Opinion on a notification for Prior Checking received from the Data Protection Officer of the Commission on the Security Investigations at the Joint Research Centre Petten

Brussels, 19 March 2013 (Case 2012-0782)

1. Proceedings

On 10 September 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 investigations at the DG Joint Research Centre in Petten ("JRC Petten").

This notification follows the withdrawal by the Commission of a first notification on "investigations by staff of safety environment security sector (SES) at JRC-IE in Petten" (case 2008-0013). The reason given for the withdrawal is that the analysis of the processing operations by the JRC Petten has shown that the legal regimes for investigations are very different for the different areas covered in the notified processing operations. The JRC clarified that it 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, whereas safety and environmental incident investigations in most cases are linked to requirements of national legislation. Therefore, JRC Petten notified two different processing operations, one on safety and environmental inspections (2012-0783) and one on security investigations (2012-0782) at the JRC Petten site.

The EDPS also notes that the JRC had already notified processing operations in the context of security investigations for another of its centres, namely JRC Ispra (case 2007-0507). The processing operations were analysed before the adoption of the abovementioned Memorandum. Lastly, the EDPS notes that the Commission Security Decision C(94)2129 which defines the general tasks of the Security Service is under revision and a new security decision will contain a provision, providing for the possibility of performing certain security checks at local level. This will lead to a new Memorandum of Understanding. At the time of this Opinion however, discussions between DG.HR.DS and the JRC were still ongoing. Therefore, this Opinion is based on the existing Commission Security Decision and Memorandum of Understanding.

Complementary information was requested from JRC Petten on 9 November 2012. On 18 December 2012, the EDPS received the answers from the JRC. Given the complexity of the case, on the basis of Article 27.4, the EDPS decided to extend the deadline for a period of two months the same day. On 19 February 2013 the EDPS sent the Draft Opinion to the DPO for comments. The feedback was received on 18 March 2013

2. Examination of the matter

Within JRC Petten, the security service is responsible, among others, for the security of persons, premises and information of JRC Petten. It implements the policies and procedures set up for the purpose of ensuring the overall security of the site.

This prior check analyses whether the data processing operations carried out by the security service of JRC Petten in the context of security investigations are in conformity with Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001"). The processing operations covering the procedure on a basis of a security report, which is drafted following an incident is not covered by the current notification because such aspect of the procedure is not of the competence of the JRC on the basis of the memorandum, which only covers processing operations that lead to the drafting of the said report.

2.1 The Facts

The ***purpose of the processing*** on security investigations is to obtain information associated to security related incidents such as traffic accidents, parking violations and vandalism that has occurred in JRC Petten premises with the final purpose of drafting a report describing the occurrence. These investigations may be carried out in case of need by the security service.

Based on the existing memorandum in force, the tasks [...] that shall be undertaken by the respective JRC security services (except Brussels) relate to: a) physical protection, b) personnel security and document and information security, c) IT security and security of CIS (communication and information system), d) Staff matters and visitors, e) Liaison with the Commission's Security Directorate (HR.DS) and the local security and police forces in the host countries concerned and f) inquiries[1].

A security investigation usually concerns the following processing operations:

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

In constituting the paper dossier, the security service shall undertake the following tasks:

- Document and describe occurrences and facts of security incidents including information regarding involved intervening parties.

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

[1] The Memorandum foresees that the Security Services shall in close cooperation with the Commission's Security Directorate (HR.DS):

a) Collect and evaluate information to identify specific threats against JRC sites;

b) Perform inquiries regarding minor security related incidents which involve other individuals or assets in these sites and which have limited impact, thefts, vandalism, road accidents, etc.

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

2) Consultation of local databases like visitor registration (DPO-1524) and staff photos (DPO-1704), video-surveillance footages (DPO-1521) and when necessary any other information deemed useful for the investigation and usually requested to services like the Human Resources, Social Service, Medical Services, Informatics Unit, etc.

3) 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.

4) Production of an Investigation Report that will be stored with the Local Security Officer (LSO).

The data controller explained that this procedure is in line with the agreed tasks in the Memorandum of Understanding.

The ***primary responsibility for the data processing*** lies with the Unit of JRC Petten responsible, among others, for security operations of JRC Petten. The data processing operations carried out while running security investigations are performed by the security service.

In the context of running security investigations, the ***automated and manual data processing operations*** are interrelated. A security investigation concerns the constitution of paper dossiers or reports where complaints, testimonies or declarations of any intervening parties are collected along with any elements, like photographs etc. At the end, the report will contain the main conclusions of the investigation.

Based on the notification:
- 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. According to the available information, by knowing the existence of the DPO notification a person should be aware that data can be collected.

