Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission on "First Aid, Accidents at work and other Medical Examinations" at JRC (Joint Research Centre) in Ispra

Brussels, 25 January 2008 (Case 2007-0372)

1. Proceedings

On 21 May 2007, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of the European Commission a notification for prior checking relating to "First Aid, Accidents at work and other Medical Examinations" at JRC (Joint Research Centre) in Ispra.

On 21 June and 27 July 2007, the EDPS requested some complementary information from the European Commission DPO. Certain aspects were clarified during a telephone conversation with the controller on 27 September 2007. A further information request together with the draft facts was sent on 8 October 2007, and a partial reply was received on 12 October 2007. Certain outstanding issues were clarified during a meeting with the controller, the DPO and the DPC (Data Protection Coordinator of the JRC) and EDPS staff members that took place on 13 October 2007. Furthermore, certain information requested was provided on 14 November 2007. Finally, on 20 December 2007, the draft opinion was sent to the DPO for comments and factual clarification. The comments together with the outstanding requested information were received directly from the controller on 17 January 2008.

2. Examination of the matter

2.1. The facts

Purpose of the processing activity

The purpose of the processing is medical surveillance including clinical tests performed during the pre-employment and periodical visits and vaccinations, the documentation of provision of first aid and proper processing of accidents at work[1].

Categories of data subjects

[1] However, Individual Medical Files as well as the processing of the clinical test results within PowerLab are subject to a separate prior checking (EDPS 2007-272 and EDPS 2007-649 respectively).

Postal address : rue Wiertz 60- B-1047 Brussels
Offices : rue Montoyer 63
E-mail : phustinx@edps.eu.int
Tel.: 02-283 19 00 - Fax : 02-283 19 50

The data subjects involved in this processing activity are all JRC staff and their family members, external staff under JRC contract, visitors on-site.

Categories of data

The categories of data processed are the following: first name, surname, personal number, birth date, place of work, case history, clinical findings, kind of treatment, accident declaration. This data will integrate the individual medical file (see Opinion 2007-0329).

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 in case the data subject has questions related to the processing of personal data 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.

The Privacy Statement specified that the results from medical tests and diagnosis cannot be modified, but a comment of the data subject can be added.

Automated / Manual processing operation and storage media

The following processing activities are conducted in an automated way (data is stored in computers):

- Spirometry: test results are stored automatically in a computer attached to the spirometry machine.
- First aid: introduction of personal and medical data in a stand-alone computer.

The following processing activities are conducted manually (data is stored in paper files):

- Accidents at work: processed through manually administrated registers.
- Radiology: processed through manually administrated registers.
- Vaccinations: processed through manually administrated registers.

Recipients to whom the data might be disclosed

Personal data related to accidents at work are transferred to the Safety inspector and the Director or Head of unit concerned in accordance with an internal procedure established for the analyses and prevention of work injuries.

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;

c) the European Ombudsman, on his request; or

d) the EDPS.

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 (radiation exposure) years after the end of work (based on Italian Legislative Decrees 626/94[1], 230/95[2], 241/00[3]).

Time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject)

Upon a justified request by the data subject the personal data will be modified within 14 days. Results from medical tests and diagnosis cannot be modified, but the patient's comments can be added.

Security measures

The paper files are stored in locked cupboards. The computer is not connected to the internal network backups; access is protected by user-id and password. The Medical Service is protected by an anti-intrusion system and a smoke-detection system. Furthermore, the Medical Service is under security-service surveillance outside working hours.

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 related to clinical tests and vaccinations, the documentation of provision of first aid and data resulting from proper processing of accidents at work 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 processing of personal data is carried out partly by automatic means and data

[1] Italian 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, 90/679/EEC, 93/88/EEC, 97/42/EEC and 1999/38/CE concerning improvement of health and security during work

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

[3] Italian Legislative Decree 241/00 transposing Directive 96/29/Euratom concerning the protection of general public and workers against the dangers arising from ionising radiation

processed manually are 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 is directly related to the processing of 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 210 days (179 + the month of August). The Opinion will be issued no later than 18 February 2008 (17 February 2008 being a Sunday).

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 33 and 59.6 of the EC Staff Regulations (pre-employment and periodical visits).

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

Finally, the further processing of medical data collected in the above mentioned context (pre-employment visits, first aid) 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. 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"*. In any case, such consent must be explicit.

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 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 7 is complied with (see point 2.2.6 below).

[1] Dosimetry data is not processed in Spain.

[2] 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, 90/679/EEC, 93/88/EEC, 97/42/EEC and 1999/38/CE concerning improvement of health and security during work

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 files mentioned in the present Opinion 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 to them that they ensure the respect of the rule.

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 and clinical tests 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, in order to ensure the completeness of the files, 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 is the current practice.

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 2.2.8).

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 (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.

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 for alleged occupational disease even after several years after the end of occupation, 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 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. This could be done by categories of data or documents.

2.2.6. 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, personal data related to accidents at work are transferred to the Safety inspector and the Director or Head of unit concerned in accordance with an internal procedure established for the analyses and prevention of work injuries.

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 complied with.

In order to ensure compliance with Article 7.3 of Regulation, the EDPS recommends that the Human Resources Unit is reminded of its obligation to process the data only for the purpose for which they have been transmitted. The same reminder must also be sent to the Services and Institutions mentioned above.

2.2.7. 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. As described in point 2.1 of the present Opinion, Article 13 of the Regulation is respected.

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 that any other information submitted by the data subject, such as opinions by another medical officer or a Court decision concerning an element of the medical file, is being placed in his file so as to ensure up-dated information.

2.2.8. 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. Both Articles are applicable in the present case since the data processed are partly provided by the data subjects and partly by the respective Medical Service staff.

As indicated above, the data subjects will be informed via a Privacy Statement posted on the Medical Service waiting hall board, as well as on the respective Intranet webpage. The information included in the Privacy Statement respects 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 another means in order to ensure that the data subject receives this information. In particular, the information listed in Articles 11 and 12 of the Regulation may be personally given before the examination of the patient.

2.2.9. 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:

- 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 to them that they ensure the respect of the rule;
- examine, in the context of the Collège des Chefs d'administration what conservation periods are necessary for specific medical documents; this could be done by categories of data or documents;
- 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.

Done at Brussels, 25 January 2008

Peter HUSTINX
European Data Protection Supervisor