Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the database ARDOS

Brussels, 15 December 2008 (Case 2007-380)

1. Proceedings

On 6 June 2007, the EDPS received a notification for prior checking under Article 27 (3) of Regulation (EC) No 45/2001 ("the Regulation") from the Data Protection Officer (DPO) of the European Commission. The data processing operations relate to the database ARDOS, the security service information system of the Joint Research Centre (JRC) at Ispra. Annexed to the notification were various annexes on the processing.

The EDPS requested complementary information on 27 June 2007. Due to technical problems, the information was provided only on 17 March 2008. Additional information was requested from the controller on 1 and 2 April, and received on the same day. On 14 April, the EDPS sent the draft Opinion to the controller for comments, which were received on 22 April 2008. Due to the complexity of the matter, the EDPS extended the period for a further month. A further set of questions was sent to the controller on 21 May 2008. Information was received on 19 June 2008, but so far a clear legal base has not been provided. In the absence of an answer on such a legal basis, the EDPS issues his Opinion today.

2. The facts

This prior check concerns a database called ARDOS. ARDOS is the Security Service Information system as well as the archiving database for all documents requested by and presented to the Security Service of JRC Ispra.

The ARDOS database has several **purposes**.

(i) It supports the issuance of the so called "Nulla Osta" assessment for any recruited member of staff for all JRC sites except Karlsruhe. Nulla Osta ascertains and confirms a selected candidate's good conduct. ARDOS manages the processing of Nulla Osta requests, along with any other security related information collected during the existence of a contractual link with the data subject, including any original police record.

The reports on security investigations are also stored in ARDOS.

(ii) The photographs collected are used for printing personalised staff passes (badges) and shared with the Commission Directory or Service Guide. Photographs of all JRC staff are stored. Staff passes are also issued for JRC Sevilla.

(iii) The information regarding the presence of people on-site is also used to be able to apply the 72 months On-site presence rule, also known as "règle anti-cumul de 6 ans". This means that the maximum duration of a non civil servant (including trainees, grant holders, fellows, visiting scientists, seconded national experts, contract and temporary agents) on JRC site is 72 months. This maximum duration period is counted over a twelve year period. Periods served in other services of the Commission are also taken into account.

The issuance of Nulla Osta implies the evaluation of the conduct of the data subject. The presentation of a clean original and authentic criminal record is the most important and relevant element. In case specific entries in the criminal record are found - which is quite rare - they are evaluated and if deemed necessary the person concerned may be interviewed by more than one Security Service Officer to personally evaluate if the person would pose a security risk. Care is taken also in establishing any missing information on application forms and curriculum vitae as well as stays in potentially dangerous countries.

Nulla Osta is described as a security clearance in the privacy statement of the Security Service Archive (ARDOS). The recruitment services of all JRC sites collect the criminal record/certificat of good conduct necessary to issue the security clearance[1].

Manual and **automated** data processing are interrelated. The documents of the data subject are registered in a scanned and/or paper version. It should be noted that the JRC currently no longer keeps documents in paper form and is in the process of transforming past paper documents into a digital format. Data can also be imported from Sysper2 to update active staff table and internal service as well as office location details. Manual processing operations are used for the maintenance of the updated list of all "active" people working on-site, for the issuance of Nulla Osta and "On-Site Presence" as well as for the archiving of all historical information. The reference system for all Security Service Long Term Authorisations (i.e. Staff Passes) or Special Authorisations is also a manual processing operation.

The **persons concerned** by the processing operation are the pre-selected candidates for a post at the Joint Research Centre, all categories of JRC staff members and other staffs (external contractor) that need to regularly enter the Ispra site (those who have been issued a "staff pass"). It has to be noted that the processing does not concern the daily visitors that enter the site on an occasional basis[2].

The **data** processed are the following:

The 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 and long term permit start and ending dates, request for Security Clearance form, Candidate's CV, Identity Document, Photograph, Certificate of

[1] This specific wording is used in the five notifications on recruitment of JRC staff that have been prior checked by the EDPS: 2008-140, 2008-141, 2008-142, 2008-143, 2008-136.

[2] About the "daily visitors pass" see the letter dated 29 November 2007 concerning the SECPAC database available on EDPS website:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Letters/2007/07-11-28_Commission_JRC_SECPAC_EN.pdf

Good Conduct and relevant Vacancy Notice, data related to *Foresteria*[3] facilities, varied documentation and vetting documentation. By vetting documentation, the Security Service means the security investigations files that are stored in the ARDOS database.

The Security Service has put in place a procedure where data subjects may request and verify what data are registered and associated with them. The JRC SECPAC SUPPORT service (jrc-secpac-support@ec.europa.eu) is the main point of contact and is responsible for providing **access** to or correction of personal data. For example, a special procedure for returning the original 'Police Record' has been put in place. At any given moment in time, data subjects may request and perform an update of their photograph possibly including a photograph taken by an external photographic service. Personal address and personal contact in case of emergency is usually updated upon issue, renewal or replacement of a staff pass, but may be updated at any time.

Upon a justified request from the data subject after the conclusion of a contractual link, his data can be modified, frozen or eventually erased in a maximum period of 14 days.

As far as **conservation of data** is concerned, ARDOS currently holds historical information and all data collected which have been kept over time. The Security Service foresees to adopt the following conservation periods:
- Data collected for candidates that give up their job application or are not recruited but have had a Security Nulla Osta processed for them will be kept for a period of 1 year.
- Data will be kept for as long as there is a contractual link with the member of staff concerned and for an additional period of 1 year after the ending of the contractual link.
- Data will be kept as long as follow-up actions linked to the 72 months On-site presence rule are necessary. As a consequence, data related to any interaction with Security Service will be deleted after 12 years.

ARDOS is for internal use of the Security Service. ARDOS data are never directly **transferred** or accessible from outside the Security Service as the information system resides in a physically isolated network. Information provided with a justified 'need to know' based on ARDOS data is always processed and edited in a standard document template (Nulla Osta or On-site Presence templates). Only key Human Resources people responsible for the recruitment process in all sites may request a Security Nulla Osta from the Security Service. A legal clause is attached to the requested Nulla Osta. The clause mentions Articles 7.3 and 4.2 of Regulation 45/2001. The Ispra Site Director may ask for extra information in case of an emergency or investigation.

Staff Pass Photographs of Statutory Staff of all JRC sites are exported from ARDOS and then transferred to the Guide des Services, i.e. Commission Directory based on SYSPER2. A legal clause is attached to the list of Staff Photographs. The clause mentions Articles 7.3 and 4.2 of Regulation 45/2001.

The recipients are the following: within Core Security Service staff, there are several profiles which include Security Officer and Security Archivist and Administrator. Security Officers may access personal data and photographs. 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. Key authorised Statutory Staff responsible for recruitment process are also recipients.

[3] The JRC offers *Foresteria* facilities (apartments) to non permanent staff (grant holders, etc.). The register of who is living in the *Foresteria* facilities is also stored in ARDOS.

A privacy statement is to be published on the JRC Intranet. It includes information on the identity of the controller, purposes of the processing, the categories of data concerned, recipients of the data, the existence of the right of access, and the right to rectify, the time-limit for storing the data, the right to have recourse at any time to the EDPS. No other explicit communication is foreseen due to the need to comply with varied obligations including those related to the management of Nuclear Sites. All data subjects also know that their photograph is necessary to physically produce their staff pass. The Welcome Desk directs and accompanies people in taking their photograph.

[...]

3. Legal aspects

3.1. Prior checking

This prior check Opinion relates to the collection and further processing of personal information carried out by the JRC to support the JRC's decision to issue or deny Nulla Osta for pre-selected JRC Staff applicants (except Karlsruhe staff). The ARDOS database also processes photographs of all JRC employees and information regarding the presence of people on-site (Ispra).

Regulation (EC) No 45/2001 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 or which fall within the scope of Community law*"[4]. 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 in order to determine whether individuals are eligible for Nulla Osta. Second, the personal data collected undergo "automated processing" operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001, as well as manual processing; in the last case, data form part of a filing system or are intended to form part of a filing system. Indeed, the personal information is first collected both on paper and electronically and is then stored in the ARDOS database. Finally, the processing is carried out by a Community body, in this case by the JRC, in the framework of Community 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".* Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (a), the processing of data relating to "*suspected offences, offences, criminal convictions or security measures"*. This type of information is collected to enable the JRC to assess the reliability of individuals in order to decide whether or not a Nulla Osta should be issued. In addition, under paragraph (b) *processing operation intended to evaluate personal aspects relating to the data subject, including (...) his conduct* should be subject to prior checking. The aim of the Nulla Osta procedure is to ascertain and confirm a pre-selected candidate's good conduct. In case Security Officers have some doubts about the

4 See Article 3 of Regulation (EC) No 45/2001.

elements given by the data subject, they will interview the person concerned to evaluate his conduct. Therefore the processing operations must be prior checked by the EDPS.

It has to be noted that the database ARDOS also contains the reports issued within the framework of security investigations at JRC Ispra. This specific processing operation has been prior checked by the EDPS on 31 July 2008 (file 2007-507)[5].

Since prior checking is designed to address situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. In this case however the processing operation has already been established. In the present case, this is a serious problem taking into account the conclusions of this opinion. Indeed, to be in compliance with Regulation EC 45/2001, an appropriate legal basis should be identified, produced or established and the rest of the recommendations made by the EDPS should be adopted (see conclusions in point 4).

The Notification was received on 6 June 2007. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was extended with one month due to the complexity of the matter, and suspended for a total of 401 days, plus two months of August.

3.2. 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 grounds that justify the processing operation appear to be based on Article 5(a), pursuant to which data may be processed if the processing is "*necessary for the 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 in question comply with Article 5(a) of Regulation (EC) No 45/2001 two elements must be taken into account: first, whether either the Treaty or other relevant legal instruments foresee a public interest task that entails the processing of personal data by the controller as currently at stake (legal basis), and second, whether the processing operations are indeed necessary for the performance of that task (necessity test). It should be noted at this point that no other grounds have been referred to as relevant, so that the current analysis can be limited to Article 5(a) of the Regulation.

"Nulla Osta" legal basis

In ascertaining the legal grounds in the Treaty or other relevant legal instruments (including national legislation) that could in principle legitimise the processing operation (*legal basis)*, a general remark has to be made. The Nulla Osta procedure applies to staff members of all JRC sites except Karlsruhe. This means that different countries are concerned (Spain, Italy, Belgium and the Netherlands) as well as different activities (protection and security of the citizens, environment and sustainability, health and consumer protection, etc.). Therefore, part of the legal documents proposed as legal basis by the controller referring to nuclear activities and Italian legislation are not relevant, as explained below, for non nuclear sites and and/or non Italian sites.

[5] See EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2008/08-07-31_Commission_security_investigations_Ispra_EN.pdf

In what follows, an analysis will be made of the different instruments that have been proposed by the controller as legal basis.

First, the Italian Law L. 1° agosto 1960, n.906 approving the execution of the agreement between the Italian government and the Commission has been mentioned in the notification. Article 2 of annex F refers to general security measures such as: (1) external security is guaranteed by Italian Authorities, (2) Italian Authorities will intervene on-site only upon request and consensus of the Commission, and (3) the Ispra site should not, even temporarily, host anyone who is prosecuted according to Italian law. For the record, Article 21 of annex F insists on the secrecy protection and Article 35 states that all the necessary measures should be taken by the Commission to avoid abuse of the agreement.

The points 1) and 2) of Article 2 of annex F are actually a legal basis to prevent the intervention of the Italian Authorities within the Ispra site without the consent of the Commission, while ensuring that an external problem around the site, like a demonstration, would be dealt with by the Italian Authorities. A personal security check as the Nulla Osta assessment can not be covered by these points. On the other hand, point 3) might be of particular relevance in the case in point.

Indeed, to better understand the *ratio legis* of Article 2 of annex F, it has to be reminded that the law in point establishes the agreement between the Commission and the Italian State for the founding of the nuclear research centre. Within this particular framework as within the general framework of the establishment of a Community authority or institution in a Member State, the hosting State and the Institution agree to cooperate in security matters. The rules stated in Article 2 allow defining their respective competences. The application of Article 2, point 3) requires that specific security measures are taken by the Ispra Security Service to prevent the recruitment of persons prosecuted according to the Italian law. Nevertheless, this general legal basis would only apply in the Ispra site and, even so, cannot justify investigations beyond the fact of being subject to prosecution. As to the other sites concerned, the Italian Law L. 1° agosto 1960, n.906 does not apply to JRC sites established in other countries.

Second, the JRC Physical Protection Plan, approved by a decree of the Italian Ministry of Industry (VII-260, 21/7/1987) and to which the EDPS did not have access, can not be used as a legal basis for issuing the Nulla Osta either. As the EDPS understands, this plan is established to ensure physical security in the sense of the sanitarian protection of the population working on the Ispra site and security of nuclear facilities (evacuation, etc) and not to define the Nulla Osta procedure. Moreover, the plan applies to the Ispra site and not to all JRC sites.

The Physical Protection of Nuclear Material and Nuclear Facilities document of the International Atomic Energy Agency (IAEA) gives guidelines in accessing nuclear material or facilities. The EDPS does not question the access control to nuclear material or facilities which by essence should be very scrupulous. The EDPS questions the fact that the general access to every JRC site is governed by such nuclear plan, whatever activities are performed on the site. Therefore, this document can not be considered as a legal basis for the Nulla Osta procedure.

Third, the Commission decision of 8 September 1994 describes the tasks of the Security Office of the Commission in terms of: protection of persons, protection of buildings and property and protection of information, data transmission and processing. According to the decision, the task shall include: gathering information to assess potential threats or risks to

Commission departments (Article 3.a.) and monitoring compliance with current security rules by Commission departments (Article 3.d.). Article 6 states that the Security Office shall handle relations with national security and intelligence services with a view to collecting the information required to assess potential threats and risks to the Commission, and with national authorities with respect to questions concerning the protection of Commission buildings, application of criminal laws and the immunity of officials from legal proceedings where matters of security are involved.

As it is developed below it appears necessary to adopt special security measures to ensure the protection of JRC sites. The Commission decision develops in details the tasks of the Security Office. The text nevertheless does not foresee individual security checks except *in flagrante delicto* or in the frame of an administrative investigation. The Nulla Osta procedure, being a systematic "a priori" security check, goes beyond the situations covered by the decision.

The EDPS is of the opinion that, even if the Commission decision could be used as a general legal base to implement the Nulla Osta procedure, its text is not explicit enough in describing the nature and scope of that procedure to satisfy the requirements of accessibility and predictability of a legal base under Article 8 (2) of the European Convention on Human Rights, which are also relevant under Articles 7 and 52 of the EU Charter of Fundamental Rights.

Moreover, the EDPS observes that the above legal framework does not provide a crystal-clear picture of the concrete tasks and competences that pertain to the Commission's security office (DG ADMIN Security Directorate) and those allocated to the security offices at the level of institutions, services and departments, such as the Security Service of JRC Ispra. In this regard, there is a question as to whether the Security Service of JRC Ispra is entitled to carry out activities described in the decision or whether this competence is limited to the Commission's Security Office (DG ADMIN).

Finally, Article 28 of the Staff Regulations and Articles 12.2.c and 82.3.c of the Conditions of Employment of other Servants of the EC have been mentioned in the notification. Those Articles state that a servant may be appointed only on condition that he produces the appropriate character references as to his suitability for the performance of his duties and that he enjoys his full rights as a citizen. The data processing operations notified for prior checking go far beyond the criterion established by the Staff Regulations: "*suitability for the performance of his duties*". The "Nulla Osta" is not performed by the recruitment units but by the Security Service and it is described in various documents handled by both security and recruitment services as a "security clearance". The security clearance in the EC context is performed for persons who require access to classified information (2001/844/EC, ECSC, Euratom: Commission Decision of 29 November 2001 amending its internal Rules of Procedure (notified under document number C(2001) 3031) and not as a condition for recruitment. The EDPS underlines the distinction that should be made between the collection of criminal records as a condition for recruitment and the processing operation that takes place to issue a Nulla Osta. The processing operation can not therefore take place on the basis of this legal base.

The EDPS does not challenge the necessity for the JRC to collect the criminal record in order to fulfil the condition of recruitment foreseen in Article 28. The EDPS does not challenge either the necessity to obtain EC security clearance for some staff members (see the analysis below). The EDPS questions the existence of a clear legal basis for the Security Service to perform a systematic prior Nulla Osta/security check for every single JRC staff member. For those specific aspects/needs that are not covered by Article 28 or by the EC security

clearance, the Ispra Security Service should be explicitly endowed with additional specific competences for the strictly defined needs of security. A specific legal basis should then be identified, produced or elaborated for the system, bearing in mind that the legal basis should be sufficiently precise, cover different JRC activities and countries, and respect the necessity and proportionality criteria which are developed here below.

Legal basis for staff passes and data related to foresteria

The legal basis for printing badges for all categories of JRC staff members and other staff that need to regularly enter the Ispra site can be found in the Italian Safety Regulation 626/1994 which contains articles related to the need to maintain access lists to the site and critical areas along with real-time evacuation lists should either a conventional or nuclear incident occur. The Article 34.2 of the Law L. 1° agosto 1960, n.906 is the legal basis to collect and store the data relating to the *foresteria*.

Necessity test

As to the necessity of the processing, the EDPS takes note that the protection of JRC sites is sensitive due to the nature of some activities and to the confidentiality of information processed. Taking into account the relevance of these interests and in order to prevent the unauthorised disclosure of this information (secrecy protection for e.g. as it is mentioned in Italian Law L. 1° agosto 1960, n.906, Article 21), it appears necessary for the JRC to adopt special security measures, not only vis-à-vis external threats but also vis-à-vis internal risks. The Nulla Osta procedure seems to be an internal control measure aimed towards safeguarding the nuclear policy and JRC confidential information.

Among others, such internal controls aim at preventing the access to the JRC premises of those individuals who, in the light of their background, particularly criminal history, may constitute a threat to the JRC. By the same token, in order to minimise the risk, it is important for the Centre to hire only individuals whose criminal history does not question their capacity to maintain high standards of professional ethics in the performance of their duties at the JRC. In order to filter individuals who may not be up to such standards or whose mere presence in the JRC premises may pose a threat to the JRC, it seems necessary to collect and further process personal data that reveal the criminal history of such individuals.

However, the EDPS is of the opinion that issuing a Nulla Osta of the same level for all staff is excessive in respect to the "need to know" principle. Sensitive data or areas should request specific authorisations whereas regular administrative work for instance and regular premises should not. In addition, as described above, the security clearance standard procedure exists to give access to sensitive information and premises.

The EDPS is of the opinion that the JRC should revise its policy regarding staff Nulla Osta in terms of proportionality and necessity, keeping in mind a tool like the EC security clearance.

3.3. 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.

The data processing obviously includes data relating to criminal offences and pending investigations, which is regulated under Article 10.5 of Regulation (EC) No 45/2001. For example, in all cases individuals have to provide a criminal record. 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 criminal records is authorised by the legal instruments mentioned in point 3.2 above as far as the recruitment is concerned.

As stated above in the analysis of the legal basis, the condition foreseen in Article 10.5 will only be fulfilled if a legal instrument authorising the Security Service of Ispra to collect data required to conduct a Nulla Osta procedure can be relied upon.

As far as other 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 notification for prior checking it does not appear that data falling under the categories of data referred to in Article 10.1 are processed in ARDOS. Taking into account the overall purpose pursued by JRC Ispra when it engages in data processing operations to issue the Nulla Osta, the EDPS understands that the collection of those special categories of data is not intended by JRC Ispra.

3.4. 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 they are collected and/or further processed. This is referred to as the data quality principle. In analysing whether the processing at point, which involves mainly the processing of data relating to suspicions, offences or criminal convictions, is in line with this principle, the EDPS notes the following:

First, the Privacy statement mentions the collection of a police record whereas the invitation letter for recruitment requests from the civil servant and temporary agent a recent certificate of good conduct and for the contract agent a recent certificate of good conduct/criminal record certificate. In legal terms and particularly in certain Member States, certificates of good conduct contain information that goes beyond a record containing criminal convictions. In particular, in some Member States a certificate of good conduct may contain information about the character of an individual, his moral behaviour, etc. Even if, in principle, the EDPS considers that the collection of those documents is lawful, a case by case analysis of the content of the national police record/criminal record/certificate of good conduct should be carried out so as to collect only relevant data in the light of the Staff Regulation requirements.

Second, in the absence of a clear legal basis, the data collected by the Security Service (application forms, CVs, etc) are excessive in relation to the purposes for which they are collected. The application form and the CV are not collected for the purpose of issuing a Nulla Osta but rather to secure for the institution the services of persons of the highest standard of ability, efficiency and integrity. The EDPS is of the opinion that the necessity of every category of data collected by the Security Service in the ARDOS database has to be demonstrated by the JRC. In addition, this raises the question of the legitimacy of the transfer of those data from the recruitment services to the Security Service (see point 3.6 below). The Nulla Osta file made up in the ARDOS database should under no circumstances become a duplicate of the personal file. The EDPS would like to remind that Article 26 of the Staff Regulations states that "there shall be only one personal file" and therefore CVs, application

forms, etc. which are part of the personal file should not be copied and stored in the ARDOS database.

Third, there are no criteria established to help Security Officers in issuing Nulla Osta. As mentioned above, this entails an excessive collection of data. The EDPS is of the opinion that the adoption of a formal document describing and defining the procedure put in place would help the JRC to ensure the data quality principle.

As far as individual investigation/inquiry is concerned, the necessity, the relevance and the adequacy of the data collected are analysed in the Opinion 2007-507, security investigations at JRC Ispra referred above.

Article 4.1.a of the Regulation requires that data be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 3.2.). The issue of fairness is closely related to what information is provided to data subjects, which is further addressed in Section 3.9.

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 data include criminal records. The system itself should ensure that the data are accurate. The data subject provides for the data that will be processed: CV, application form, criminal record. A procedure whereby data subjects may request and verify what data are registered and associated with them has been put in place. In this respect, see discussion under section 3.8.

3.5. 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 identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

The EDPS considers as appropriate the retention period foreseen by the JRC (data are kept for as long as there is a contractual link with the member of staff concerned and for an additional period of 1 year after the ending of the contractual link). Indeed, in case the JRC would have a legal basis to conduct a Nulla Osta procedure, it seems appropriate for the Security Service to be able to go back to the information that constituted the basis for the issuance of the Nulla Osta at any time during the employment contract plus certain additional time. On the other hand, it does not seem appropriate for the JRC to keep information for both Nulla Osta or condition of recruitment about crimes that have become outdated and which would not be reflected any longer in a criminal record. For this reason, the JRC should find a system whereby information about such crimes should be deleted. This may be achieved through the right of access and rectification, as described below under 3.8. Another solution would be a "standard form" stating that the person is suitable for the performance of his duties kept in the file whereas the criminal record would be returned to the person. The EDPS recommends that the JRC implements the retention period foreseen as soon as possible.

Moreover, data are also necessary to apply the 72 months On-site presence rule. In this regard, data related to any interaction with Security Service will be deleted after 12 years. The EDPS is of the opinion that only the data necessary for the purpose of the management of the 72 months rule should be kept.

The EDPS recommends that all historical information is kept in anonymous form or deleted from the database, in compliance with Article 4.1.e.

3.6. Transfer of data

According to the facts, information may be transferred in case of emergencies or security investigation to the Ispra Site Director (see Opinion 2007-507). Staff Pass Photographs of Statutory Staff of all JRC sites are exported from ARDOS and then transferred to the Commission Service Guide. The "Nulla Osta" can only be transferred to key Human Resources people responsible for the recruitment process in all sites, but in no circumstances will the data be transferred outside the Commission. Accordingly, Article 7 of Regulation (EC) No 45/2001 which sets forth certain obligations for data controllers when they transfer personal data to Community institutions or bodies will apply.

The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data be transferred "*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 Security Service must ensure that (i) the recipient has the appropriate competences and (ii) the transfer is necessary. This seems to be the case here. It has to be noted that the EDPS has been consulted on the introduction of photographs in the Commission Directory[6].

Pursuant to Article 7.2, where the data are transferred following a request from the recipient, both the controller and the recipient shall bear the responsibility for the legitimacy of this transfer. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified. In the case in point, the Nulla Osta procedure starts upon request of the Human Resources unit but the transfer of supporting documents (CV, application form) is requested by the Security office. The need of the transfer should be assessed once the legal basis is established.

In addition to the above, pursuant to Article 7 of Regulation (EC) No 45/2001 a notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted[7]. For reminder, notices are sent to the key Human Resources people responsible for the recruitment process and to the Commission Service Guide.

3.7. Processing of personal number or unique identifier

Article 10 (6) of the Regulation provides that "*the EDPS determines the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*".

The ARDOS database contains the personal number of the data subject. The EDPS considers that the personal number can be used appropriately in this context since it allows for the identification of the respective staff member and facilitates the follow-up in an appropriate way. There is no reason to determine any further conditions in this case.

3.8. Right of access and rectification

[6] See letter of 6 January 2005, 2005-347

[7] This issue has been discussed in the EDPS Opinion of 8 March 2006 on a notification for prior checking on "Disciplinary cases (including related administrative reviews of complaints and grievances, Ombudsman and Court cases)" (Case 2004-270).

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 Security Service provides the right of access and rectification to the database. Individuals are notified of the possibility to exercise such rights and they are given information about whom to contact to exercise these rights. In order to ensure that access requests will be dealt with in a timely fashion and without constraints, the JRC sets up a reasonable time limit of 14 days. As an example, at any given moment in time, data subjects may request and perform an update of their photograph possibly including a photograph taken by an external photographic service.

The application of the right to rectify inaccurate data may enable individuals to request the update of the criminal record. Indeed, as noted above under 3.5, crimes become outdated after a certain period of time and, as of this moment, they are not reflected any longer in a criminal record. Under Article 14 of the Regulation individuals have the right to rectify inaccurate or incomplete data, which in the case in point means that individuals should be able to update - provide for an updated version of - their criminal record in order to reflect accurately their current situation. As said above, in keeping information about crimes that have become outdated the JRC would contravene the data quality principle described above according to which personal data must be *"accurate and, where necessary, kept up to date"*.

In order to apply Articles 14, 4(1)(d) and 4(1)(e) of Regulation (EC) No 45/2001 (right of rectification, data quality and conservation principles), the JRC should set up a system intended to ensure the effective application of the content of these rights and principles as far as certificate of good conduct and criminal record are concerned.

In setting up this system, the EDPS notes that it may be difficult and cumbersome for the JRC alone to operate a scheme that deletes information on crimes that have become outdated on its own initiative, particularly because this may differ from country to country. The JRC may not be in a position to verify on an on-going basis whether the crimes contained in the certificates of good conduct of each individual are outdated or not. However, the JRC is in a position to inform individuals of the possibility of providing updated certificates of good conduct or criminal records throughout their employment relationship with the JRC.

Thus, the EDPS calls upon the JRC to remind individuals of such possibility. This can be done in the privacy statement or separately. In providing individuals with this possibility, the JRC is in fact enabling individuals to exercise their right of rectification of data that is inaccurate as recognised under Article 14 of the Regulation. It is also contributing to the application of the data quality principle. Furthermore, it is implementing the principle that limits the conservation of information when it is no longer necessary for the purposes for which it was processed.

In this regard, the EDPS notes that the JRC may need to keep certificates of good conduct for a certain time in order to have evidence justifying why it took the decision to issue a negative Nulla Osta. This need may justify the keeping of certificates of good conduct until it is no longer possible to challenge a given negative decision. This should not prevent the individual from providing an updated certificate of good conduct to be kept along side with the former one, which will be definitively deleted after the above mentioned period.

Finally, the EDPS would like to underline that the special procedure put in place for returning the original criminal record is not a means for the data subject to exercise his right of access or rectification. In addition, a copy of the criminal record is kept in ARDOS, yet the form "Police Record Return Request" lets the data subject think the contrary. This procedure does not respect the fairness of the processing operation; the procedure is not transparent and the "Police Record Return Request" should therefore be modified to avoid confusion.

3.9. Information to the data subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed. 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. Article 12 applies as the data have not been obtained directly from the data subject, the data are provided to the Security Service by the recruitment services.

The privacy statement will be posted on the Intranet. The EDPS considers that this is an appropriate method of providing the information but suggests that a copy of the privacy statement be given to individuals so that the JRC is sure that every person concerned (even the candidates who have not been recruited) is aware of the privacy statement, for example, if they want to know how to exercise their rights or how the data processing takes place.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Article 12 of Regulation (EC) No 45/2001. The EDPS considers that the privacy statement contains most of the information required under Article 12 of the Regulation; however, he considers that several amendments would contribute to ensure full compliance with Article 12, in particular:

(i) The "72 months on site rule" purpose should be added.
(ii) JRC should clarify what data are covered in the sentence "along with any other security related information collected during the existence of a contractual link with the data subject".
(iii) In order to ensure full transparency and fair processing, it would be appropriate to inform the data subjects about the origin of the data.
(iv) It would be appropriate to indicate that the "Nulla Osta" declaration is transferred to the recruitment Services.
(v) Once established a legal basis to conduct the "Nulla Osta" procedure, that legal basis should be mentioned in the privacy statement.
(vi) The words security clearance should be avoided as the JRC Security Service made clear that the Nulla Osta and the "Security Clearance" have no common points (see vocabulary used in the privacy statement and by the recruitment units).

3.10. Security measures

According to Articles 22 of Regulation (EC) No 45/2001, the controller must 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. 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.

The technical and organisational measures appear to be suitable in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected. [...]

4. Conclusion:

The processing operation as described appears to be in breach of the provisions of Regulation 45/2001 unless a clear legal basis is identified, produced or established. The EDPS moreover recommends that in order to ensure compliance with the Regulation, the above considerations are fully taken into account also in other aspects, namely:

- a case by case analysis of the content of the national police record/criminal record/certificate of good conduct should be carried out so as to collect only relevant data in the light of the Staff Regulation requirements;
- the necessity of every category of data collected by the Security Service in the ARDOS database for the purpose of the issuance of Nulla Osta has to be demonstrated;
- a formal document describing and defining the procedure put in place should be adopted to ensure the data quality principle in compliance with Article 4.1.c;
- the JRC should find a system whereby information about crimes that have become outdated are deleted. This may be achieved through the right of access and rectification or, for instance, by the adoption of a "standard form" stating that the person is suitable for the performance of his duties kept in the file whereas the criminal record would be returned to the person;
- the retention period foreseen by the JRC should be implemented as soon as possible in compliance with Article 4.2.e;
- only the data necessary for the purpose of the management of the 72 months rule should be kept in compliance with Article 4.1.e;
- all the historical information should be kept in anonymous form or deleted from the database, in compliance with Article 4.1.e;
- a system should be set up that is intended to ensure the effective application of the content of the rights of access and rectification as far as a certificate of good conduct/criminal record/police record is concerned;
- the "Police Record Return Request" should be modified following the recommendation made in point 3.8;
- several amendments should be made to the privacy statement to ensure full compliance with Article 12, as described in this opinion;
- [...]

Done at Brussels, 15 December 2008

(signed)

Peter HUSTINX
European Data Protection Supervisor