- 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 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 a contact through other Commission services e.g. HR.DS. For this reason, follow-up with national judicial authorities or law enforcement agencies may be made until the necessary information is collected for performing the investigation.

The data processing involves the following ***types of data subjects***: "All staff in active employment, retired officials, external staff working under contract, visitors or any other person that addresses itself to the JRC 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 (care)[2].

Regarding the **categories of personal data** being processed, it is explained in the notification that as all details are included in a written detailed security investigation report it is difficult to determine exactly which data may be considered.

However, categories of data usually concern the people and the incident:
- 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 (photographs, video surveillance footage, etc.).

Conservation periods will vary depending on the outcome of the investigation. Two periods of conservation are foreseen in the notification:

- Data of security investigations resulting in an effective applicable measure (e.g. interdiction in accessing the site or a particular area linked to the task of granting permits to access JRC site and protected areas) needs to be kept until that applicable measure has to be enforced or tracked. Maximum retention period to be considered is of five years.

- The security investigation reports and related information resulting in a dossier that may need to be handled under criminal law would be kept for a maximum of ten years, starting from the conclusion date of the investigation. It is stated that this time period usually corresponds to their legal prescription.

The EDPS asked to clarify what would happen in terms of conservation in the case of investigations that may not result in final reports. The JRC replied that it has yet to perform such investigation. It was stated that if such situation would arise, if e.g. an item of a small value is reported stolen, then only comparable resources and efforts would be allocated to an investigation.

In some cases, some ***transfers*** may take place. Data can be handed over to national law enforcement agencies upon written request and duly authorised by the controller in case of investigations regarding threats to the security of the JRC sites or the European Commission and with implications at national level.

As far as the ***rights of access and rectification*** are concerned, a privacy statement was annexed to the notification and stresses that individuals can address queries concerning this processing operation. It states that such queries can be addressed to the controller through the security service and it provides contact details about this. The notification underlines that people concerned with an investigation are always invited to contact the 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.

As to the right of rectification, the notification also contains a reference that justified legitimate requests addressed to security service will be considered with immediate effect.

[2] to be preferred instead of the word "solicitude".

Regarding the ***right to information***, the privacy statement foresees this information. Where possible, such a privacy statement is handed over directly to data subjects. Based on the information provided, it was stated that it will be published on the JRC-Petten intranet and in case of an investigation the security service will inform witnesses and parties subject to an investigation.

It is also underlined in the notification that data subjects may always contact security service through the use of a functional e-mail.

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. As explained above, 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 ***security measures*** [...]

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 Petten's security investigations. 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.

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 carrying out investigations of incidents such as traffic accidents, parking violations and vandalism, the security service will process information which may relate to alleged offences. This is further confirmed if one takes into account that the final purpose of the processing is the drafting of a report describing the occurrence and eventual transfer to enforcement and judicial authorities.

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 involvement in given occurrences, thus triggering the application of Article 27.2(b).

Ex post 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, however, the processing operations have already started and may still evolve in the future with the clarifications of the security rules between DG.HR.DS and the JRC. Any recommendations made by the EDPS at this stage still need to be adopted accordingly. Any significant change in the procedure having an impact on the processing of personal data as described in the present notification or on the present Opinion should be timely notified to the EDPS.

Notification and due date for the EDPS Opinion. The notification of the DPO was received on 10 September 2012. The two-month period within which the EDPS must deliver an Opinion was suspended during 39 days + two months extension to obtain additional information and + 27 days to enable the DPO and data controller to provide comments on the EDPS Draft Opinion. The Opinion will therefore be adopted no later than 19 March 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 Article 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* (...)".

In order to determine whether the processing operations comply with Article 5(a) of Regulation (EC) No 45/2001, three elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out by security service of the JRC Petten; second, whether the processing operations are performed in the public interest; and third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

Relevant legal grounds in the Treaty or in other legal instruments. The EDPS takes note of a range of legal instruments, described below, which from a general to a more specific way provide the legal grounds that legitimise processing operations that take place in the context of conducting investigations.

The main legal basis for the processing operations stems from the Memorandum of Understanding of 25 November 2010 between the DG.HR.DS and the JRC regarding the tasks performed in the field of security, which determines the tasks and competences of the respective competent services on security issues. This Memorandum is based on legal documents which define the powers of the security services of the European Commission. The Memorandum focuses on the tasks allocated to the security services of the JRC. It states that the tasks regarding the security at all JRC sites except Brussels shall be undertaken by the JRC security services for the sites in question under the coordination of the JRC Security and Safety coordinator, also on behalf of other Commission services on those sites. Moreover, it is stated that in carrying out these tasks, the services concerned shall act fully in accordance with the Commission's internal security rules. The Memorandum also contains a table on the delineation of responsibilities between JRC and HR.DS for enquiries that underlines that JRC is competent to perform investigations only as regards traffic accidents, parking violations and vandalism. For all other types of incidents, either JRC performs the investigation and

reports to HR.DS or it informs HR.DS of the incident and agrees with HR.DS how to proceed or JRC informs HR.DS which performs the investigation. The EDPS also acknowledges that a new Decision from the European Commission will more clearly establish the respective competences of the DG.HR.DS and the JRC Security services. A new Memorandum will also complement the Decision and will replace the existing one.

