Opinion on a notification for prior checking received from the Data Protection Officer of the European Parliament concerning the "Administration of Accident Insurance"

Brussels, 30 April 2007 (Case 2006-303)

1. Procedure

Notification within the meaning of Article 27(3) of Regulation 45/2001, concerning the case *"Administration of Accident Insurance"*, was given by the Data Protection Officer (hereafter: DPO) of the European Parliament by letter on 19 June 2006.

The European Data Protection Supervisor (hereafter "the EDPS") identified certain priority topics and selected a number of processing operations subject to prior checking *ex-post* which required notification. The case *"Administration of Accident Insurance"* is one of them, and in particular one of the cases which reveal data relating to health (Article 27(2)(a)).

In connection with this notification, questions were put to the European Parliament's DPO by e-mail on 6 July 2006 and replies received on 28 November 2006. A further request for information was made on 21 December 2006, to which the DPO responded on 13 March 2007. Clarifications were requested on 15 March 2007 and replies given on 16 March 2007. Additional questions were sent on 19 March 2007 and replies received on 2 April 2007. The draft opinion was sent to the DPO on 13 April 2007 for comments; the DPO provided us with further information on 19 April 2007. The deadline was extended for clarifications on 20 April 2007, to which the DPO replied on 23 April 2007.

2. Facts

This dossier concerns processing carried out by the Social Insurance Service, and in particular by the Accidents Section, of DG Personnel at the European Parliament. The processing forms part of the administration of accident and occupational disease insurance for European Parliament officials, temporary staff, retired staff members (if the accident occurred while they were in active employment), and contract staff.

The processing in question is carried out in accordance with Article 73 of the Staff Regulations of officials of the European Communities (hereafter: "the Staff Regulations"), Article 28 of the Conditions of Employment of Other Servants (hereafter: "the CEOS") and the common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease which entered into force on 1 January 2006, agreement between the Institutions having been recorded by the President of the Court of Justice (hereafter: "the common rules on accident and occupational disease insurance").

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

Under Article 18 of the common rules on accident and occupational disease insurance, decisions recognising the accidental cause of an occurrence, and decisions linked thereto, recognising the occupational nature of a disease are taken by the appointing authority. The appointing authority notifies the data subject, or those entitled under him/her, of the draft decision and of the findings of the doctors appointed by the appointing authority. Within a period of sixty days, the data subject may request that the Medical Committee[1] deliver its opinion.

In addition, an insurance company is contracted with the European Parliament on the basis of a service contract concluded between the European Community, represented by the Commission, on behalf of the European Parliament and all the institutions, and the insurance company. This service contract applies in all European Union institutions[2]. Article 8.1 of the contract, entitled *data protection,* provides that *the personal data referred to in the contract shall be processed in accordance with Regulation (EC)No 45/2001 ... they may only be processed for the purposes of the performance, administration and monitoring of the contract by an entity appointed as data processing controller, without prejudice to their possible transmission to bodies charged with auditing or inspection functions under Community law. The policyholder has a right of access to and right to rectification in respect of personal data relating to him/her. For any question concerning these data, the policyholder shall contact the entity appointed as data processing controller. The policyholder has the right to have recourse at any time to the European Data Protection Supervisor.* Article II.9.1, concerning confidentiality, also provides that the insurance company *shall undertake to treat as strictly confidential all information and documents relating to the performance of the contract and not to make use of them or disclose them to third parties. The contractor shall continue to be bound by this undertaking after the tasks have been completed.* Where the insurance companies are concerned, a new agreement is being drawn up with a view to specifying administrative costs.

External doctors, if appointed by the appointing authority, received a notification of appointment. The sample notification of appointment received by the European Parliament's DPO was concluded between the European Parliament's Social Affairs Unit and a doctor resident in France. The appointment describes the nature of the contract (contract for the performance of services), the financial conditions and the rules governing meetings between the data subject and the doctor.

The data processed are as follows: data in the form of identification numbers (staff number combined with the accident number and case number provided by the insurers), data relating to the health, family and private sphere of the data subject (home address, personal mobile telephone number, vehicle registration number in the case of a traffic accident with a report drawn up by the police), remuneration, benefits and bank accounts, career, social security and pensions, medical treatment and expenses and full medical reports drawn up by the data subject's doctors and by the doctors appointed by the appointing authority. It is specified that data relating to bank accounts are required in the event that benefit is paid, that data relating to career and remuneration are required in order to calculate invalidity benefit or benefits to be paid in the event of death to those entitled under the insured party and that data relating to

---

[1] Article 22 of the common rules on accident and occupational disease insurance stipulates that the Medical Committee shall consist of three doctors, one appointed by the insured party or those entitled under him/her, one appointed by the appointing authority and one appointed by agreement between the first two doctors.

[2] Article I.1.1. of the contract stipulates that *"the object of the contract is insurance against the risks of accident, occupational disease and death from natural causes for officials, temporary staff and contract staff of the institutions of the European Union".*

medical expenses are required for the purposes of additional reimbursement in the case of an accident. The mobile telephone number and home telephone number are obtained only in the - very rare - case of urgent situations in which the administrator is unable to contact the insured party through the normal channels of communication (office telephone number and e-mail). These urgent situations occur, in particular, where, following an accident, the data subject is unable to travel, in cases where an accident is reported not by the data subject but by a family member, a colleague or another department (for instance the welfare department) or if data contained in important documents (for instance, a medical certificate) are inaccurate (wrong date).

Certain data are collected by ARPEGE, which is DG Personnel's database for administering the staff of the institution. The data collected by ARPEGE are person-specific data, data relating to the administrative position of the data subject, data relating to the data subject's career and data relating to family members, family relationships and allowances. The person-specific data are: surname, first name, staff number, sex, address for correspondence and language for correspondence. It is specified that for reasons of confidentiality the Accidents Unit sends correspondence not to the office address but to the data subject's home. In the case of common surnames, ARPEGE is a means of carrying out checks to ensure that a file is not opened on the wrong person. As regards data relating to the data subject's administrative position (in active employment, early retirement, termination of service, leave on personal grounds, transfer to another institution, place of employment), it is stated that occasionally even individuals who are not covered by accident insurance, for instance retired persons or individuals who have had an accident during leave on personal grounds but have not been contributing, submit an accident report. In that case, ARPEGE enables these irregularities to be detected. In addition, in cases where the data subject is transferred to another institution, insured parties may send their accident reports to the wrong institution. ARPEGE serves as a means of carrying out checks in this respect. Data relating to the data subject's career are collected only in case of need, in order to calculate a benefit based on the individual's salary. As for data relating to the data subject's family, in the event of the death from natural causes of a person in receipt of the household allowance, the Social Insurance Service has to pay benefits to family members.

Processing is partly automated. Manual processing is carried out within a structured set of data accessible according to criteria determined in conformity with Article 2(c) of the Regulation. In particular, the data subject sends the accident report and all relevant documentary medical evidence (magnetic resonance imaging - MRI -, test results etc.), as it becomes available, to the administrators in the Accidents Section. The completed forms are printed and the paper forms are inserted in each data subject's accident file. While the file remains open, the paper forms are scanned.

It is important to note that an accident file is compiled and archived by the Accidents Section of the Social Affairs Unit pursuant to Article 73 of the Staff Regulations and the common rules on accident and occupational disease insurance. The purpose of this file is to ensure 100 % reimbursement of all expenses resulting from an accident until the consequences of the accident have consolidated, to enable the degree of permanent invalidity to be defined and a benefit to be paid, and, lastly, to enable the case to be re-opened, and further 100 % reimbursements made, if the insured party's condition has become aggravated.

The accident file comprises

- the accident report,
- all administrative correspondence with
    - ✓ the data subject,

    - ✓ the insurers,
    - ✓ the service which deals with absences for medical reasons,
    - ✓ in the case of a workplace accident, the Prevention and Well-Being at Work Unit,
- any reports drawn up following an enquiry which have been forwarded to the police,
- the draft decision,
- the insured party's response to the draft
- the appointing authority's decision
- medical documentation:
    - ✓ medical certificates,
    - ✓ prescriptions for medical treatment and tests following the accident,
    - ✓ medical reports by the general practitioner and external doctors appointed by the appointing authority and, if applicable, medical reports by the Medical Committee and experts consulted.

Each accident file therefore includes a medical element.

It is specified that the appointing authority's decision relates to the data subject's health: it indicates whether or not the event which occurred on nn/nn/200. was due to an accident, it defines the official's degree of permanent invalidity, and if applicable his/her degree of physical disfigurement and of impairment of social relationships, it indicates the forms of treatment which will continue to be reimbursed under Article 73 and specifies the amount of any benefits to be paid.

As regards correspondence between the Accidents Section and the insurance company, the procedure is as follows: the Accidents Section notifies the insurance company that a file has been opened and sends it the accident report and medical certificate. The Accidents Section sends the successive medical certificates to the insurance company, notifies it of the request for consolidation of the data subject's accident, of the data subject's being called to attend a consultation by the external doctor appointed by the appointing authority, of the appointing authority's draft decision under Article 73 of the Staff Regulations and of the data subject's agreement or disagreement and request for referral to a Medical Committee. Lastly, the Medical Committee's report, if applicable, and the appointing authority's final decision are sent to the insurance company by the Accidents Section.

As for the recipients of the data, the accident report is forwarded to the doctors appointed by the appointing authority involved in the various stages of the procedure for administering accident insurance, so that they can issue their report. The doctors in question are external doctors specialising in bodily injury. The accident report and medical certificates are then forwarded to the European Parliament's Social Insurance Service and to the insurance company contracted with the European Parliament. The Medical Committee provided for in Article 22 of the common rules on accident and occupational disease insurance is a possible recipient, if the data subject so requests. Other recipients are also specified, inter alia the Well-Being at Work Unit which receives the accident report in the case of workplace accidents and the service which deals with absences for medical reasons, to which the accident report, the initial medical certificate and certificates covering absence from work are forwarded, the office responsible for settling claims, which receives the accident report, and the other institutions in the event that the data subject is transferred before the file is closed or an application is made for the file to be re-opened because the data subject's condition has become aggravated.

As for the right of access, the data subject can access all the documents in his/her file in the offices of the Accidents Section, in the presence of an official of the Section. If the data subject so requests, a copy of his/her file is given to him/her. As for administrative correspondence between the Accidents Section and the insurance company, a data subject wishing to gain access to this correspondence has to submit a request and will then be supplied with a copy. In accordance with the common rules on accident and occupational disease insurance, the draft decision and then the appointing authority's decision are forwarded to the data subject together with the report by the appointing authority's doctor on which the decision is based and, in the event of referral to the Medical Committee, the Committee's report. If the external doctor's or Medical Committee's report includes a psychiatric/psychological report, the data subject is notified and asked to name the general practitioner to whom the report should be addressed so that he can take note of it as appropriate.

The data subject may add to his/her accident file any medical document which s/he considers necessary.

As regards the right to information, it is specified that an information clause is to be added to the first communication sent to the data subject.

Data are retained throughout the lifetime of the data subject in case s/he submits an application for the file to be re-opened because his/her condition has become aggravated, as the data subject is entitled to do under Article 21 of the common rules on accident and occupational disease insurance. According to the European Parliament, this timescale is necessary because the consequences of an accident can unfold slowly over time - for instance, it can take years for an official to recover from an accident. It is also specified that files must be retained until after the termination of service, and the death, of the official since an aggravation of his/her condition can be cited by the former official or by the persons entitled under him/her, provided that the accident occurred when the official was in active employment. An accident file can be re-opened on grounds of aggravation 15 or 20 years later and every data subject is entitled to request that a file be re-opened, even if, following a medical examination, his/her application is refused. The department cannot decide, a priori, that the file will never be re-opened and deprive an official of the right to have the case re-opened or impede the exercise of that right.

Decisions adopted by the appointing authority are kept by the Accidents Section in the accident file rather than the personal file. If the data subject makes a formal request for the appointing authority's decision to be kept in his/her personal file, the decision will be placed in that file together with his/her request.

The file will be eliminated when files relating to deceased persons are being scanned, if it appears that there is no longer any possibility of its being re-opened. Except for certain occupational disease files (mesotheliomas attributable to exposure to asbestos, in particular), no provision is made for subsequent processing for historical, statistical or scientific purposes.

Security measures have been adopted. Access to the network is password-protected and reserved exclusively for administrators in the Accidents Section. Data are filed in locked filing cabinets. The accident file can only be accessed by staff of the Accidents Section. The medical element of the accident file cannot be accessed by the European Parliament's Medical Service, except through the data subject him/herself. It should also be noted that the data subject's medical file cannot be accessed by the Accidents Section or by external doctors appointed by the appointing authority.

3. Legal aspects

3.1 Prior checking

Regulation 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 the processing of data by the European Parliament, i.e. a Community institution, and a processing operation within the framework of first pillar activities and hence the scope of Community law.

The processing operation in question here, which forms part of the administration of accident insurance, is both manual and automated, since the data processed are contained in a file. The processing operation also forms part of a filing system or is intended to form part of a filing system (Article 3(2) of the Regulation). Article 3(2) therefore applies in this case.

Consequently, this processing operation falls within the scope of Regulation (EC) 45/2001.

Pursuant to Article 27(1) of Regulation 45/2001, "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" are subject to prior checking by the European Data Protection Supervisor.

According to Article 27(2)(a), "the following processing operations are likely to present such risks: processing of data relating to health [...]", which applies in this case, since the data indisputably fall within the category of "data relating to health".

In principle, checks by the European Data Protection Supervisor should be performed before the processing operation is carried out. 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 facto. This does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented. However, the check should be regarded as a genuine prior check as regards aspects relating to the follow-up database being set up.

The EDPS received the notification from the DPO by mail on 19 June 2006. Under 27(4), this opinion must be delivered within two months, in this case no later than 20 August 2006. Questions were put to the European Parliament's DPO by e-mail on 6 July 2006 and replies received on 28 November 2006. A further request for information was made on 21 December 2006, to which the DPO responded on 13 March 2007. Clarifications were requested on 15 March 2007 and replies given on 16 March 2007. Additional questions were sent on 19 March 2007 and replies received on 2 April 2007. On 13 April 2007 the procedure was suspended for 7 days pending comments. On 20 April the procedure was suspended again, since further information has been supplied and clarifications have been requested. Owing to the 227 (157+116+1+17+7+3) days of suspension, the EDPS will deliver his opinion by 30 April 2007 (19 June plus 301 days' suspension), as stipulated in Article 27 (4) of the Regulation.

3.2 Legal basis and lawfulness of processing

Lawfulness of processing must be assessed in the light of Article 5(a) of Regulation 45/2001 which requires that *"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 or in the legitimate exercise of official*

authority vested in the Community institution". Recital 27 of the Regulation also specifies that "*processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies*".

In this case, the European Parliament needs to adopt appropriate measures to ensure that the financial costs of an official's or staff member's accident or occupational disease are covered by an insurance company. The Parliament is therefore contracted with the insurance company in question in the context of its task carried out in the public interest and in the context of an operational necessity. The proposed processing operation is consequently lawful.

The legal basis for this processing operation is to be found in Article 73 of the Staff Regulations, Article 28 of the Conditions of Employment of Other Servants, the common rules on accident and occupational disease insurance and the provisions of the contract.

Article 73 of the Staff Regulations stipulates, in particular, that *"an official is insured, from the date of his entering the service, against the risk of occupational disease and of accident subject to rules drawn up by common agreement of the institutions of the Communities after consulting the Staff Regulations Committee*".
As for temporary staff, Article 28 of the Conditions of Employment of Other Servants stipulates that Article 73 of Staff Regulations shall apply by analogy. In the case of contract staff, if they are insured, Chapter 8, entitled "social security benefits", stipulates that Article 28 shall apply by analogy.

The common rules on accident and occupational disease insurance also lay down, in accordance with Article 73 of the Staff Regulations, the rules according to which the insured party is covered, worldwide, against the risks of accident and occupational disease.
Article I.1.1 of the contract specifies that the object of the service contract between the European Parliament and the insurance company is insurance against the risks of accident, occupational disease and death from natural causes of officials, temporary staff and contract staff of the institutions of the European Union. Article 73 of the Staff Regulations indeed obliges the European Communities to insure their staff against the risks of an accident or occupational disease. Moroever, in the light of the principle of good administration, it is strongly recommended that the European Communities cover their staff against these risks via an insurance contract with an external organisation.

The legal basis is consequently valid and supports the lawfulness of the processing.

3.3 Processing of special categories of data

Article 10 of Regulation 45/2001 stipulates that the processing of personal data concerning health is prohibited, unless it is justified on the grounds referred to in Article 10(2) or (3) of the Regulation.

This case involves the processing of personal data concerning health, since the administration of accident and occupational disease insurance reveals information on the data subject's state of health.

In this case, the processing of medical data is justified since it is necessary for the purpose of complying with the European Parliament's specific rights and obligations in the field of employment law, as stipulated in Article 10(2)(b).

Data concerning health are collected by administrators in the Accidents Section who also receive medical reports, along with the "Well-Being at Work" Unit, the service which deals with absences for medical reasons and the office responsible for settling claims. Medical data are also transferred to the doctors appointed by the appointing authority to enable them to issue their report and the report is forwarded to the insurers for their opinion. If applicable, an opinion is also required from the Medical Committee, and psychological reports may be transferred to the general practitioner. That is why Article 10(3) of Regulation 45/2001, concerning special categories of data, applies in this case. It stipulates that: *"Paragraph 1* (prohibiting the processing of personal 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."*.

As regards doctors appointed by the appointing authority and, where applicable, the Medical Committee and the general practitioner, in view of their functions they are subject to the obligation of professional secrecy. Article 10(3) of the Regulation is therefore complied with.

Administrators in the Accidents Section and the other recipients referred to above are not health professionals. The EDPS therefore recommends that these individuals be reminded that they are subject to an equivalent obligation of professional secrecy, to ensure compliance with Article 10(3) of the Regulation.

As for the insurers, the EDPS recommends that it be explicitly stated, in Article II.9 of the service contract between the European Parliament and the insurance company, that the insurers subscribe to an equivalent obligation of secrecy in accordance with Article 10(3) of the Regulation.

3.4. The controller and the processor

Under Article 2(d) of the Regulation, the controller is the "*Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data*". The controller is responsible for ensuring compliance with the obligations laid down by the Regulation (provision of information to the data subject, protecting the rights of the data subject, the choice of processor, notification of the data protection officer, etc.). The processor is the "*natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*" (Article 2(e)).

In this case, the European Parliament is contracted with the insurance company via a service contract. The Parliament is also bound by a notification of appointment issued to the external doctors appointed by the appointing authority.

The European Parliament is considered to be the controller since it determines the purposes and means of collecting data relating to the data subjects in accordance with the contract.[3] The insurance company is a processor, since - on the basis of the service contract concluded - it processes the data subjects' medical data collected on behalf of the Parliament in that it

[3] Article I.8 of the contract also specifies that data may be processed only for the purposes of the performance, administration and follow-up of the contract by the European Parliament as controller and that the insurance company should consult the Parliament on all questions concerning the right of access and rectification.

determines the amounts to be reimbursed on the basis of medical reports, provided that the collection and subsequent processing of the data are necessary to comply with the Parliament's specific obligations and rights in the field of employment law as laid down in Article 10(2)(b) of the Regulation. External doctors are also considered as processors, since they process medical data on behalf of the Parliament in that they issue medical reports to the Parliament's Social Insurance Service so that the amounts to be reimbursed can be estimated by the insurance company.

3.5 Data quality

Article 4(1)(c) of the Regulation provides that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Even though European Parliament officials' or staff members' files will always contain certain standard data, such as administrative data relating to the data subject's private sphere, the precise content of a file relating to health will obviously vary according to the case. However, there must be some guarantee that the principle of data quality is complied with. This could take the form of a general recommendation addressed to the persons handling the files, asking them to ensure that this rule is observed.

With regard to the administrative data described in point 2, the question which arises is whether all these data collected by the Parliament's Social Insurance Service are relevant to the purposes for which they are collected. Having examined the reasons given by the DPO, as set out in point 2 of this opinion, the EDPS considers that these data are required for the purposes of the processing operations in question and are not excessive, given that some of these data are not collected systematically but only in certain cases.

The sole purpose of the data relating to health and of the full medical reports drawn up by the doctors must be to enable insurance against the risk of accident and occupational disease to be administered. This is important, firstly, because the doctors must submit their report to the insurers in order for the insurers to prepare reports concerning reimbursements relating to an accident or occupational disease under the provisions of the service contract. This enables reimbursements to be ensured in accordance with the purpose of the processing operation in this case and as provided for in Article 73 of the Staff Regulations.

The data transmitted to the insurance company are the accident report and medical reports. These data, both administrative and medical, would seem to be required to enable the insurance company to exercise all the rights and obligations deriving from the contract. The common principles of the law of contract which can be derived from general European practice include the right for the insurance company to obtain sufficient information about the accident or occupational disease to be able to exercise all the rights and actions provided for in the contract. This follows from the principle of the appropriate defence of one's rights. Moreover, in this case, it is important that all elements relating to an accident or occupational disease be taken into consideration so that the insurance company's reports are as full and as precise as possible.

The EDPS therefore considers that Article 4(1)(c) of the Regulation is complied with.

Data must also be *"processed fairly and lawfully"* (Article 4(1)(a)). Lawfulness of processing has already been considered in point 2 of this opinion. As for fairness, it is related to the information which must be supplied to the data subject (see point 3.11 below).

Article 4(1)(d) of the Regulation provides that the data must be *"accurate and, where necessary, kept up to date*". In addition, according to this article, "*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 question in this case are, on the one hand, administrative data (data relating to the private sphere, benefits, social security etc.) and, on the other hand, medical data, i.e. medical certificates issued following the accident, medical reports drawn up by doctors appointed by the appointing authority, reports by the experts consulted, and - if applicable - the opinion of the Medical Committee.

As regards medical data, it is not easy to ensure, or assess, their accuracy. Nonetheless, the EDPS wishes to emphasise the need to take all reasonable measures to ensure that up-to-date and relevant data are available. The EDPS recommends that doctors' reports be filed separately from those containing administrative data and that all data relating to health be kept up to date by European Parliament administrators who must be subject to an equivalent obligation of professional secrecy.

The data subject's rights of access and rectification constitute the second means of ensuring that data relating to him/her are accurate and up-to-date (see 3.10, right of access).

3.6 Data retention

The general principle laid down in Regulation 45/2001 is 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"*. (Article 4(1)(e) of the Regulation).

It may be recalled that data are retained throughout the lifetime of the data subject in case the data subject applies for the case to be re-opened because his/her condition has become aggravated, as s/he is entitled to do under the common rules. According to the Parliament, this timescale is necessary because the consequences of an accident can unfold slowly over time - for instance, it can take years for an official to recover from an accident. It is specified that an accident file can be re-opened on grounds of aggravation 15 or 20 years later, and every insured party is entitled to request that a file be re-opened, even if, following a medical examination, his/her application is refused. The department cannot decide, a priori, that the file will never be re-opened and deprive an official of the right to have the file re-opened or impede the exercise of that right.

It should be emphasised that in the case of medical reports relating to occupational diseases, the possibility of data being stored for more than 30 years was raised in a note from the Board of Heads of Administration on 4 October 2006 concerning time-limits for storing data. In his opinion on the conservation of medical documents, the EDPS emphasised that the conservation for more than 30 years of medical documents acquired under Article 73 of the Staff Regulations was to be regarded as justified[4].

[4] Opinion of the EDPS of 26 February 2007 on conservation periods for medical documents, page 2.

The EDPS therefore considers that the period for which data are retained in this case, that is throughout the lifetime of the data subject, under Article 73 of the Staff Regulations, is justified. It is also explicitly stated in Article 21 of the common rules on accident and occupational disease insurance that, with regard to aggravation and cases which have been terminated, insured parties may at any time apply for the case to be re-opened.

It is also important to note that long-term data retention must be accompanied by appropriate guarantees. Appropriate measures must be taken for the transmission and storage of these data, like all sensitive data.

It is stated that except for certain occupational disease files (in particular, mesotheliomas attributable to exposure to asbestos), no provision is made for subsequent processing for historical, statistical or scientific purposes. The EDPS therefore recommends that data be rendered anonymous in accordance with Article 4(1)(e) of the Regulation.

3.7 Change of purpose/compatible use

Some data are taken from the ARPEGE database. The processing operation under consideration does not entail a general change in the intended purpose and is not incompatible with that purpose, since ARPEGE is a tool of the staff of the a Management Unit. Consequently, Article 6(1) of the Regulation does not apply in this case, and Article 4(1)(b) of the Regulation is complied with.

3.8 Transfer of data

Article 7(1) of the Regulation provides that personal data may only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimite performance of tasks covered by the competence of the recipient.

Firstly, this case involves transfers within a single institution, since the medical service, the service which deals with absences for medical reasons, the Well-Being at Work Unit and the Medical Committee are departments within the European Parliament. Data can also be transferred to other institutions - to the office responsible for settling claims at the Commission and to other institutions if the data subject is transferred. The transfer consequently complies with Article 7(1), since the data collected are required in order to carry out the processing operation and are also "*necessary for the legitimite performance of tasks covered by the competence of the recipient*".

Article 7(3) of Regulation (EC) 45/2001 provides that "*the recipient shall process the personal data only for the purposes for which they were transmitted*". The EDPS recommends that recipients in the European Parliament and other institutions be reminded that they should process data only for the purposes for which they were transmitted.

Since the doctors appointed by the appointing authority are external (according to the specimen notification of appointment, the independent doctor engaged under a services contract is resident in France) and the insurance company is an external entity governed by Belgian law, the recipients in question are subject to national - French and Belgian - legislation adopted pursuant to Directive 95/46/EC. The processing operations will therefore be examined in the light of Article 8 of Regulation 45/2001 with reference to these data transfers. In this case, the transfer will be covered by Article 8(b) which provides 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 interest might be prejudiced*". The necessity of transferring the

data to the two recipients (external doctors and the insurance company) is justified, respectively, by the contract and by the notification of appointment by which the European Parliament is bound. Since the principle of data quality is complied with (see the analysis in point 3.5), the transfer will not prejudice the legitimate interests of data subjects. It is recommended, however, that external recipients be reminded that they may only use data strictly for the limited purpose of performing their contract and their notification of appointment, respectively.

In cases where the external doctor's or Medical Committee's report includes a psychiatric/psychological report and the data subject is informed of this and asked to give the name of the general practitioner to whom this report is to be sent, Article 8(b) of Regulation 45/2001 applies, assuming that the doctors are recipients governed by national legislation adopted pursuant to Directive 95/46/EC. Since the general practitioner monitors the data subject's file and is subject to professional secrecy by virtue of his functions, the transfer of the psychiatric/psychological reports will not prejudice the legitimate interests of data subjects.

3.9 Processing including the staff number or identifying number

Article 10(6) of the Regulation provides that "*The European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*".

A staff number is collected and processed in connection with the administration of accident and occupational disease insurance and Article 10(6) should therefore be applied. The use of an identifying number is, in itself, only a means - a legitimate one, in this case - of facilitating the work of the controller of personal data; it can, however, have significant consequences. It was indeed for this reason that the European legislator laid down a framework for the use of identifying numbers in Article 10(6) of the Regulation, which provides for the intervention of the EDPS. The aim here is not to define the conditions under which the European Parliament may process an identifying number but to emphasise that attention must be paid to this point in the Regulation. In this case, the use by the Parliament of a staff number is reasonable since it is a means of facilitating the processing - specifically, in the procedure for reimbursements.

3.10 Right of access and rectification

Under Article 13 of Regulation (CE) 45/2001, concerning the right of access, data subjects have the right to obtain confirmation as to whether or not data relating to them are being processed; information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and communication in an intelligible form of the data undergoing processing and of any available information as to their source.

Article 14 of Regulation (EC) 45/2001 lays down a right of rectification for the data subject. Just as the data subject has a right of access, s/he may also have his/her personal data amended if necessary.

It should be noted that data subjects can have very extensive access to their accident file and can at any time add a new document or medical report to the file.

The EDPS is consequently pleased to note that the obligations laid down in Articles 13 and 14 of Regulation 45/2001 are being complied with.

.

3.11 Information to be given to the data subject

Articles 11 and 12 of Regulation 45/2001 specify the information to be supplied to the data subject to ensure that his/her personal data are processed in a transparent manner. These articles list a series of items of information, mandatory and optional. The latter apply insofar as they are necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. In this case, some of the data are collected directly from the data subject while other data are collected from other persons.

The provisions of Article 11 (*Information to be supplied where the data have been obtained from the data subject*) on information to be provided to the data subject apply in this case insofar as data subjects themselves supply administrative information and information concerning their accident or occupational disease.

The provisions of Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) on information to be provided to the data subject also apply in this case, since data are collected, via ARPEGE, from external doctors and from insurers.

It is stated that information clauses are to be included in the first communication sent to data subjects.

The EDPS therefore recommends that all the information specified in Articles 11 and 12 of Regulation 45/2001, both mandatory and optional, since the latter ensures fair processing and does not entail any additional effort for the controller, be referred to in an internal memorandum or statement, for forthcoming communications to data subjects.

3.12 Processing by a processor

Where a processing operation is carried out on behalf of a controller, Article 23 of Regulation 45/2001 stipulates that the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by the Regulation. The carrying out of a processing operation by way of a controller must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the confidentiality and security obligations with regard to the processing of personal data shall also be incumbent on the processor.

It should be pointed out that the service contract concluded by the Commission, on behalf of the European Parliament and all the institutions, and the insurance company, includes provisions concerning data protection (Article I.8) and confidentiality (Article II.9).

However, Article I.8 is confined to data "*referred to in the contract*", which is not sufficient as regards data transferred as a consequence of the performance of the contract. Article II.9 is also inadequate since there is no reference to security measures. Nor does the notification of appointment concluded between the European Parliament and external doctors make provision for security measures. The EDPS considers, therefore, that the provision relating to data protection (Article I.8 of the contract) must be reworded to refer to data which are transferred and processed as part of the processing operations concerned. It is also essential that both Article II.9 of the contract and the notification of appointment contain a reference to the level of security adopted in accordance with Article 23(2)(b) of the Regulation. Since both

processors (the insurance company and the external doctors) are governed by national law (Belgian and French, respectively - Member States' legislation), it is necessary, in particular, for both processors to be subject to the obligations in respect of security laid down in national legislation pursuant to the second indent of Article 17(3) of Directive 95/46 EC.

3.13 Security

Under Article 22 of Regulation No 45/2001, the controller is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must, in particular, prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and all other unlawful forms of processing.

Having carried out a thorough review of the security measures adopted, the EDPS considers that they are appropriate, having regard to Article 22 of Regulation (EC) No 45/2001.

Conclusion

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

- ensure that Parliament administrators are bound by an equivalent obligation of secrecy and that it is explicitly stated in Article II.9 of the service contract between the European Parliament and the insurance company that the insurers are bound by an equivalent obligation of secrecy in accordance with Article 10(3) of the Regulation,

- establish that the principle of data quality is complied with in respect of all data relating to health. These guarantees could take the form of a general recommendation addressed to persons processing data, asking them to ensure that this rule is complied with,

- guarantee that doctors' reports are filed separately from those containing administrative data and that all data relating to health are kept up to date by Parliament administrators who must be subject to an equivalent obligation of professional secrecy,

- ensure that long-term data retention is accompanied by appropriate guarantees. In cases where certain occupational disease files are kept for historical purposes, the data must be rendered anonymous,

- remind recipients in the Parliament, and other institutions, to process data only for the purposes for which they were transmitted and remind external recipients to use data strictly for the limited purpose of performing the insurance contract,

- specify all the information, both mandatory and optional, referred to in Articles 11 and 12 of Regulation No 45/2001, in an internal memorandum or statement to be addressed to data subject for forthcoming communications,

- ensure that the provision concerning data protection (Article I.8 of the service contract) is reworded to refer to data transferred and processed in the course of the processing operations in question. It is also essential that both Article II.9 of the contract and the notification of appointment contain a reference to the level of security laid down in national legislation.

Done at Brussels, 30 April 2007

Peter HUSTINX
European Data Protection Supervisor