**Opinion on a Notification for Prior Checking received from the Data Protection Officer of the European Commission on Individual Medical Files at Joint Research Centre in Ispra / Seville**

Brussels, 6 February 2008 (Case 2007-329)

## 1. Proceedings

On 21 May 2007, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of the European Commission (DPO) a notification for prior checking relating to Individual Medical Files at Joint Research Centre (JRC) in Ispra / Seville.

On 7 June 2007, the EDPS requested some complementary information to the controller. A partial answer was received on 2 July 2007. A telephone conversation with the controller took place on 27 September 2007, where some aspects were clarified. Further information was requested on 8 October 2007, and a partial response was received on 12 October 2007. Finally, a meeting with the controller, the DPO and the DPC (Data Protection Coordinator of the JRC) and EDPS staff members took place on 13 November 2007, where all the remaining questions were clarified.

The draft opinion was sent to the DPO on 20 December 2007 and these were provided directly from the controller on 14 January 2008. Due to the complexity of the matter and in particular, interactions with other notifications concerning processing of medical data by JRC Medical Service in Ispra under examination (Cases 2007-505 and 2007-508), the final deadline was extended for 22 days.

## 2. Examination of the matter

### 2.1. The facts

*Purpose of the processing activity*

The purpose of the processing of personal data contained in the Individual Medical Files is to survey and to promote staff's health, according to legal and statutory obligations. It includes pre-employment visits, fitness-for-work certificates, periodic visits, final visits, radioprotection, and documentation of first aid treatment and registration of sickness. In fact, medical data contained in the Individual Medical Files (notwithstanding their origin) may be used for preventive purposes. In addition, the data collected within the (general and/or radioprotection) pre-employment visits are also used to determine the insurability or (the possible limitation of) the social security benefits of the recruited candidates.

*Categories of data subjects*

The data subjects involved in this processing activity are civil servants, temporary agents, contractual agents, auxiliary staff, grant holders and national experts.

*Categories of data*

The categories of data processed are the following: photo, first name, surname, personal number, birth date, birth place, marital status, children, profession, address, place of work, risk assessment sheet[1], dosimetry data, including WBC[2] data, medical history, actual clinical status, laboratory tests, x-ray, ECG[3], further medical tests (ophthalmologist, audiometry, spirometry, etc.) as necessary for the individual subject and other medical documents.

*Information to be given to data subjects*

Data subjects will be informed by a privacy statement. The privacy statement will be put on the board in the waiting hall of the Medical service. Furthermore, it will be published on the Intranet website of the Occupational Health and Safety Unit.

The privacy statement refers to the identity of the controller, the purposes of processing, the recipients, the existence of the right of access, the time limits for storing the data, contact information and the right to have recourse to the EDPS.

*Procedures to grant rights of data subjects*

In case the data subject want to verify which personal data are stored regarding him or her by the responsible controller, have the data modified, corrected, or deleted, he/she can write an e-mail message to the functional mailbox address indicated in the contact information, explicitly specifying the request. Upon a justified request by the data subject the personal data will be modified within 14 days.

The notification form specified that the results from medical tests and diagnosis cannot be modified, but a comment of the data subject can be added. Furthermore, a copy of all laboratory tests and technical examinations is handed over on the occasion of the periodic visit and the decision on fitness for work is communicated.

*"Employee's Declaration of Consent Form"*

According to the document entitled "Employee's Declaration of Consent Form" submitted for review (in a related notification for prior checking (2007-649)), the data subject has to declare that he/she is *"freely giving his/her consent to the authorised and competent doctors nominated by his/her employer to process his/her personal data"* collected within his/her Personal Health Document, fitness-for-work certificate, as well as the related laboratory tests.

*Automated / Manual processing operation*

The medical files are manually processed.

[1] Fiche de poste de travail.
[2] Whole body counter (external dosimetry)
[3] Electrocardiogram.

*Recipients to whom the data might be disclosed*

- Other Institutional Medical Services (Brussels, Luxembourg, agencies): on request, medical files will be sent to other institutional Medical Services in case of transfer of the employee.

- JRC Qualified Nuclear Physicist Experts as identified in the Directive 96/29 and Legislative Decree 203/95 receive some document from the medical service but always without diagnosis.

- Human Resources Unit: the fitness-for-work certificate is send after the (general and radioprotection related) pre-employment visit, the radioprotection related periodical visit, the sick leave or accident and after the final visit.

Furthermore, data could also be sent temporarily to the following recipients:

a) Legal Service, in the framework of an appeal at the European Union Civil Service Tribunal, for the preparation of their intervention;

b) judges of the European Union Civil Service Tribunal, in case of request; or

c) the European Ombudsman, on his request.

*Retention policy*

The medical files are kept for the whole time of employment of the data subjects and up to 30 (standard and/or radiation exposure) or 40 years (carcinogenic agents) after the end of work (based on Legislative Decrees 626/94, 230/95, 241/00).

Article 34 of the Directive 96/29 (ionising radiation) transposed into Legislative Decree 230/95 requires a storage of medical records containing results of pre-employment and periodical visits "until the individual has or would have attained the age of 75 years, but in any case not less than 30 years from the termination of the work involving exposure to ionising radiation".

The retention period of medical files of data subjects that have not been recruited after pre-employment visit is five years.

*Security measures*

The medical files are stored in locked file containers. Outside working hours there is an alarm system connected to the security service in case of opening by force. The medical files for retired and out-of-contract staff are accessible with card and code reader by medical staff only.
A smoke-detection system is installed in all rooms, where files are kept.

## 2.2. Legal aspects

### 2.2.1. Prior checking

*Presence of elements that trigger the application of Regulation (EC) No. 45/2001*

The prior checking relates to the processing of personal data contained in Individual Medical Files held by the DG JRC of the European Commission (Articles 2(a) and (b) of Regulation (EC) No. 45/2001 (hereinafter "the Regulation"). The processing activity is carried out by a European institution, in the framework of Community law (Article 3.1 of the Regulation). The data processed form part of a filing system (Article 3.2 of the Regulation). As a consequence, the Regulation is applicable.

*Assessment of whether the data processing operations fall under Article 27 of the Regulation*

Article 27.1 of the Regulation subjects to prior checking by the EDPS all *"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.

Under Article 27.2(a) of the Regulation, *"processing of data relating to health"* shall be subject to prior checking by the EDPS. In the case in point, the processing operation clearly involves health related data.

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, the processing activities have already started. However, considering the circumstances of this particular case, this is not a serious problem as far as any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 21 May 2007. According to Article 27.4 the present Opinion must be delivered within a period of two months. The procedure has been suspended during 184 days (128 + 25 + month of August) and extended for 22 days. The Opinion will be issued no later than on 13 February 2008.

### 2.2.2. Lawfulness of the processing and legal basis

The processing in question has to be examined in light of Article 5 (a), (b) and (d) of the Regulation.

Article 5(a) of the Regulation stipulates that personal data may be processed only 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"*. Recital 27 of the Regulation further specifies that *"processing of data for the performance of tasks carried out in the public interest of the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies"*.

In order to determine whether the processing operations comply with Article 5(a) of the Regulation three elements must be taken into account: first, whether either the Treaty or other legal instruments foresee the data processing operations carried out by the JRC; 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.

As far as the first element is concerned, the legal basis for the data processing being analysed can be found in Articles 28, 33 and 59 of the EC Staff Regulations, as well as in Article 1 of the Annex VIII to the EC Staff Regulations.

Article 28: *"An official may be appointed only on condition that: (...); (e) he is physically fit to perform his duties; (...)".*

Article 33: *"Before appointment, a successful candidate shall be medically examined by one of the institution's medical officers in order that the institution may be satisfied that he fulfils the requirements of Article 28(e).*

*Where a negative medical opinion is given as a result of the medical examination provided for in the first paragraph, the candidate may, within 20 days of being notified of this opinion by the institution, request that his case be submitted for the opinion of a medical committee composed of three doctors chosen by the appointing authority from among the institution's medical officers. The medical officer responsible for the initial negative opinion shall be heard by the medical committee. The candidate may refer the opinion of a doctor of his choice to the medical committee. Where the opinion of the medical committee confirms the conclusions of the medical examination provided for in the first paragraph, the candidate shall pay 50% of the fees and of the incidental costs".*

In addition, Article 1 of Annex VIII of the Staff Regulations provide that if *"the medical examination made before an official takes up his duties shows that he is suffering from sickness or invalidity, the appointing authority may, in so far as risks arising from such sickness or invalidity are concerned, decide to admit that official to guaranteed benefits in respect of invalidity or death only after a period of five years from the date of his entering the service of the Communities"* (i.e. decide that expenses arising from such sickness or invalidity are to be excluded from the reimbursement of expenditure provided for in Article 72 of the Staff Regulations). The medical questionnaire / pre-employment visit also contribute to the determination of the insurability of the data subject.

Moreover, Article 59 of the EC Staff Regulations stipulates: *"1. An official who provides evidence of being unable to carry out his duties by reason of illness or accident shall be entitled to sick leave.*

*The official concerned shall notify his institution of his incapacity as soon as possible and at the same time state his current address. He shall produce a medical certificate if he is absent for more than three days. This certificate must be sent on the fifth day of absence at the latest, as evidenced by the date as postmarked. Failing this, and unless failure to send the certificate is due to reasons beyond his control, the official's absence shall be considered as unauthorised.*

*The official may at any time be required to undergo a medical examination arranged by the institution. If the examination cannot take place for reasons attributable to the official, his absence shall be considered as unauthorised as from the date that the examination is due to take place.*

*If the finding made in the examination is that the official is able to carry out his duties, his absence shall, subject to the following sub-paragraph, be regarded as unjustified from the date of the examination.*

*If the official considers the conclusions of the medical examination arranged by the Appointing Authority to be unjustified on medical grounds, he or a doctor acting on his behalf may within two days submit to the institution a request that the matter be referred to an independent doctor for an opinion.*

*The institution shall immediately transmit the request to another doctor agreed upon by the official's doctor and the institution's medical officer. Failing such agreement within five days of the request, the institution shall select a person from a list of independent doctors to be established for this purpose each year by common consent of the Appointing Authority and the Staff Committee. The official may within two working days object to the institution's choice, whereupon the institution shall choose another person from the list, which choice shall be final.*

*The independent doctor's opinion given after consultation of the official's doctor and the institution's medical officer shall be binding. Where the independent doctor's opinion confirms the conclusion of the examination arranged by the institution, the absence shall be treated as unjustified from the date of that examination. Where the independent doctor's opinion does not confirm the conclusion of that examination, the absence shall be treated for all purposes as having been justified.*

*2. If, over a period of 12 months, an official is absent for up to three days because of sickness for a total of more than 12 days, he shall produce a medical certificate for any further absence because of sickness. His absence shall be considered to be unjustified as from the thirteenth day of absence on account of sickness without a medical certificate.*

*3. Without prejudice to the application of the rules on disciplinary proceedings, where appropriate, any absence considered to be unjustified under paragraphs 1 and 2 shall be deducted from the annual leave of the official concerned. In the event that the official has no outstanding leave entitlement, he shall lose the benefit of his remuneration for the corresponding period.*

*4. The Appointing Authority may refer to the Invalidity Committee the case of any official whose sick leave totals more than 12 months in any period of three years.*

*5. An official may be required to take leave after examination by the institution's medical officer if his state of health so requires or if a member of his household is suffering from a contagious disease.*

*In cases of dispute, the procedure laid down in the fifth to seventh subparagraph of paragraph 1 shall apply.*

*6. Officials shall undergo a medical check-up every year either by the institution's medical officer or by a medical practitioner chosen by them.*

*In the latter case, the practitioner's fees shall be payable by the institution up to a maximum amount fixed for a period of no more than three years by the Appointing Authority after consulting the Staff Regulations Committee."*

As far as the second element is concerned, the processing of medical data in the present context can be considered as an activity conducted in the public interest.

As far as the third element is concerned, the necessity of the processing has to be evaluated in the light of the purpose. In the present case, the processing is, in principle, necessary for the purposes described.

Furthermore, the current processing is *"necessary for compliance with a legal obligation to which the controller is subject"* (Article 5(b) of the Regulation). Indeed, the controller has to respect several Italian laws imposing specific obligations concerning protection of

occupationally exposed workers against conventional and ionising radiation related[1] risks. In particular, he has to comply with the medical surveillance obligations laid down in Articles 81, 83 - 85, 87, 90 - 91 of the Legislative Decree 230/95[2] (transposing EC Directives concerning ionising radiation) and Articles 16 and 17 of the Legislative Decree 626/94[3] (transposing EC Directives concerning conventional risks).

Finally, the further processing of medical data collected in the above mentioned context (pre-employment visits, registration of sick leave[4] and external annual visits) for preventive purposes shall be examined in light of Article 5(d) of the Regulation according to which the processing must be based an *"unambiguous consent"* of the data subject. Consent is also gathered in case of HIV test.

In terms of Article 2(h) of the Regulation, the data subject's consent is *"any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*. It should be also noted that the present case concerns consent in the employment context and therefore, the following remarks of the Working Party 29 in its Opinion 8/2001[5] should be duly taken into account: "*where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 [of the Directive 95/46/EC] as it is not freely given. If it is not possible for the worker to refuse, it is not consent. Consent must all times be freely given. Thus a worker must be able to withdraw consent without prejudice*".

The EDPS is of the opinion that the further processing of medical data for preventive purposes could be considered as lawful provided that it is based on an informed and freely given consent of the data subject (see point 2.2.9). In this context, the EDPS would like to express concerns as to the current practice related to the use of the "Employee's Declaration of Consent Form". In any case, the data subject should be given a possibility to refuse and/or withdraw his/her consent with respect to further processing of his/her medical data for preventive purposes.

### 2.2.3. Processing of special categories of data

According to Article 10 of the Regulation, the processing of personal data concerning health is prohibited unless grounds can be found in Article 10(2) and 10(3).

As it has been explained above, the justification for processing of health related data is to be found in the EC Staff Regulations, as well as in the Italian Legislative Decrees transposing the EC Directives concerning the protection of occupationally exposed workers. The processing in question is therefore compliant with Article 10(2)(b) according to which the prohibition shall not apply where the processing is *"necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised*

---

1 Dosimetry data is not processed in Spain.

2 Legislative Decree 230/95 transposing Directives 89/618/Euratom, 90/641/Euratom, 92/3/Euratom and 96/29/Euratom concerning ionising radiation

3 Legislative Decree 626/94 transposing Directives 89/391/EEC, 89/654/EEC, 89/655/EEC, 89/656/EEC, 90/269/EEC, 90/270/EEC, 90/394/EEC, 90/6 79/EEC, 93/88/EEC, 97/42/EEC and 1999/38/CE concerning improvement of health and security during work

4 See EDPS opinion in case 2007-508 (control of sickness or accident related absences at JRC Ispra and Seville)

5 Opinion 8/2001 on the processing of personal data in the employment context of 13 September 2001 (5062/01/EN/Final. WP 48)

*by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof".*

The prohibition regarding the processing of data concerning health can also be lifted where the processing is *"necessary for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy"* (Article 10(3)). By virtue of their function, the medical officers and nurses are health professionals subject to the obligation of professional secrecy. In any case, the further processing of medical data for preventive purposes shall be based on an informed consent of the data subject (see above point 2.2.2.).

Furthermore, in the event of the transfer of data relating to health to third parties other than the Medical Service, it must also be ensured that Article 10 is complied with (see point 2.2.7. below).

### 2.2.4. Data Quality

According to Article 4(1)(d) personal data must be *"adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed".*

Even though certain standard data will always be present in medical files such as the name, data of birth and personnel number, the precise content of a medical file will of course be variable according to the case. 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 the files reminding them of the rule and recommending that they ensure its respect.

Data quality must also be ensured in any medical questionnaire submitted to potential or actual agents during the respective medical visits. Any information requested must be pertinent as concerns the purpose for which the data are collected. In particular, the data subjects need to be clearly informed about the purposes for which the particular data are collected and further processed (see point 2.2.9.) and the further processing of medical data for preventive purposes has to be based on their informed consent (see point 2.2.2.).

The primary purpose of the questionnaire used for the pre-employment visits is to determine whether or not the person is physically and/or mentally fit to perform his/her duties[1]. This raises the issue as to what can be considered as medical data which are likely to have an impact on the performance of an agent's duties. In any event the type of data will vary according to the type of function (office work or other, for example). The EDPS would like to underscore the fact that the relevance of a series of data collected in the questionnaire must be demonstrated as concerns the medical fitness to carry out one's duties: on this point the EDPS questions the relevance of information such as that concerning the spouse or children's past or present medical condition. The EDPS recommends an evaluation of the data in the questionnaire on medical relevance in the light of the data protection principles.

[1] See also cases T-121/89 and T-13/90 in which the Court of First Instance has found that "the medical officer of the institution may base his finding of unfitness not only on the existence of present physical or psychological disorders but also on a medically justified prognosis of potential disorders capable of jeopardizing the normal performance of the duties in question in the foreseeable future".

The medical questionnaire submitted at the time of the medical examination for recruitment also contributes, then, to the determination of the insurability of the data subject (with respect to certain social security benefits). However one must bear in mind that no more data than strictly necessary for this precise purpose may be communicated to the Appointing authority and by the authority to the payment unit.

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 case concerns processing of medical data such as results of medical examinations or notes taken down by a medical officer. The accuracy of these data cannot be easily ensured or assessed. However, the EDPS underlines the necessity for the institution to take every reasonable step to ensure that the data processed are accurate and kept up to date. For example, so as to ensure the completeness of the file, any other medical opinions submitted by the data subject must also be kept in the medical files. As described in point 2.1 of the present Opinion, this policy is respected.

Lastly, data must also be *"processed fairly and lawfully"* (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, it is related to the information to be given to the data subject (see below point 2.2.9.).

### 2.2.5. Conservation of data/ Data retention

Personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes"* (Article 4(1)(e) of the Regulation).

As indicated above, the medical files are kept for the whole time of employment of the data subjects and up to 30 (standard and/or radiation exposure) or 40 years (carcinogenic agents) years after the end of work (based on Legislative Decrees 626/94, 239/95, 241/00), in view of possible occupational diseases' related claims. In addition, the data of non-recruited candidates are kept for five years after the pre-employment visit.

Considering that the storage of accurate data related to the exposure to occupational risks may have significant relevance in the context of medical treatment of the individual, and/or in view of possible claims even after several years for alleged occupational disease, the EDPS finds reasonable the time limit prescribed by law for which the personal data are kept.

As to the storage of the "standard" data, the EDPS would like to recall his recommendations issued on 26 February 2007 in case 2006-532 in response to the request of the Collège des Chefs d'administration to comment on the Collège's proposal of a uniform 30-year conservation period for all medical data across the Community institutions. In his recommendations, the EDPS invited the Collège to examine, on a case by case basis, what conservation periods are necessary for specific medical documents, considering that Article 4(e) of the Regulation requires that data should be kept no longer than is necessary for the purposes for which they are processed.

A further point must be made as concerns the conservation of medical exams concerning candidates, which, even after having been subjected to a medical examination have not been recruited whether or not this is linked to a medical reason. The EDPS maintains that the data should only be kept within a certain time frame, which could be that of the period during which the data or decision taken on the basis of such data, can be contested or the time during which the examination is valid. Therefore, the conservation time has to be reduced, and data has to be destroyed after this moment.

### 2.2.6. Change of purpose / Compatible use

Article 4(1) (b) of Regulation 45/2001 provides that personal data must be *"collected for specified, explicit and lawful purposes and not further processed in a way incompatible with those purposes"*.

As indicated above, medical data collected during pre-employment visits, registration of sick leave and external annual visits may be also used for preventive purposes. The EDPS is of the opinion that this further processing does not involve a general change of purpose provided that the person concerned is clearly informed about the possibility of this further processing and the processing is based on his/her explicit consent (see points 2.2.2 and 2.2.9).

### 2.2.7. Transfer of data

Article 7 of the Regulation stipulates: *"(1) 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"*.

As explained above, the medical files may be transmitted to other institutional Medical Services (Brussels, Luxemburg, agencies) in case of transfer of the employee. In addition, certain data can be transferred to the JRC Qualified Experts and the fitness-for-work certificate is transferred to the Human Resources Unit after the pre-employment visit, the radioprotection related periodical visit, the sick leave or accident and the final visit. These transfers are necessary for the legitimate performance of the supervisory tasks in the area of protection against occupational risks.

Moreover, data can also be transferred to the Legal Service, the European Civil Service Tribunal, the Ombudsman and the EDPS. In those cases, Article 7.1 is also respected.

Article 7.3 of the Regulation specifies the obligation to process data only for the purpose for which they have been transmitted. This rule is respected in what concerns the transfer to the Human Resources Unit. The same reminder should also be sent to the Services and Institutions mentioned above in case of transfer.

### 2.2.8. Right of access and rectification

According to Article 13 of the Regulation, 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.

Article 20 of the Regulation provides for certain restrictions to this right notably where such a restriction constitutes a necessary measure to safeguard the protection of the data subject or of

the rights and freedoms of others. In certain cases, for instance when the patient suffers from a mental illness and accessing his/her data could be detrimental for him/her, the access could be restricted to the data subject (Article 20.1(c)). In those circumstances, an indirect access should be guaranteed, for instance by the patient's physician.

As described in point 2.1 of the present Opinion, Article 13 of the Regulation is respected since the right of access is guaranteed.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. This right is somewhat limited as regards medical data to the extent that the accuracy or completeness of medical data is difficult to guarantee. It may however apply when it concerns other types of data contained in medical files (administrative data, for example). Furthermore, as mentioned above (quality of data, point 2.2.4), the data subject may request the completeness of his medical file in the sense that he/she may request that information such as contra opinions by another medical officer or a Court decision on an element of the medical file be placed in his file so as to ensure up-dated information.

### 2.2.9. Information to the data subject

Articles 11 and 12 of the Regulation provide for information to be given to data subjects in order to ensure the transparency of the processing of personal data. Article 11 provides that when the data is obtained from the data subject, the information must be given at the time of collection. When the data have not been obtained from the data subject, the information must be given when the data are first recorded or disclosed, unless the data subject already has it (Article 12).

In the present case, Article 11 of the Regulation is applicable to the collection of information during the medical exam prior to the entry into service. This should be the occasion to provide the data subject with adequate information at least concerning the processing of medical data in the framework of the medical examination. In the cases where the data is received from the medical service, compliance with Article 12 must be assured at the moment of the recording of such data.

The information included in the Privacy Statement respects, in principle, the content of those Articles. Nevertheless, it has to be noted that when consent is required (see point 2.2.2) information has to be given in the light of Article 11.1(d) of the Regulation. Furthermore, the means to provide these information do not necessarily ensure that the data subject will actually receive it (it may happen that the data subject does not read the board in the waiting hall of the Medical Service; people who have not yet been engaged do not have access to the Intranet). Therefore, the EDPS recommends, given the character of the data being processed, that the data controller uses other means in order to ensure that the data subject receives this information. In particular, the Privacy Statement could be included in the form / questionnaire that the data subject has to fill in).

### 2.2.10. Security measures

After careful analysis by the EDPS of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

**Conclusion:**

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the above considerations are fully taken into account. In particular, the JRC should:

- modify the "Employee's Declaration of Consent Form" used in connection with processing of medical data so that the data subject is given a possibility to refuse and/or withdraw his/her consent with respect to further processing of his/her medical data for preventive purposes;
- provide guarantees 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 the files reminding them of the rule and recommending that they ensure its respect;
- assess the relevance of a series of data collected in the questionnaire as concerns the medical fitness to carry out one's duties. The EDPS recommends an evaluation of the data in the questionnaire on medical relevance in the light of the data protection principles;
- not communicate more data than strictly necessary for the precise purpose mentioned to the Appointing authority and by the authority to the payment unit;
- take every reasonable step to ensure that the data processed are accurate and kept up to date. For example, so as to ensure the completeness of the file, any other medical opinions submitted by the data subject must also be kept in the medical files;
- examine, in the context of the Collège des Chefs d'administration, on a case by case basis, what conservation periods are necessary for specific medical documents, considering that Article 4(e) of the Regulation requires that data should be kept no longer than is necessary for the purposes for which they are processed;
- reduce the conservation time of data related to candidates, who even after having been subjected to a medical examination, have not been recruited;
- provide information in the light of Article 11.1(d) of the Regulation when consent is required;
- use other means in order to ensure that the data subject receives the information. In particular, the Privacy Statement could be included in the form / questionnaire that the data subject has to fill in.

Done at Brussels, 6 February 2008

Peter HUSTINX
European Data Protection Supervisor