Taking into account this forthcoming Decision and the new Memorandum, the EDPS considers that the legal ground foresees the tasks of the security services of the JRC sites, based on the existing rules applicable in the European Commission. From this perspective, the EDPS is satisfied that this instrument constitutes a valid legal ground to legitimise the data processing operations carried out for the purposes of finding out information related to incidents occurred in JRC Petten premises.

Processing operations are carried out in the public interest. The EDPS notes that the security service of JRC Petten carries out the processing activities in the legitimate exercise of its official authority. This service has the competence and the obligation to engage in investigations for the overall purpose of protecting persons, property and information under the responsibility of JRC Petten. Taking into account the nature of such activities it is clear that they are performed in the public interest insofar as the public interest is served if measures are taken to investigate the authorship of such events and prevent further occurrences in the future.

Necessity test. In order to engage in investigations to find out information about related incidents occurred in JRC Petten premises it appears necessary to process personal data. Unless such data are processed it would not be possible for JRC Petten to carry out its duties. Thus, from a general perspective, the processing appears necessary for the purposes of performing investigations. This being said, it should be taken into account that the "necessity" of the data processing also has to be analysed *in concreto*, for each particular case, here, for each specific investigation. From this perspective, it has to be kept in mind that the processing of personal data to be conducted in the context of the processing of the information of *ad hoc* incidents has to be proportional to the general purpose of processing (to ensure the security of the persons, buildings) and to the particular purpose of processing in the context of the case under analysis. Thus, the proportionality has to be evaluated on a case-by-case basis.

2.2.3. Processing of Special Categories of Data

Taking into account that the purpose of the processing is to facilitate the collection of information about incidents that constitute alleged wrongdoings, it is expected that in a number of cases this information will be related to offences, criminal convictions or security measures. 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, processing of the mentioned data is authorised by the legal instruments mentioned in point 2.2.2 above.

As far as special categories of data are concerned, Article 10.1 of Regulation 45/2001 establishes that "*the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited*".

From the list of data described in the notification for prior checking it does not appear that data falling under the categories of data referred to in Article 10.1 Regulation 45/2001 are processed in the context of the investigations. Taking into account the overall purpose pursued by JRC Petten when it engages in data processing operations, the EDPS understands that the collection of special categories of data is not JRC Petten's main goal.

However, the EDPS considers that in the context of the investigation, JRC Petten may become, perhaps involuntarily, in possession of special categories of data, which will often be of no interest/relevance to the investigation. In this regard, the EDPS recalls the application of the data quality principle, according to which data must be adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed (Article 4.1.c). Pursuant to this principle, if special categories of data that clearly are not relevant for the purposes of investigating the incident are collected, they should not be reflected in the written report. The data controller confirmed that the security officers in charge of performing and drafting reports are already aware that only relevant categories of data should be assembled and that the controller (which is also the hierarchical superior of the security service) is responsible for ensuring this.

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"*. This is referred to as the data quality principle.

Even though certain standard data will always be present in the investigation of incidents such as the name, date of birth, etc, the precise content of a file will of course be variable according to the case, as it was also underlined by the data controller in the notification. Guarantees must however be established in order to ensure the respect for the principle of data quality. This could take the form of a general recommendation to the persons handling these files, reminding them of the principle and asking them to ensure that it is respected.

The EDPS also recommends that whenever access to personal data appears to be necessary for the purposes of the investigation, such access should respect appropriate guarantees, taking into account any potential risk of inadmissibility of the evidence in a possible future criminal case, which could arise if the fundamental rights to privacy and personal data protection were not respected when the evidence was collected. Particular attention must be paid to respecting these principles when access to files which are manifestly of a private nature seems necessary for the purposes of the investigation.

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"*.

This principle is very much connected to the exercise of the rights of access, rectification, blocking and erasure (see point 2.2.7 below). Furthermore, an investigation system that guarantees the inclusion of evidence of charge and discharge is of relevance as concerns the accuracy and the completeness of the data being processed. As a consequence, and considering its importance from a data quality perspective, the EDPS recommends that security officers are made aware of this principle.

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 conservation period varies depending on the categories of data. The EDPS takes note that a five years period is deemed necessary by the JRC regarding cases that result in the application of concrete measures (i.e. interdiction in accessing a site or a particular area). The EDPS also takes notes of the ten year period that applies to information that relates to cases that result in a dossier that is handled under criminal law as this deadline takes into account the period of time necessary under national legislation for this category of infractions to be expunged.

2.2.6. Transfer of Data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made *ex* Article 7 to EU institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46. Transfers of data under Article 9 of the Regulation are not foreseen.

Transfer of personal data within or between EU institutions or bodies

Data may be transferred to European Union institutions and bodies such as OLAF, IDOC or to the Security Directorate of the European Commission.

Article 7.1 of the Regulation stipulates: *"Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

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. The proportionality factor has to be considered in this regard, taking into account, for instance, the nature of the data collected and further processed, and the competence of the recipient. 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 investigations and the cases under which such transfers will be compulsory.

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.

Transfer of personal data to Member States. Pursuant to the Notification, data may be handed over to national law enforcement agencies upon written request and duly authorised by the controller in case of investigations regarding threats to the security of the JRC sites or the European Commission and with implications at national level in accordance with Article 8 of Regulation (EC) 45/2001.

The EDPS considers that in such transfers based on Article 8 of the Regulation, two scenarios can be observed in Member States: (a) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC covers every sector of the national legal system, including the judicial sector; and (b) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC does not

cover every sector, and particularly, not the judicial sector. As to the first scenario, Article 8 of the Regulation foresees: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, (...)."* Thus, even if judicial authorities do not fall within the scope of application of Directive 95/46/EC, if the Member State, when transposing Directive 95/46/EC into internal law, has extended its application to these public authorities, Article 8 of the Regulation has to be taken into account. For those countries that have not extended their implementation of Directive 95/46/EC to judicial authorities, consideration to Article 9 of the Regulation has to be given. In those cases, Council of Europe Convention 108 and its Additional Protocol, which for the matter under analysis can be considered as providing an adequate level of protection, is in any case applicable to judicial authorities.

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 information can then be obtained directly by the data subject (this is the so-called "direct access") or, under certain circumstances, by a public authority (this is the so-called "indirect access", normally exercised by a Data Protection Authority, the EDPS in the present context).

The privacy statement declares that individuals direct queries concerning this processing operation to the data controller. It gives a functional e-mail box as the contact person to exercise this right. However, contrary to the notification, it does not specifically state that data subjects have a right of rectification. The EDPS suggests clarifying this in line with the wording of the notification.

The data controller also clarified that for investigations covered JRC-Petten (see MOU), the JRC does not consider Article 20 of Regulation 45/2001. Application of this article is applicable for investigations conducted by DG.HR.DS.

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.

In assessing whether the data controller for the case in point provides information to individuals, one must address two issues: first, the extent to which the information is effectively provided in a way that enables individuals to read the information and, second, the extent to which the information provided, i.e. its content, is in line with Regulation (EC) No 45/2001.

- *The communication channel:* According to the notification, the information channel through which individuals are informed is a privacy statement that is normally handed over to the data subject(s). It is also available upon request and on the intranet of the security service of the JRC Petten site. In addition, according to the data controller, 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.

The EDPS considers that the publication of the proposed general Privacy Statement on the Intranet of the security service of the JRC Petten site is a positive practice towards informing individuals. But this can not considered sufficient, for instance, for individuals who may not have access to the intranet. Assuming that a person should be "aware" that data could be collected by knowing the existence of the DPO notification would not ensure correct information of every data subjects. Therefore the EDPS recommends publishing the Privacy Statement on the Internet of the JRC (as general information).

Furthermore, the EDPS considers that any witness or person concerned that would be involved with the security service should be individually informed of the processing of his/her personal data through specific information notice in all cases of verbal or written declarations and be able to document it. Like this, JRC Petten shall ensure the full information of the data subjects pursuant to Articles 11 and 12 of the Regulation.

- *The content of the privacy statement.* The EDPS has also checked the content of the information provided in the privacy statement and considers that for the most part 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 data 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.

It also contains the right to have recourse at the European Data Protection Supervisor. The EDPS however would recommend including a specific paragraph on the rights of access and rectification and not only the right of "queries", as stated on point 2.2.7 above.

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. JRC confirms that it has adopted the security measures required under Article 22 of the Regulation.

[...]

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 Petten must implement the following:

- When data are transferred within EU institutions and bodies and also to national (police and judicial) authorities a notice should be given to the recipients of the data informing them that the data can only be processed for the purpose for which they were transmitted. Furthermore, it should be ensured that this only happens when the transfer is necessary. This necessity should be duly assessed and documented before the transfer takes place;
- The privacy statement should be amended in the light of the comments above for both the communication channel and its content.

Done at Brussels, 19 March 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor