long as there is a contractual link with the concerned person and that 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.

The collected personal data and all information related to the above mentioned processing is stored on dedicated servers of JRC Ispra Security Service, the operations of which underlie the Commission's IT Security decisions and provisions for this kind of servers and services.

Access to data is done with unique individual access protected by a username/password. Within Core Security Service staff, there are also several profiles which include *Security Officer* and *Security Archivist and Administrator*. Security Officers may access personal data. *Security Archivists* may access all registered information including documental information. *Administrators* have full access to full ARDOS functionality which includes the management of such profiles.

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.

It is also stated in the notification that Security Service has eliminated and screened all its paper documentation that has been kept for more time than mentioned above and that is no longer needed. The JRC clarified that with regard to the historical documentation collected in the context of the Nulla Osta procedure, as far as the documentation stored in paper format is concerned, the JRC effectively destroyed all the documentation that was in its possession. In what concerns other possible electronic documentation collected for the Nulla Osta check, the JRC states that a procedure which will delete all information which can be uniquely identified to be exclusively linked to the Nulla Osta (e.g. application forms, CV's, etc.) is being elaborated and will be concluded by the end of 2013.

Regarding the ***recipients*** of the data, 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.

Regarding the ***right to information***, a specific privacy statement was annexed to the notification and stresses that individuals can address queries concerning this processing

operation. It states that queries can be addressed to the controller through a specific functional e-mail as a single contact point and it provides contact details about this. It states that the purpose of the processing of personal data is to ascertain and confirm the trustworthiness of people, associated with a corresponding long-term authorisation request.

As to the privacy statement itself, it contains information on the purpose of the processing operation (with a short description), the identity of the controller, the information on the relevant legal basis, the recipients of the data, the data storage as well as the time limits for storing the data. 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 far as the ***rights of access and rectification*** are concerned, in order to ensure transparency, the JRC Ispra Security Service 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 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. Such request has to be made using the "original police record update or return form". This currently only concerns External Staff.

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

As regards ***security measures***, the notification refers to the detailed answers to the questions related to the implementation of technical and organizational measures adopted for ARDOS.

[...]

2.2. Legal aspects

2.2.1. Prior checking

This prior check Opinion relates to the processing of personal data in the context of JRC Ispra Security trustworthiness check. 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 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 Regulation (EC) No 45/2001 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.
According to the JRC as controller, processing of information falls under Article 27 for what concerns:
(a) criminal convictions or security measures;
(b) processing operations intended to evaluate personal aspects relating to the data subject mainly concerning conduct;
(c) processing operations for the purpose of excluding individuals from a right, benefit or contract.

In the first place, such data processing operations fall under Article 27.2(a) of Regulation (EC) No 45/2001, 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 in point, by processing the abovementioned data, the security service may process information which may relate to alleged offences/criminal convictions. The reference to the notion of security measures in Article 27.2(a) is not relevant as the interpretation of security measures is not understood as such as the described measures[2].

In addition, the notification also falls under Article 27.2(b) of the Regulation (EC) No 45/2001 which stipulates that data 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 case under analysis, the conduct of individuals will be evaluated in order to ascertain their trustworthiness, thus triggering the application of Article 27.2(b).

Finally, the EDPS does not consider that Article 27.2(d) would apply here. Indeed, this provision refers to processing operations the aim of which is to exclude individuals from a right, a benefit or a contract (this typically refers to black lists). This does not seem to be the purpose of the trustworthiness check which aim is, on the contrary, to allow unescorted access to the JRC site.

Ex-ante prior checking. 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, the processing should replace the abolished nulla osta procedure and should therefore be considered ex-ante and any recommendation should be taken into account before the implementation of the procedure.

Notification and due date for the EDPS Opinion. The notification of the DPO was received on 20 December 2012. The analysis was suspended between 9 January 2013 and 23 April 2013, day where the case was unsuspended. The draft was sent for comments on 31 May 2013 and these were received on 14 June 2013. Therefore, the two-month period within which the EDPS must deliver an Opinion was suspended during 104 days + 14 days to enable the DPO and the JRC as controller to provide comments on the EDPS Draft Opinion. The Opinion should therefore be adopted no later than 19 June 2013.

2.2.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in article 5 of Regulation (EC) No 45/2001.

The notification states that the lawfulness of the processing falls under Articles 5(a), 5(b), 5(d), 5(e) of the Regulation. However, of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the EDPS considers that the processing operation notified for prior checking only falls under Articles 5(b) *-the processing is necessary for compliance with a legal obligation to which the JRC is subject-* and 5(a), 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* (...)*".*

As stated in the proceedings, the JRC is subject to the recommendation 4.26 of the document (INFCIRC/225/fifth) from the International Atomic Energy Agency (IAEA) which states that "persons authorized unescorted access to the protected area should be limited to those whose trustworthiness has been determined" and to the Physical Protection Plan approved by the Italian Ministry of Industry decree and therefore Article 5(b) of the Regulation applies. JRC

[2] Indeed, the reference in Article 27.2(a) actually refers to what are considered "safety measures" or "mesures de sûreté" as adopted in the French version of the Regulation.

Ispra as nuclear operator and holder of a nuclear licence under Italian law is obliged to implement many different security measures.

As stated in his third inspection follow-up report of 5 December 2012 the EDPS recommended that this legal obligation be completed with the new Commission's Decision on security and the updated MoU. Indeed, the Italian decree and the IAEA stipulate the principle of trustworthiness check but do not described how and by whom (between the JRC security service and DG HR/DS) this check must be conducted. In addition, if one can deduce from the IAEA recommendation that the trustworthiness determination will entail the collection and processing of personal data, the recommendation does not as such impose the processing of personal data.

For this reason the future new Commission Decision on Security and the updated MoU between DG JRC and DG HR are of paramount importance to reinforce the empowerment to the JRC for carrying out security checks and therefore strengthen the lawfulness and the legitimacy of the Security Trustworthiness Check processing operation.

Both the new Commission's Decision on security and the new MoU will have to be provided to the EDPS in order to be analysed as they complement the current 5(b) ground (Italian Law) with the 5(a) ground.

As a consequence the EDPS takes note of the following legal instruments, which provide the legal grounds that legitimise processing operations that take place in the context of conducting investigations:

- Italian Law 906/1960 regarding establishment of the Joint Research Centre-Ispra;

- Physical Protection Plan approved in Italian Ministry of Industry decree) that includes all additional measures on top of those referenced in the IAEA INFCIRC/225 [3] and considered as implicitly the basis of such a document;

- Commission Decision of 8 September 1994 on the tasks of the Security Office of the European Commission[4], **once revised;**

- 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), **once updated**.

As to the necessity of the processing, besides the reference to the new Commission's Decision on security and the new Memorandum of understanding, the EDPS considers that the processing is necessary in order to comply with international and Italian legislation concerning nuclear sites.

Taking into account the forthcoming Decision and the new Memorandum, the EDPS considers that the legal ground foresees the tasks of the security services of the JRC Ispra, based on the existing rules applicable in the European Commission.

[3] http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

[4] The Commission Decision C(2001)3031 (also 2001/844/EC) and Commission Decision C(2007)513/Euratom mentioned in the notification is not considered the main relevant document in this case.

2.2.3. Processing of Special Categories of Data

Taking into account that the purpose of the processing is to ascertain and confirm the trustworthiness of people needing unescorted access to the JRC Ispra nuclear and related sensitive areas, certain documentation may eventually fall under Article 10.

In this regard, the EDPS recalls the application of Article 10.5 of Regulation (EC) No 45/2001 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, an exemption is provided under Article 10.5, i.e. such processing data is authorised 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 (cfr legal instruments mentioned in point 2.2.2 above.).

2.2.4. Data Quality

Pursuant to Article 4.1.c of Regulation (EC) No 45/2001, personal data must be *"adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed"*.

The data that are processed in the context of the Trustworthiness Security check seems to be limited to what is necessary in order to comply with the purpose of the processing operations, hence complying with Article 4.1.c of Regulation 45/2001.

As regards criminal records, the JRC makes reference to the term "Police Record". As stated in the procedure regarding the inspection at the JRC (2010-0834), the EDPS already expressed that this term should not be used. Only an extract of criminal records delivered by the competent authority of the relevant country can be collected. Therefore, documents like "certificate of good conduct" or similar should not be collected, except where a national criminal record does not exist in that country. Furthermore, the EDPS recalls that the JRC created a list of so-called "extracts of criminal records" for all the Member States in the languages of origin. This document is the one that should be requested. Therefore, the EDPS invites the JRC to amend the terms that is currently being used in the planned procedure. Furthermore, given the numbers of foreign nationals involved, the candidates should also be informed whether the extract of the criminal records should come from their country of current and/or past residence, and/or their country of nationality".

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 the extract of criminal records, such document has a very limited period during which it can be considered accurate. Therefore, the EDPS invites the JRC to assess the necessity to keep such extract for a long period (see also point 2.2.5 below).

2.2.5. Conservation of Data/ Data Retention

Pursuant to Article 4 (1) e) of Regulation (EC) No 45/2001, 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.

1) The JRC foresees the retention of data for as long as there is a contractual link with the concerned person (whether internal or external staff). An additional period of 2 years after the conclusion of that contractual link is also foreseen (i.e. retirement, temporary contract duration limits, etc.).

The EDPS takes note that the JRC considers this retention as necessary for the trustworthiness processing operation. However, as concerns the extract of criminal records and as analysed above, the data contained in an extract of criminal records have a limited period during which they can be considered accurate. Therefore, the EDPS questions the retention period of the extract of criminal record, which he considers should be limited to a maximum of two years after it has been provided. Indeed, this would correspond to the period during which the Court of Auditors would check such document (for further processing). Records that have been checked by the Court of Auditors before this deadline can be destroyed earlier. This interpretation has been formally accepted by the Court of Auditors. The retention period foreseen in the notification and privacy statement should be modified in order to reflect this.

2) After the period foreseen under point 1, it is foreseen that all personal and documental data related to *Trustworthiness Checks* will be deleted or rendered anonymous but that, 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 person after leaving the Ispra site.

The EDPS takes note that the JRC Ispra considers this retention period as necessary for the purpose of further processing in case of investigations. The EDPS wants to insist that such retention should however be exceptional and duly justified.

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. The EDPS takes note of this retention period.

The JRC also states in the notification that the Security Service has eliminated and screened all its paper documentation that has been kept for more time than mentioned above and that is no longer needed. The EDPS understands that this procedure applies to the Nulla Osta documents which have been collected through the years before the Director General of the JRC decided to abolish this procedure. Indeed, although the EDPS welcomes that a procedure is foreseen for any new data being processed in the context of the Trustworthiness Security check, it is also important that the JRC establishes rules about the already existing data

2.2.6. Transfer of Data

On the basis of the information provided, only Article 7 of Regulation (EC) No 45/2001 applies. Indeed, actual data is never directly transferred or accessible from outside Security Service as such information system resides in a physically isolated network. Furthermore, only security vetted core Security staff can access the data and the Ispra Site Director may ask for

extra information in case of an emergency or security investigations. As stated in the documents received (Privacy statement). The Security Service, responsible for managing access to the Ispra site, may also transfer data for security reasons to the Security Directorate (DG HR/DS) of the Commission.

Data may be transferred to European Union institutions and bodies such as OLAF, IDOC, the EDPS, or to the European Ombudsman within their sphere of competence.

Given the competences of the recipient bodies, it appears that such data transfers are necessary for the legitimate performance of tasks covered by the competences of the recipients. Besides, the new security rules will also clearly have to distinguish between the competences of the JRC and the competences reserved to DG.HR.DS. in terms of security and the cases under which such transfers could take place.

In any case, notice has to be given to the recipient that, in accordance with Article 7.3 personal data can only be processed for the purposes for which they were transmitted.

No transfer of personal data to Member States or to third countries is foreseen.

2.2.7. Rights of Access and Rectification

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the data controller. According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source.

The privacy statement states that individuals direct queries (to verify which personal data is stored, to have it modified, corrected or deleted) concerning this processing operation to the data controller. It gives a functional e-mail box as a dedicated contact point to exercise this right.

2.2.8. Information to the Data Subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, the controller is required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Article 11 refers to information to be supplied where the data have been obtained from the data subject and Article 12 refers to information to be supplied where the data have not been obtained from the data subject. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The JRC as controller provided a privacy statement covering the security trustworthiness check. The notification does not contain, however, information as to how this privacy statement is handed over to the data subjects. The notification contains the following statement: "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. Therefore, the EDPS would like to stress that the privacy statement should be provided at that moment. This

should be made clear in the procedure Furthermore, as regards external staff of a subcontractor, the privacy statement should be provided at the time where the data are being collected.

The EDPS has also checked the content of the information provided in the privacy statement and considers that it contains the information required under Articles 11 and 12 of Regulation (EC) No 45/2001. Indeed, it contains information on the purpose of the processing operation (with a short description), the identity of the controller, the information on the relevant legal basis, the recipients of the data, the data storage as well as the time limits for storing the data, a functional e-mail for queries. However, the references to the new Commission's Decision on security and the new Memorandum of Understanding will have to be made, once they are adopted.

2.2.9. Security Measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller must implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

[...]

Therefore, the EDPS has no reason to believe that JRC has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided the considerations in this Opinion are fully taken into account. In particular, JRC Ispra must implement the following:

- comply with the retention periods established for the processing of the extract of criminal records,
- foresees that the privacy statement is provided to the different data subjects concerned (internal as well as external staff) at the appropriate moments and is amended accordingly, as explained above,
- Provides the EDPS with the relevant documents forming the legal basis (new European Commission Decision on security and new Memorandum of Understanding) when these documents are available.

Done at Brussels, 19 June 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor