Opinion on the notification for prior checking from the European Commission's Data Protection Officer regarding the dossier "Asbestosis: Screening and follow-up – 'Asbestos' Database (Medical Service and psychological/social measures BXL)"

Brussels, 27 July 2007 (Dossier 2004-227)

1. Procedure

By letter received on 26 February 2007, the Commission's Data Protection Officer (DPO) gave notification within the meaning of Article 27(3) of Regulation (EC) No 45/2001 (hereinafter referred to as "the Regulation") regarding the dossier "Asbestosis: screening and follow-up – "Asbestos" Database (Medical Service and psychological/social measures BXL)".

Some questions on the dossier were put to the controller in an e-mail from the European Commission's Data Protection Officer on 1 March and 14 May 2007, and replies were sent on 13 April and 6 July respectively. On 23 July, the DPO was given a period of 10 days to comment on the European Data Protection Supervisor's draft opinion. His reply was received on 27 July.

2. Facts

The processing of medical data in the dossier "Asbestosis: screening and follow-up – "Asbestos" Database (Medical Service and psychological/social measures BXL)" is intended to establish and safeguard the personal interests of staff (identification of potential occupational disease) who worked in the "Berlaymont" and "Guimard" buildings before those buildings were evacuated (because of the presence of asbestos used in their construction).

The data subjects are officials and temporary staff who worked in the two buildings, the Berlaymont and the Guimard, before they were evacuated, and who attended "Asbestos" screening sessions organised by the Commission.

The categories of personal data processed in the "Asbestos" database are as follows:

- Principal data:

–Personnel No.
–Status
–Date of birth
–Surname and first name
–Sex
–Nationality
–Language

- File

–General comments
–Dates: of opening, coordination, evaluation, closure, re-contact
–Building
–No months

- Tests

–Date
–Type
–Report
–Invoice
–Clinic
–Doctor
–Comments
–List of tests carried out

- Accounting

–List of invoices[1] (Number, date, amount in currency, currency, amount in BEF, GIBUS No[2], date of payment)

- Doctors

–List of doctors consulted (Type of doctor, name of doctor, date of beginning, date of end)

Persons whose data are in this database are aware that their medical data are being processed, because it was they themselves who went to the asbestos screening organised by the Commission. Screening is not compulsory; staff are free to decide whether or not to take the tests.

In addition, a confidentiality declaration is published on the Commission's intranet. The link to this declaration was sent by e-mail (blind copy) to all those who had undergone screening. This declaration contains the following information: the identity of the controller; the purposes of the processing; the recipients or categories of recipients of the data; the existence of the right of access to, and the right to rectify, the data concerning him or her (the data subject); the time-limits for storing the data and the right to have recourse at any time to the European Data Protection Supervisor (EDPS).

On written request to the head of the Medical Service, the officials and temporary staff concerned may have access to their medical records, under the conditions laid down in Conclusion 221/04 of the Board of Heads of Administration: their data are communicated to them when consultation is authorised. This document acknowledges that "Officials and

[1] Reimbursements are made directly by the Medical Service (MS) itself. At the time of the transaction, the MS states the reason for the payment and the invoice number, but the patient's name is not mentioned.
DG BUDG can inspect payments, but the invoice remains in the Medical Service; it is not forwarded to DG BUDG. The patient's name is known only to the MS, except in the case of ex post audits by the Directorate or ADMIN/D.

[2] GIBUS no longer exists. It was replaced first by Sincom1, then by Sincom2; since January 2005 it has been replaced by ABAC **(A**ccrual **B**ased **AC**counting). ABAC is the Commission's accounting system, for which DG Budget is responsible. The ABAC No is entered in place of the GIBUS No.

temporary staff shall have the widest possible access to their medical files, under the following conditions: 1. The file must be consulted on the premises of the Medical Service of the institution, in the presence of a person designated by the Medical Service. (...) 3. The official or servant may not have access to personal notes by doctors if, under the terms of Article 20(1)(c) of Regulation No 45/2001 and on the basis of a case-by-case examination, this is necessary to safeguard the protection of the person concerned or the rights and freedoms of others".

In addition, point 5 of the confidentiality declaration, which replies to the question "How do you check, amend or delete your administrative data?", states: "If you wish to check, amend, correct or erase your personal data, you must apply to the Head of the Medical Service in Brussels, who acts as controller for this processing operation. The results of medical examinations and the diagnosis cannot be changed, but your comments may be added (...)".

The data processing is partially automated. Data recording and paper archiving are done by an individual member of staff in the Medical Service's accounts unit. The data in question are encoded via a Visual Basic 6.0 client-server interface between the Oracle database and the Data Centre (DC). The data contained in the database are made available to medical officers and their medical secretariats at their request.

Documents on paper (medical reports) are filed under the person's name and kept in secure archives to which only authorised personnel have access.

Consultation of the files containing medical data remains strictly reserved for medical officers of the Institution and two outside lung specialists who are under a duty of professional secrecy[3].

The hospital centre[4] which carries out the tests sends a copy of the reports and medical tests to the doctor of the person concerned and to the Commission. The Commission then forwards the results of the tests to the person concerned.

In the course of a request for recognition of an occupational disease (Article 73 of the Staff Regulations), the applicant's medical reports and tests are forwarded to the department of the Sickness Insurance Office of the European Institutions which deals with this procedure for recognition of occupational diseases.

---

[3] In 1996, given the urgency and sensitivity of the issue, an agreement was concluded between the European Commission (Mr F. De Koster, Director-General for Staff and Administration) and the General Coordinator of the KUL/Leuven (Prof. J. Peers). In that agreement, concluded for an indefinite period, the KUL undertakes to submit to the Commission a pilot study on the possible effects of asbestos in the Berlaymont. The study was sent to the Commission on 28 October 1996.

The agreement also provides for lung specialists to be consulted on each of the data subjects. The lung specialist is required to make a full medical report to the Commission Medical Service and to the person's doctor.

The lung specialists are outside doctors with full medical independence who are subject to Belgian legislation on data protection and medical confidentiality. At the time Directive 95/46 was still quite recent and the duty of medical confidentiality offered sufficient guarantees, so that there was no need for special instructions on the security of data processing.

[4] The hospital centres were chosen by the head of unit at the time, in response to the express request made by the Commission in October 1995. These hospitals were chosen mainly in the light of their medical expertise (references in pneumology) and also the fees charged. The persons concerned who are required to undergo one of these tests receive a list of specialists, from which they are free to choose. The doctor sends the invoice directly to the Medical Service.

In addition, some data in the files may be made temporarily available to:

(a) the Legal Service, so that it can prepare a statement of defence in the event of proceedings before the Civil Service Tribunal; or

(b) the Judges of the Civil Service Tribunal, at their request; or

(c) the European Ombudsman, at his request.

The data in this database are kept for 40 years after exposure to carcinogens or mutagens.

Directive 2004/37/CE of the European Parliament and of the Council of 29 April 2004 on the protection of workers from the risks related to exposure to carcinogens or mutagens at work is the legal basis which lays down how long records must be kept.

Article 15 : *« Record keeping:*

1. *The list referred to in point (c) of Article 12, and the medical record referred to in Article 14(4) shall be kept for at least 40 years following the end of exposure, in accordance with national laws and/or practice. (…)»*

The data may be blocked or erased within 15 working days following a substantiated request to the controller.

Security measures have been adopted. All the security measures are integrated into the application.

The database is accessible to those in charge of the DIGIT IT project, the Medical Service and the DC, with appropriate security managed by the DC (user and Oracle role attributed to users); it is not accessible on the network.

It is a local database but accessible via the net1 network on the dedicated Oracle server managed at the DC.

Access to paper archives and to the building is restricted to authorised persons.

3. Legal aspects

3.1 Prior checking

Regulation (EC) No 45/2001 applies to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law (Article 3(1)). This case involves data processing carried out by the Commission, in the course of activities which fall under the first pillar, and thus within the scope of Community law.

The processing of files in the case in point is both manual and automated, so Article 3(2) is applicable. This processing therefore falls within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 makes subject to prior checking by the EDPS any *"processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes"*.

The processing also comes within the provisions of Article 27(2)(a): *"the following processing operations are likely to present such risks: processing of data relating to health ..."*, which is the case here, since there can be no doubt that the data fall within the scope of "data relating to health "[5] and medical data.

In principle, checks by the EDPS should be performed before the processing operation is implemented. In this case, as the European Data Protection Supervisor was appointed after the system was set up, the check necessarily has to be performed *ex post*. However, this does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented.

Notification was received from the Commission's DPO on 26 February 2007. Pursuant to Article 27(4) of the Regulation, the EDPS should have delivered his opinion within two months. Taking into account the days of suspension, the EDPS will deliver his opinion by 6 August 2007 at the latest (26 April 2007 plus 100 days suspended), as laid down in Article 27(4) of the Regulation.

3.2. Lawfulness of processing and legal basis

Article 5(a) of the Regulation provides 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 in the legitimate exercise of official authority vested in the Community institution*". Management of the dossier "Asbestosis: screening and follow-up – "Asbestos" database (Medical Service and psychological/social measures BXL)" comes within the legitimate exercise of official authority vested in the Community institution; the processing operation is therefore lawful.

Furthermore, Article 5(d) of the Regulation provides that personal data may be processed only if *"the data subject has unambiguously given his or her consent"*. In the case in point, the data subject is free to undergo screening, and gives his or her consent in order to be able to do so.

The legal basis for the processing comes under Articles 59 and 78 of the Staff Regulations of Officials of the European Communities.

Article 59 provides: *"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. (...)"*.

Article 78 provides: *"An official shall be entitled, in the manner provided for in Articles 13 to 16 of Annex VIII, to an invalidity allowance in the case of total permanent invalidity preventing him from performing the duties corresponding to a post in his function group. (…) Where the invalidity arises from an accident in the course of or in connection with the performance of an official's duties, from an occupational disease, from a public-spirited act or from risking his life to save another human being, the invalidity allowance may not be less than 120% of the minimum subsistence figure. In such cases, moreover, contributions to the*

[5] Judgment of the Court of Justice of the European Communities of 6 November 2003, Lindqvist, C-101/01, ECR. p. I-0000.

pension scheme shall be paid in full from the budget of the institution or body referred to in Article 1b."

The legal basis is therefore correct.

In addition, data on health are described in Article 10 of Regulation (EC) No 45/2001 as "special categories of data".

3.3. Processing of special categories of data

Article 10 of the Regulation prohibits the processing of personal data concerning health, unless it can be justified on one of the grounds given in Article 10(2) and (3) of Regulation (EC) No 45/2001. The case under consideration very clearly relates to the processing of personal data concerning health.

Article 10(2)(b) applies in the case in point : *"Paragraph 1* (prohibiting the processing of data concerning health) *shall not apply where : (b) 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 Commission, in its capacity as employer, is complying with Article 10(2)(b) by processing the data submitted.

In addition, Article 10(2)(a) is also relevant to the case under consideration : *"Paragraph 1* (prohibiting the processing of data concerning health) *shall not apply where : (a) the data subject has given his or her express consent to the processing of those data (…)"*. As stated in point 3.2 of this opinion, the data subject has given his or her consent to the processing in question.

Lastly, Article 10(3) of the Regulation also applies here. It states : *"Paragraph 1* (prohibiting the processing of data concerning health) *shall not apply where processing of the data is required for the purposes 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"*. By definition, the doctors involved are under a duty of professional confidentiality. That provision further implies that there must be functional separation of these practitioners; this is the case, since the Medical Service is a functionally separate part of the Commission's Personnel Division (separate Medical Service). In this instance, Article 10(3) of the Regulation is duly complied with.

However, the EDPS points out that all the administrative departments responsible for processing files containing medical data with the framework of social medicine are themselves under a duty of professional confidentiality. The EDPS recommends that they be reminded of this fact.

3.4 Data quality

Data must be "*adequate, relevant and not excessive*" (Article 4(1)(c) of Regulation (EC) No 45/2001). The processed data described at the beginning of this opinion should be regarded as fulfilling these conditions in relation to the processing operation.

Even though medical records will always contain some standard data such as name, date of birth and personnel number, their precise content will of course vary from case to case.

However, there must be some guarantee that the principle of data quality is complied with, especially in the open field "comments". This could take the form of a general recommendation to the persons handling the records asking them to ensure that this rule is observed. Furthermore, great care must be taken during processing to ensure that unauthorised persons are not sent or given access to purely medical data.

Pursuant 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".*

The data in this case include doctors' notes and the results of medical examinations. It is not easy to ensure or assess the accuracy of data of this nature. However, the EDPS would emphasise that the institution must take every reasonable step to ensure that data are up to date and relevant. For example, to ensure that medical records are complete, any other medical opinions submitted by the data subject must also be kept in the file.

In this instance, Article 4(1)(d) of the Regulation is duly complied with. The data subject is made aware of his or her rights to access and rectify data in order to ensure that the file remains as comprehensive as possible. These rights are the second means of ensuring data quality. They are discussed in section 3.9 below.

Furthermore, the data must be *processed fairly and lawfully* (Article 4(1)(a) of Regulation (EC) No 45/2001). The matter of lawfulness has been reviewed above. Given the sensitivity of the subject, fairness warrants considerable attention. It is linked to the information to be given to the data subject (see section 3.10 below).

3.5 Data retention

Article 4(1)(e) of Regulation (EC) 45/2001 lays down the principle that 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 legal reference for this requirement is Directive 2004/37/EC[6]. For the record, in the case in point, personal data are kept for 40 years after the exposure to carcinogens or mutagens, this being the maximum period allowed. This period was considered necessary for the purposes of the processing operations under consideration[7]. The Regulation is therefore complied with.

3.7 Data transfer

Transfer of personal data within or between Community institutions or bodies

The processing operation should also be scrutinised in the light of Article 7(1) of Regulation (EC) No 45/2001. The processing covered by Article 7(1) is the transfer of personal

[6] Where there are no specific rules applicable to the Communities on a given area, in the field of health and safety at work the Commission applies those rules which offer its staff the greatest protection, in particular the Directive cited below, which, it should be noted, is designed to harmonise national legislation. Hence a number of processing operations carried out by the Medical Service are based on the relevant Directives. Application of these Directives is justified, inter alia, by the fact the European institutions are required to abide by the requirements they impose on the Member States

[7] See the EDPS's recommendations of 26 February 2007 in reply to the consultation by the Board of Heads of Administration.

data 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*".

The case in point concerns transfers within the same institution (the Sickness Insurance Office of the European Institutions). It also concerns transfers between institutions, since the personal data may also be transferred to the Legal Service, so that it can prepare a statement of defence in the event of proceedings before the Civil Service Tribunal; or to the Judges of the Civil Service Tribunal, at their request; or to the European Ombudsman, at his request.

Care should therefore be taken to ensure that the conditions of Article 7(1) are fulfilled; that is the case since the data transferred (or potentially transferred) are, in principle, necessary for the legitimate performance of tasks covered by the competence of the recipient. As regards these transfers, only relevant data must be transferred. Such transfers are therefore lawful insofar as the purpose is covered by the competences of the recipients. Article 7(1) is therefore duly complied with.

Article 7(3) of Regulation (EC) No 45/2001 provides that "*the recipient shall process the personal data only for the purposes for which they were transmitted*". There should be explicit assurance that any member of the Commission's Medical Service receiving and processing data may not use them for other purposes. Accordingly, the EDPS recommends that, in the case in point, the Commission should specify that the persons responsible for processing may not use those data for any other purpose. The same principle applies to any other recipients referred to. Furthermore, the EDPS recommends that when making transfers to other institutions, only persons authorised to access health data who are bound by professional confidentiality should receive medical records.

Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC

Furthermore, data may be transferred, at the data subject's request, to his or her regular doctor. If these doctors are established in countries whose national law was adopted pursuant to Directive 95/46/EC, the processing will come under Article 8 of Regulation (EC) No 45/2001 as regards the transfer of data. The same principle applies to the two outside lung specialists. The transfer is covered by Article 8(b), which stipulates that data may be transferred if "*the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.*"

The necessity of the transfer to the regular doctor is demonstrated by the fact that it is the data subject who requests it. As regards the two outside lung specialists, necessity is demonstrated by the need for a totally independent opinion on each dossier.

Transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to Directive 95/46/EC

Lastly, transfers to recipients who do not come within the scope of 95/46/EC (if these external doctors are established in a country with national legislation not based on Directive 95/46/EC) need to be examined in the light of Article 9 of Regulation No 45/2001. It states : "*1. Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out*".

If the country of the recipient does not ensure an adequate level of protection, the exceptions provided for in Article 9(6) and (7) of Regulation (EC) No 45/2001 may apply. In the case under examination, Article 9(6)(a) would be particularly relevant: "*By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if (...) (a) the data subject has given his or her consent unambiguously to the proposed transfer (...)*".

3.8 Processing including the personal or identifying number

The Commission uses personal numbers in the "Asbestos" database. While the use of an identifier is, in itself, no more than a means (and a legitimate one in this case) of making the controller's work easier, its effects may nevertheless be significant. This was why the European legislature decided to regulate the use of identifying numbers under Article 10(6) of the Regulation, which makes provision for action by the European Data Protection Supervisor. In the case in point, use of the personal number may allow the linkage of data processed in different contexts. Here, it is not a case of establishing the conditions under which the Commission may process the personal number, but rather of drawing attention to this point in the Regulation. In the case in point, it is reasonable for the Commission to use personal numbers because it makes the work of processing easier.

3.9 Right of access and of rectification

Article 13 of the Regulation establishes a right of access – and the detailed rules for its exercise – at the request of the data subject. Pursuant to Article 13 of the Regulation, the data subject has the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing processing and of any available information as to their source.

Article 20 of the Regulation places certain restrictions on this right, especially where such restriction is necessary to safeguard the protection of the data subject or of the rights and freedoms of others.

The EDPS wishes to point out that the rule laid down in the Regulation is intended to enable the data subject to have access to his or her personal data. Accordingly, no restrictions may be placed on this right, except under strict conditions.

In relation to point 3 of Conclusion 221/04 (personal notes by doctors), the restriction based on the "rights and freedoms of others" (others may not include the controller) refers to the fact that the rights and freedoms of an identified third person take precedence over the data subject's right of access. The EDPS welcomes the fact that this is subject to examination on a case-by-case basis in accordance with the principle of proportionality. This restriction should not result in a blanket refusal to allow access to doctors' personal notes in medical records.

Article 14 of Regulation (EC) No 45/2001 allows the data subject a right of rectification. In addition to being given access to their personal data, data subjects may also have that data amended if necessary. This right is somewhat limited as regards medical data, in that it is difficult to guarantee the accuracy or completeness of such data. It may, however, apply to other types of data contained in medical records (administrative data, for example). Furthermore, as mentioned above (under section 3.4 "Quality of data"), the data subject may request that his or her medical records in the "Asbestos" database be complete in the sense that he or she may request that information such as counter opinions by another doctor or a Commission decision on an aspect of the medical records be placed in his file so as to ensure it

contains up-to-date information. As a result, the EDPS feels that the reply to question 5 of the "Confidentiality declaration" should add this possibility.

3.10 Information to be given to the data subject

The Regulation (EC) 45/2001 provides that the data subject must be informed where his or her personal data are processed and lists a series of specific items of information that must be provided. In the present case, some of the data are collected directly from the data subject and other data from other persons.

Article 11 (*Information to be supplied where the data have been obtained from the data subject*) on the information to be given the data subject is applicable in this case, insofar as the official provides the information during medical check-ups.

Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) on the information to be given the data subject also applies in this case, since information may be obtained from the various parties involved in the process (for example, outside doctors).

For the record, data subjects are informed through the "Confidentiality declaration ".

For the processing to be fully compliant, Articles 11(f) and 12(f) should also be mentioned. The EDPS therefore recommends adding the legal basis for the processing.

The person concerned should also be informed of the potential recipients of the data. In this case, the controller should add a mention of transfers to external lung specialists and the possibility of transfer to the EDPS in the "Confidentiality declaration".

3.11 Security measures

Pursuant to Article 22 of Regulation (EC) No 45/2001 concerning security of processing, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected".*

The entire procedure is confidential. Ad hoc security measures are provided for with respect to consultation of the file by the data subject and retention of such files or with respect to guaranteeing the confidentiality of communications when information is transferred to and from the Medical Service. Article 22 of the Regulation is therefore duly complied with.

Conclusion:

The proposed processing does not appear to involve any infringement of the provisions of Regulation (EC) No 45/2001, provided that the above comments are taken into account. This means that the Commission must, in particular:

- remind all the administrative departments responsible for processing files containing medical data within the framework of social medicine that they are themselves under a duty of professional confidentiality,

- abide by the principle of data quality, especially in the open field « comments ». This could take the form of a general recommendation to the persons handling the records

asking them to ensure that this rule is observed. Furthermore, great care must be taken during processing to ensure that unauthorised persons are not sent or given access to purely medical data,

- specify that persons responsible for processing may not use these data for other purposes. The same principle applies to any other recipients mentioned. In addition, the EDPS recommends that where data are transferred to other institutions, only persons authorised to have access to data relating to health, who are subject to a duty of professional confidentiality, should receive medical records,

- not allow any blanket refusal of access to doctors' personal notes in the medical records,

- authorise the data subject to request that his or her medical records in the "Asbestos" database should be complete, i.e. to request that information such as counter opinions by another doctor or a Commission decision on an aspect of the medical record be placed in his/her file so as to ensure it contains up-to-date information. The EDPS therefore considers that the reply to question 5 of the "Confidentiality declaration" should add this possibility,

- add to the "Confidentiality declaration" the legal basis of the processing operation, the transfer to outside lung specialists and the possibility of transfer to the EDPS.

Done at Brussels, 27 July 2007.

(Signed)

Joaquín BAYO DELGADO
Assistant Supervisor