Opinion on a notification for Prior Checking received from the Data Protection Officer of the Commission on Entrance Permission and Access Control for Physical Protection in JRC-ITU

Brussels, 24 July 2012 (Case 2008-0726)

I. Proceedings

On 28 November 2008, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of the Commission ("DPO") a notification for prior checking ("the Notification") regarding the data processing operations relating to the operation of an Entrance Permission and Access Control for Physical Protection in the Joint Research Center - Institute for Transuranium Elements, in Karlsruhe ("JRC-ITU").

On 26 January 2009, the EDPS made a request for additional information, which the Commission's DPO answered on 20 February 2009. The additional information added complexity to the matter, requiring further analysis of the case. For this reason, on 23 February 2008 the EDPS decided to extend the period of further analysis for additional 3 weeks. On 4 March 2009 a second information request together with the draft facts was sent to the Commission's DPO. On 09 April 2009 the EDPS asked feed-back on two additional questions.
The EDPS received the answers on 4 May 2009.

On 11 May 2009, the EDPS sent the draft Opinion to the Commission's DPO for comments. Reminders were sent to the Commission DPO on 5 December 2011 and 26 June 2012. The comments on the draft Opinion were not transmitted to the EDPS.

II. The facts

The Entrance Permission and Access Control for Physical Protection System ("EPACPP System") is part of the JRC-ITU security infrastructure in order to control and manage access rights to JRC ITU premises. In addition, the EPACPP also assists the radioprotection Service within the JRC ITU to control the radioprotection status of visitors. This prior checking will analyse the processing of the data for the first purpose. However, it will not address the data protection issues related to this secondary purpose insofar as the EDPS already prior checked the processing operations carried out to handle personal radiation exposure coming from dosimetry measurements[1].

In this context it is important to take into account the important public interest in the security and safety of the underlying activities which motivate the data processing. At the same time, it is important that such security and safety activities are carried out without jeopardising the data protection and privacy rights.

[1] Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission on "AGS-EDV Database at JRC-ITU in Karlsruhe", Brussels, 10 January 2008 (Case 2007-378).

The ***purpose*** of the EPACPP System is twofold: *(i)* To control and manage access rights to JRC-ITU. This applies to the entire JRC-ITU site insofar as the whole JRC-ITU is deemed a nuclear facility. *(ii)* To control radioprotection status.

The ***primary responsibility*** for the data processing lies within JRC-ITU, in particular within the Unit competent for nuclear safety (Unit E07) which represents the data controller ("JRC-ITU") for the processing at stake. Two data processors are used, one to perform physical protection duties (referred to as "Physical Protection Group") and another one to maintain and develop the software and hardware used for the processing of data.

As for the ***description of how the processing takes place***, the following is relevant.

Regarding the processing of data of visitors and short term contractors:

(i) *Enrolment phase*: During this phase visitors and short term contractors fill in a form ("Application Form") with their identity information, place of birth, nationality, passport number, private address, and their employer. In addition, the host person completes the Application Form with information regarding the length of the stay, whether access to controlled areas is necessary and the reason for the stay and the person/s to be visited. This information is transferred to DG ADMIN DS for the purpose of issuing a security clearance (see below).

(ii) *Issuing of a badge:* Upon analysis of the Application Form and having received the security clearance, a badge with the authorised access rights will be issued by staff working for the Physical Protection Group. The badge will contain the first and last name, badge number, and a photo in order to identify at any time the person and his/her access rights for the different security areas.

(iii) *Use of the badge:* Every time that the badge holder wishes to access a security areas, a verification of the identity of the individual and his/her access rights will be carried out by the Physical Protection Group, i.e., guards performing physical protection duties.

(iv) *Storage of data:* All the data will be introduced in the central database ZES of the Physical Protection Group.

As for the processing of data of ITU Commission Staff and long terms contractors (altogether ITU Staff) who need an every day access to nuclear areas or other security areas):

ITU Staff undergoes the processing described above when they start working for the ITU. In addition, the additional processing also takes place, which involves [biometric] scanning:

(i) *Enrolment phase:* During this phase [a camera] takes black and white pictures of the [biometrics] of ITU Staff (referred to as "[...]-codes"). This is done by operators who have had specific training in biometrical enrolment procedures. It is conducted by the Physical Protection Group in the Application Office in the ITU Premises, one of the security areas with limited access. In case of "false rejection", it is foreseen that a manual check carried out after identification of the guards will take place.

All the ITU Staff (i.e., Commission Staff and long terms contractors) are enrolled insofar as the entire JRC-ITU site is a nuclear facility. The approximate number of ITU Staff members concerned is 400.

(ii) *Storage of [biometrics]:* The pictures of [biometrics] are stored in an [...]-Code Database. The identification data, as described above, is stored in a central database ZES. This is to ensure that the "[...]-code" is only usable if one has access to both databases at the same time. Access to both databases is limited to the Physical Protection Group.

(iii) *Scanning of [biometrics]:* [...]In the case in point, the JRC-ITU EPACPP uses a "comparison one to many" search mode. In addition to checking the [biometrics], individuals are weighted in order to measure that only one authorised person at a time will pass the sluice. In case of false rejection, it is foreseen that a manual check and identification will be carried out by the guards.

The central database server is the administrative interface with the system. It stores information about the users and their access rights. It also stores any access attempts, granted or denied.

The ***data subjects*** include members of ITU Staff and long time contractors. In addition, data of visitors and short term contractors will also be processed in the context of the issuance of temporary passes.

The following ***categories of personal data*** are concerned: (i) Identification data (name; staff number; picture, date and place of birth, nationality, private address); (ii) Work related information (company name, starting and end of work at JRC-ITU); (iii) Security clearance information; (iv) Access rights and login data (date; time; access granted or denied and, (iv) radiation protection information (training, occupationally exposed).

Some information is ***transferred*** to DG ADMIN DS. Every visitor from outside the EU who wants to have access to the ITU premises has to be cleared by DG ADMIN DS. Towards this end, information such as date and place of birth, nationality, personal identification number and private address, company and purpose of the visit are passed on to DG ADMIN DS. In case of a security incident, information might be shared with the National German competent authorities.

Regarding the use of a ***data processor***, in this case, the Physical Protection Group and a private company in charge of maintaining and developing the software and hardware used for the processing of data. The EDPS understands that data processor agreements are in place, which ensures that the processors take the appropriate security measures to safeguard the information.

Regarding the ***information given to data subjects***, according to the Notification, a privacy statement will be available on the JRC-ITU intranet and at the guard station at the entry of the ITU premises. The privacy statement contains the following elements: (i) Explanation of the ITU Entrance Permission and Access Control System; (ii) The personal information collected, for what purpose and through which technical means; (iii) The protection and safeguards of the information; (iv) The retention period; (v) The right of data subjects (access, modification, deletion) and the right to have recourse to the EDPS. The DPO included the privacy statement with the notification. The rights of the data subject are explained in the privacy statement and contact information is provided in order for data subjects to exercise these rights.

Regarding the ***conservation of the data***, according to the Notification and to the privacy statement, data of visitors with no access to a nuclear area per se are retained for 5 years after the last visit. For JRC-ITU staff, data will be deleted 5 years after expiration data of the

security clearance. The reason for keeping this information for this period is the following. Most of the visitors are specialised technicians or high level scientists who visit the JRC- ITU on a regular basis, normally for several years. Therefore JRC- ITU has decided to keep the data for 5 years in order to be able to request the renewal of security clearances without the need to collect the data from the individual each time he/she visits JRC-ITU.

For visitors and ITU Staff who have access to nuclear areas per se and are registered with dosimeter data the data will be stored for 95 years after the data of birth of the data subject. This applies to all the data except [...]-codes. They are kept in order to back trace any incident or question related to the dosimetry values and to be able to identify and contact the concerned person.

Security measures are implemented. The information is stored on secured IT systems which are hosted and managed by the Physical Protection Group. Access to the database system requires the submission of a user identification and password. The data is backed-up automatically on a tape drive. All paper based information is stored in secure areas.

III. Legal aspects

III.1. Prior checking

This prior check Opinion relates to processing of personal information carried out by JRC-ITU, to control the identity and permit or deny access of persons entering and exiting the JRC-ITU.

Regulation (EC) No 45/2001[2], applies to the "*processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system"* and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*"[3]. For the reasons described below, all elements that trigger the application of the Regulation are present.

First, personal data as defined under Article 2(a) of Regulation (EC) No 45/2001 are collected and further processed. Second, the personal data collected undergo "*automatic processing*" operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001, as well as manual data processing operations. Indeed, the personal data such as [biometric] data are collected and undergo automatic processing, for example when [biometric] templates are taken. Finally, the processing is carried out by a EU body, in this case by JRC-ITU, in Karlsruhe in the framework of the EU law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in this data processing.

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*". The EDPS considers that the presence of some biometric data such as the case in point where biometric [...] are collected, presents specific risks to the rights and freedoms of data subjects. These views are mainly based on the nature of biometric data which are highly sensitive, due to some inherent characteristics of this type of data. For example, biometric data changes irrevocably the

[2] Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community (now, EU) institutions and bodies and on the free movement of such data ("Regulation (EC) No 45/2001").
[3] See Article 3 of Regulation (EC) No 45/2001.

relation between body and identity, in that they make the characteristics of the human body machine-readable and subject to further use. In addition, regarding such data, the EDPS also notes that possibilities of inter-linkage and the state of play of technical tools may produce unexpected and/or undesirable results for individuals. These risks justify the need for the data processing to be prior checked by the EDPS in order to verify that appropriate data protection and privacy safeguards have been implemented.

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 been established. This is not an insurmountable problem provided that all recommendations made by the EDPS are fully taken into account and the processing operations are adjusted accordingly.

Notification and Due Date for the EDPS Opinion. The Notification was received on 28 November 2008. The period within which the EDPS must deliver an opinion was extended for three weeks. The period within which the EDPS must deliver an opinion was suspended for a total of 1256 days to request further information from JRC-ITU and allow for comments on the draft EDPS Opinion.

III.2. Lawfulness of the processing

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

Of the various grounds listed under Article 5 of Regulation (EC) No 45/2001, the processing operation notified for prior checking 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 or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*".

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 ("legal basis"). The EDPS understands that the ***legal basis*** for the processing is to be found in:

- Commission Decision 2001/844/EC, ECSC, Euratom (security provisions);
- Commission Decision 2006/3602/EC concerning security of information systems;
- Commission's IT security policy (PolSec);
- -German legislation including (i) Atomgesetz (AtG) §9+§12b+§12c as of 15.07.1985. (ii) Atomrechtliche Zuverlässigkeitsüberprüfungsverordnung (AtZüV) as of 01.07.1999http://www.gesetze-im-internet.de/atz_v/index.html (iii) Strahlenschutzverordnung (StrlSchV) §42 as of 20.07.2001

Second, regarding whether the processing operations are performed in the public interest, the EDPS notes that the mission of JRC-ITU is to provide the scientific foundation for the protection of the European citizen against risks associated to the handling and storage of highly radioactive material. The Commission carries out the processing activities in the

legitimate exercise of its official authority and in the light of the public interest for this research to be carried out properly and safely.

Finally, there is the question of whether the processing operations are indeed necessary for the performance of that task ("necessity test"). According to Article 5 a) of Regulation (EC) No 45/2001, the data processing must be "necessary for performance of a task" as referred to above. In this respect, recital 27 of the Regulation states that: "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*". Taking into account the highly sensitive nature of the objective and information processed within JRC-ITU, and in order to prevent the unauthorized access and disclosure of this sensitive information, it appears necessary for JRC-ITU to implement highly secure measures to control access to JRC-ITU premises. These measures include the setting up of stringent access control systems which entail the use of biometric. Therefore, in the EDPS' view, the implementation of access control systems which entail the processing of personal data, including biometric data, can in this case reasonably be considered as a necessary internal control measure towards the safeguard of highly sensitive information and other interests of the Union.

III.3. Processing of special categories of data

The notified data processing does not relate to data falling under the categories of data referred to in Article 10.1 of Regulation (EC) No 45/2001.

III.4 Data Quality

Adequacy, relevance and proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed. This is referred to as the data quality principle. In analysing whether the processing at issue here, which involves mainly the processing of biometric data, is in line with this principle, the EDPS notes the following.

(i) Responsibility for overall assessment of the impact of the data collection: The EDPS understands that JRC-ITU has reached the conclusion that the data processing, including the collection of [biometric] data in respect of other personal data is necessary in order to protect JRC-ITU buildings. However, JRC-ITU has not succeeded in demonstrating that it has engaged in any in-depth assessment of the impact of the use of the data and evaluating the reasons that justified the use of such technique and whether other, less privacy intrusive alternatives, were envisaged. Vis-à-vis the future and particularly concerning possible updates of the system, JRC-ITU should carry out a proper impact assessment which besides technical and security aspects, should also take into account privacy/data protection considerations.

(ii) Assessment of whether the data subjects from whom data are processed is adequate: As stated in the Notification, each JRC-ITU Staff member is considered a data subject. Further, the Notification describes that the system is designed to control the identity and permit or deny access at all entrances into and exits from the JRC-ITU. As a consequence, each member of JRC-ITU staff must undergo the enrolment procedures. If the entire JRC-ITU site (buildings) is deemed a nuclear facility, it appears appropriate for JRC-ITIU not to limit the number of individuals enrolled to a selected group with access to certain facilities. However, from the information provided to the EDPS it seems unclear whether staff members working in functions (for example of administrative nature) that are performed outside the nuclear and secure zones should be subject to the same security safeguards. In this regard, and vis-à-vis possible updates of the system, the EDPS recommends that JRC-ITU studies the possibility to

limit the enrolment of [...]-codes to those JRC-ITU staff members that work for nuclear and particularly secure zones.

(iii) Assessment of whether the type of data collected is adequate: The type of data collected, mainly the [biometric] templates and related identification information, corresponds to the data required to operate an access control system based on biometrics. From this point of view, the EDPS considers that the data collected are adequate and relevant for the purposes of the processing.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section III.2.). The issue of fairness is closely related to what information is provided to data subjects, which is further addressed in Section III.8

Accuracy. 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*".

In this case, the personal data at stake include mainly biometric data, used for access control purposes. Some key features of biometric systems have a direct impact on the level of accuracy of the data generated either in the enrolment or identification phases inherent to this type of system. Depending on whether the biometric system is set up in a way that integrates these key elements, the accuracy of the data will be (or not) at stake. Next we describe these key elements and analyse the extent to which they have been taken into account in the biometric system concerned.

Firstly, any enrolment phase must foresee alternative ways to identify individuals who are not eligible, even temporarily, for enrolment. This is usually referred to as "fall back procedures"[4]. In this case it is foreseen that a manual identification check will be carried out by the guards of belong to the Physical Protection Group which stand the entrance of security areas. Given that the fallback procedures in this kind of systems is very low (0% after 12 enrolment sessions), the procedures foreseen by JRC-ITU seems appropriate.

Second, similar types of measures must be foreseen for those individuals who are properly enrolled but who are wrongly identified (usually referred to as "false rejection"). If these measures are not embedded in the architecture of the system, the accuracy of the information produced by the system may be compromised. In particular, in the case of false rejection, the system will produce a record that a given individual without proper access rights intended to access a secured area, when in fact the individual did have such rights. At the same time, because the individual will be misidentified, he/she will be denied a right (the right to access specific areas) to which he/she is entitled.

In case of false rejection or other problems the concerned person has to report to the Physical Protection Group's Application Office. The EDPS considers that this solution should mitigate the burdens associated to false rejections.

Third, JRC-ITU EPACPP is based on [biometric] templates stored in central database and which are combined with the use of camera readers. The EDPS notes that this entails the use

[4] For a description of the data protection principles applicable in relation to fall back procedures, see Opinion of 13 October 2006 on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions, OJ C 313, 20.12.2006, p. 36.

of biometrics for identification and access control purposes using the "comparison one to many". This type of search mode does not always lead to correct results. In other words, it may misidentify individuals and thus create inaccurate records. An alternative search mode such as the "one to one" does not present the same problem because the biometric data are only compared to one template rather than being compared to a larger number of templates. The "one to one" search mode usually involves the storage of the template in a chip which is in the possession of the individual to be identified. However, the template can also be stored in a central database but in this case it must be accompanied by an additional identification tool which could work as follows. For example, an identification card provided with a chip could broadcast the identity of the individual to the identification unit, which would proceed to compare the template associated to the identity of the individual with the biometric data presented to it at this particular moment. Furthermore, as further described below, the "one to one" search mode entails less processing of data and hence contributes to the fulfilment of the proportionality principle.

In the case in point, the JRC-ITU EPACPP uses a "comparison one to many" search mode. [...]. In principle, the EDPS considers more appropriate to use the "one to one" search mode whereby the identification unit would compare the [biometric] of the individual with a unique template (associated to the identity). As pointed out above, such a search mode system provides more accurate results.

The EDPS understands that in this case, taking into account the limited number of templates (approximately 400) the possibility of errors is very narrow; however, as a matter of principle, he is of the view that it is more appropriate the use of "one to one". The "one to one" search mode not only provide more accurate information, it also entails less processing of data insofar as the system only has to match two sets of information pertaining to the same individual (as opposed to matching one set of information against the templates of many individuals). Hence, this search mode is inherently less privacy invasive. In selecting "one to one" search mode, systems that store the biometric templates in chips rather than in central databases are more privacy friendly. The storage in chips is obviously more privacy friendly insofar as the template is stored on a medium (e.g. badge with chip) which is in the possession of the respective data subject. Thus, the data subject him/herself has the direct control and responsibility of his/her template. No one else has access nor is in possession of his/her template. An additional problem with the storage in central databases is that it triggers the risk of so-called "fishing expeditions", accessing the database for purposes different from those for which the database has been conceived. A decentralized system solves this risk without eroding the security level.

In the light of the above, the EDPS requests the JRC-ITU to make an evaluation of its decision taken in terms of the technological choices discussed above and the choice of the best available techniques. This evaluation will be relevant in order for the EDPS to evaluate the EPACPP compliance with Article 4(1)(d) of the Regulation.

III.4. Conservation of data/ Data retention

Article 4(1)(e) of Regulation (EC) No 45/2001 sets forth the principle that "*personal data must be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the data were collected or for which they were further processed*". "*The Community institution or body shall lay down that personal data which are to be stored for longer periods for ... statistical use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subject encrypted".*

According to the Notification, data of visitors with no access to a nuclear area *per se* are retained for 5 years after the last visit. The reason for keeping this information for this period is the following. Most of the visitors are specialised technicians or high level scientists who visit the JRC- ITU on a regular basis, normally for several years. Therefore JRC- ITU has decided to keep the data for 5 years in order to be able to request the renewal of security clearances without the need to collect the data from the individual each time. The EDPS understands and agrees with the need to keep the data for such period of time regarding the type of data that is necessary for the re-issuance of a security clearance.

For visitors and ITU Staff who have access to nuclear areas per se and are registered with dosimeter data all the data will be stored for 95 years after the data of birth of the data subject. This applies to all the data except [...]-codes. They are kept in order to back trace any incident or question related to the dosimetry values and to be able to identify and contact the concerned person. This is a very long period of time. However, considering that the storage of accurate dosimetry data may have significant relevance later in the context of medical treatment of the person concerned and/or in view of possible occupational diseases' related claims, the EDPS considers that this period may be deemed to be within the reasonably margin.

The EDPS understands from the notification that no statistics on personal data are allowed after the retention period. Nevertheless, the EDPS would emphasise that where such data are used beyond the retention period, they must be made anonymous (Article 4(1)(e) of the Regulation).

III.5 Transfer of data

According to the Notification, in case of a security incident, the information is transferred to DG ADMIN DS. The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data be transferred if it is "*necessary for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, the data controller must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary.

The above transfers, according to the Notification, seem to fall within the legitimate performance of the tasks covered by the competence of the respective recipient. In fact, "ADMIN DS" have competence, among others, tasks related to the "protection of persons, protection of buildings and property and protection of information, data transmission and processing. In order to ensure full compliance with Article 7 of the Regulation, the EDPS recommends that all recipients are reminded of their obligation to process the data only for the purpose for which they were actually transmitted.

In case of a security incident, this information might be shared with the National German competent authorities, in which case Article 8 of Regulation (EC) No 45/2001 applies**.** Article 8 of Regulation (EC) No 45/2001 offers several legal grounds authorising the transfer of personal information. Given the circumstances in this case the data controller may avail itself of Article 8 (a) according to which personal data can be transferred if the data will be used to perform a task subject to public authority or if the data transfer is made in the data subject's legitimate interest. Whereas under Article 8 (a) of Regulation (EC) No 45/2001 it is up to the recipient to establish the interest, the EDPS understands this provision to mean that if the sending of the information is not carried out at the request of the recipient, is up to the sender to accredit such a need.

In accordance with the above, when the information is not sent at the request of the recipient, the data controller must accredit the necessity of the data transfer. In order to implement this rule, the EDPS recommends that the data controller lists in a reasoned opinion all the data transfers that will be carried out or have been carried out in the context of a case and describe their necessity. These procedures should be communicated to the relevant staff.

III.6. Processing data on behalf of the data controller

Pursuant to Article 23 of the Regulation, if there is a data processing on behalf of a data controller carried out by a data processor, a contract or legal act among the data processor and controller must concluded. The contract must stipulate that the processor will act on instructions from the data controller (regarding the processing of data). The processor must ensure compliance with the security obligations embodied, in this cased, in applicable national rules implementing Article 17 of Directive 95/46.

In this case, the data controller uses two data processors, one to perform physical protection duties (referred to as "Physical Protection Group") and another one to maintain and develop the software and hardware used for the processing of data. Given the very sensitive nature of the data, the EDPS wishes to stress the need for the data processor to ensure a very high level of security The EDPS understands that the data controller has agreements in place and is not aware of breaches of Article 23 of Regulation.

III.6. Right of access and rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source. Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

The Notification describes the possibility of access to and mention the possibility of rectification of personal data by a staff member. The privacy statement which was submitted to the EDPS for review provides an email for the execution of these rights. The EDPS recalls that these rights apply not only to the information provided by the individual (identification information and [biometric] templates) but also to the information generated every time an individual accesses JRC-ITU. In conclusion, from the information received, the EDPS has no reason to conclude that the conditions of Articles 13 and 14 of the Regulation are not met.

III.8 Information to the data subject

Articles 11 and 12 of Regulation (EC) 45/2001 list information that must be provided to the data subjects. These articles list a series of compulsory items and another set of information. In this case, all the data is collected directly from the data subject, thus, Article 11 (Information to be supplied where the data have been obtained from the data subject) should be observed.

According to the Notification, a privacy statement will be available on the ITU JRC intranet and at the guard station at the entry of the ITU premises. The privacy statement contains the following elements: (i) Explanation of the ITU Entrance Permission and Access Control System; (ii) The personal information collected, for what purpose and through which technical means; (iii) The protection and safeguards of the information; (iv) The retention

period; (v) The right of data subjects (access, modification, deletion) and the right to have recourse to the EDPS. The DPO included the privacy statement with the notification. A copy of the privacy statement was provided to the EDPS.

The privacy statement contains information on the purposes of the processing and how the data are processed, the conditions for the exercise of the right of access and rectification, the time limits for storing the data and the possibility to have recourse to the EDPS. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation. However, he considers that some amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

- Regarding the collection of biometric data, staff should be given additional information, including the overall functioning of the system and the practical consequences to enrol and of failure to do so.
- More information should be provided regarding the purposes of the processing, for example, the privacy policy does not refer to the need to use the information for a security clearance with DG ADMIN DS.

Regarding how this information is provided, the EDPS considers that the privacy statement should be provided to individuals who undergo an enrolment phase. It does not seem sufficient for this statement to be available on the Intranet or in the entrance to the security areas. In another prior-checking analysis[5], the EDPS acknowledged the procedure implemented at the European Central Bank (i.e. "the privacy statement will be provided in paper and individuals will be asked to sign it stating that they have read and understood the statement"). The EDPS considers that this is an appropriate method of providing the information and suggests that a copy of the privacy statement be given to individuals so that they can go back to the privacy statement in case, for example, they want to know how to exercise their rights or how the data processing takes place.

III.9 Security measures

According to Article 22 of the Regulation concerning the security of processing, "*the controller shall implement 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*". After review of the security measures described in the information provided to the EDPS, there is no reason to believe that the measures implemented in the context of the notified procedure do not comply with Article 22 of the Regulation.

IV. Conclusion:

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

- Make an evaluation of the decision to set up the Access Control for Physical Protection System as it has been described to the EDPS, in particular, assessing the

[5] See Opinion on the European Central Band access control (2007-501).

decisions taken in terms of the technological choices (use of [biometrics], use of "one to many", number of data subjects affected) and the choice of the best available techniques. In the above context, reconsider whether it is appropriate to apply the measures to all the JRC-ITU Staff members;

- In the context of the above evaluation, evaluate possible implementation, vis-a-vis the future changes to the system in terms of technological choices.
- Submit the above evaluation (report) to the EDPS within 8-10 months;
- Inform recipients of data that the personal data can only be processed for the purposes for which they were transmitted and list lists in a reasoned opinion all the data transfers carried out to authorities and describe their necessity. These procedures should be communicated to the relevant staff;
- Amend the privacy statement as recommended in this Opinion and ensure that a copy of the privacy statement is given to individuals or that it is made available to them in a way that allows them to consult it.

Done in Brussels, 24 July 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor