Opinion on a notification for prior checking received from the Data Protection Officer of the Commission related to Administration of the Accidents and Occupational Disease Insurance

Brussels, 27 July 2007 (Case 2007-157)

1. Proceedings

On 9 March 2007, the European Data Protection Supervisor (hereinafter "EDPS") received from the Data Protection Officer of the Commission a notification for prior checking regarding the data processing operations carried out in connection with the management of the Accidents and Occupational Disease Insurance (hereinafter "the Notification"). The data processing operations carried out in connection with the management of the Accidents and Occupational Disease Insurance ("Accidents and Occupational Disease Insurance") as described in the Notification are performed by the Office for the Administration and Payment of Individual Entitlements (hereinafter "PMO").

The EDPS requested complementary information on 17 April 2007. The information was provided on 25 May 2007. A meeting between PMO staff and the EDPS staff took place on 4 June 2007 to confirm factual information and clarify various aspects related to the functioning of the Accidents and Occupational Disease Insurance. On 14 June 2007 the EDPS sent the draft prior check Opinion to the PMO for comments. PMO staff and the EDPS staff met again on 10 July 2007. During the meeting PMO staff gave their oral comments to the EDPS on the draft Opinion which were reflected in the paper version of the draft Opinion on 24 July 2007.

2. Examination of the matter

2.1 The facts

The Accidents and Occupational Disease Insurance Scheme was established pursuant to various provisions of the Staff Regulations and the Conditions of employment of other servants of the European Communities[1]. According to these provisions, officials, temporary and contractual agents of EU institutions ("EU staff members")[2] are covered against accidents

[1] The provisions that set forth the Accidents and Occupational Disease Insurance are Article 73 of the Staff Regulations, Article 25 of the Annex X of the Staff Regulation and Article 28 of the Conditions of employment of other servants of the European Communities. These provisions have been developed in the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease Section 2.2.2 further develops this point.

[2] In certain cases, spouses/partners children and dependent may also be covered by the insurance ("insured parties). In this Opinion we will use the term to "EU staff members" to refer to members, officials, temporary and contractual agents who are entitled to accidents and occupational disease insurance under Article 73 and 28 referred under footnote 1. We will refer to "insured parties" to include also spouses/partners, children and assimilated dependents. References will be made to EU staff members or insured parties, as appropriate.

and occupational diseases. In particular, the insurance covers the payment of benefits in the event of death, total, permanent or partial invalidity. It also foresees a complementary reimbursement of all related medical expenses. The Communities have concluded a reinsurance contract with two insurance companies by virtue of which the Communities are insured against the risk incurred as a result of the Application of Article 73, i.e. which sets forth their obligation to act as insurers for EU staff members against accidents and occupational diseases.

The Sickness and Accidents Insurance Unit which is the Unit 3 within the PMO (hereinafter "PMO 3.") is responsible, among others, for the management of the Accidents and Occupational Disease Insurance in order to guarantee the payment of the benefits and medical expenses to EU staff members.

Insured parties who have suffered an accident or an occupational disease are asked to submit to PMO. 3 the accident report and/or request for recognition of occupational diseases, accompanied by the appropriate medical reports. An electronic data file will be created for each accident report and each request for recognition of occupational disease. The data file is progressively completed. Among others, it will contain all additional medical reports sent by the victim, the various reports of the doctor designated by the Appointing Authority, and the final decisions taken by the Appointing Authority regarding the recognition of the event under the legal provisions and the recognition of an eventual disability percentage. The dossier will also contain copies of the correspondence between the PMO 3 staff and the insurance company, which has to be kept informed of the procedure in order to execute the various payments.

Whereas PMO 3 is competent for the management of the Insurance Scheme, the final decision on whether the accidental cause of an occurrence is attributed to a occupational or non occupational risk and the decisions regarding the occupational nature of a disease are taken by the Appointing Authority, on the basis of reports carried out by external doctors designated by the Authority.

The ***overall purpose*** of the processing is to administer the Accidents and Occupational Insurance to ensure the payment of benefits and reimbursement of all related medical expenses to which EU staff members are entitled.

The ***primary responsibility*** for the data processing lies within the Sickness and Insurance Unit (PMO 3). Most of the data processing operations carried out within the scope of the administration of the Accidents and Occupational Diseases Insurance are performed by the section 3.001 competent for accidents and occupational diseases. However, some of the processing, mostly of manual nature, is carried out by the external doctors designated by the Appointing Authority.

As further described below, the manual and automated data processing operations that take place in the context of the administration of the Insurance Scheme are closely interrelated. Whereas some data processing operations such as the initial collection of information are manual and paper based, this information is invariably introduced in a software database. The list of manual and electronic data processing operations can be summarised as follows:

- The Accidents and Occupational Diseases Section (PMO. 3.001) *receives* the following two types of documents related to the Insurance Scheme: *(i)* an accident report which is a standardised report to be accompanied by medical documents (such as reports on X rays

or hospitalisation) and, *(ii)* a written application requesting the recognition of an occupational disease to be accompanied by a medical report.

- Upon receipt of this information, these documents are *scanned*. Information provided to support each report, including the medical report regarding the occupational disease and the medical certificate are also scanned. The scanned document is entered in a software database referred to as ASSMAL.
- Staff from the Accidents and Occupational Diseases Section (PMO. 3.001) *notifies* the insurance company regarding each accident and occupational diseases report.
- Staff from the Accidents and Occupational Diseases Section (PMO. 3.001) *gives the original* paper copies of *all* the information to the external doctor designated by the Appointing Authority for his/her review.
- The individual is *notified* and requested to undergo an examination with the external doctor designated by the Appointing Authority.
- The external doctor will *draft a report* after a consultation with the individual, which will be sent to the PMO 3.001 to be inserted in his/her file.
- If the dossier refers to an occupational disease, Staff from the Accidents and Occupational Diseases Section (PMO. 3.001) carries out an administrative inquiry to determine the nature of the disease, whether it resulted from the insured party occupation; the intervention of IDOC[3] will be sought in certain cases, particularly in order to determine whether the disease is linked or the result of harassment. At the end of the enquiry, staff from the Accidents and Occupational Diseases Section (PMO. 3.001) will draft a report on the administrative inquiry which will be entered in ASSMAL.
- Finally, the Appointing Authority will issue a final decision that will be communicated to the member[4].

Once the Staff of the Accidents and Occupational Diseases Section (PMO. 3.001) has entered the information into ASSMAL, access to the information is on a need-to-know basis.

The ***types of data subjects*** whose data is collected in the context of the Accidents and Occupational diseases Insurance include the following: *(i)* members and officials of the EU institutions and agencies; *(ii)* temporary and contractual staff of the EU institutions and agencies[5].

In addition to the above, other data subjects whose information is also processed include the names of external doctors, for example those who sign the accident reports as well as the external doctors designated by the Appointing Authority in the context of their tasks.

The ***categories of personal data*** collected include the following: *(i)* data intended to identify EU staff members: staff member number, institution for which he/she works, office address and home address if retired, date of birth, type of beneficiary (whether member, dependent children and equivalent or spouse); *(ii)* bank account information where payments must be made, *(iii)* salary information; and *(iv)* information related to insured parties' health (type of injury, type of occupational disease/ medical reports, proposed treatments etc).

[3] IDOC is the investigatory and Disciplinary Office established by Commission Decision C(2004 1588 of 28 April 2004. Its functions include carrying out administrative inquiries under Articles 24, 73 and 90 of the Staff Regulation.

[4] The data processing actions may vary depending on the circumstances. For example, as foreseen in the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease, insured parties may request the Medical Committee to be consulted. Obviously, this would entail the transfer of the information to such Committee for the analysis of the subject matter.

[5] In addition, in certain cases data from spouses/unmarried partners, children and persons treated as a dependent child of officials/temporary staff/contract staff of the EU institutions serving in third countries may also be processed.

As far as ***conservation of data*** *is concerned*, paper based files are stored in the archives of the Accidents and Occupational Diseases Section and in the Commission archives for a period of five years after the death of the insured party. Electronic files are stored in the software database ASSMAL, which is hosted in Luxembourg for the same length of time.

The data controller PMO 3 may ***transfer personal data*** gathered in the context of the Administration of the Accidents and Occupational diseases Insurance to the following types of recipients:

To ***Community institutions***, namely *(i)* to DG BUDGET who will make the payment of amounts related to medical expenses via the members' bank account[6]. *(ii)* to IDOC in the context of harassment cases. In addition, *(iii)* data may be transferred to DG ADM B2 (referred to as the Appeals Unit), in the context of Appeals carried out under Article 90.1 and 90.2 of the Staff Regulations. Whether a particular category of data will be transferred depends on the recipient. For example, the only information that is transferred to IDOC is the name of the person concerned and the request to open a case. No health related information is transferred to IDOC.

To ***recipients other than Community institutions and bodies***, this includes the following: *(i)* Two insurance companies established in Belgium and governed by Belgian law. The data transferred includes identification data, date of birth, private and work address, data of the accidents of occupational illness, type of injury, and bank related information. Payments to EU staff that have suffered an accident or occupational disease will be made directly by the insurance company except for the reimbursement of medical expenses[7]. *(ii)* External doctors designated by the Appointing Authority.

As far as the ***right to information*** is concerned, the prior check notification has been accompanied by a privacy statement which it is said to be available on the Commission's intranet. The Staff of the EDPS had difficulties in finding it in the intranet and only found it after obtaining further explanations from the PMO concerning its location. The privacy statement contains information on the following issues: identity of the data controller, the types of data and purposes of the processing, the recipients of the data, the existence of a right of access and rectification and the conditions to exercise the right of access. It also contains the legal basis, time limits for storing the data and the right to have recourse at the European Data Protection Supervisor.

The *right of access* and the procedures to exercise it are recognised in the privacy statement. The ***right of rectification*** is recognised.

Security measures have been implemented.

2.2. Legal aspects

2.2.1. Prior checking

Grounds for prior checking: Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001" or simply "Regulation") applies to the *"processing of personal data wholly or partly by automatic*

[6] DG BUDGET will recover the amounts later on from the insurance companies.
[7] See footnote 6.

means, and to the processing otherwise than by automatic means of personal data which form part of a filing system" and to the processing "*by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law*"[8].

For the reasons described below, all the elements that trigger the application of the Regulation exist in the processing of data that takes place in the context of the management of the Accidents and Occupational Disease Insurance:

Firstly, the EDPS notes that the management of the Insurance entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, as described in the Notification, personal data of insured parties, will be collected and further processed. This includes information related to the health of the insured parties such as reports from doctors specifying the nature of injuries, consequences of the accident, information regarding medical treatments, name of the occupational disease, etc.

Secondly, as described in the Notification, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2 (b) of the Regulation (EC) No 45/2001 as well as manual data processing operations. Indeed, the personal information is first collected in paper form directly from EU Staff members. In most cases, the information is scanned and kept in a software database which is used by the PMO.3 001 in order to ensure the management of the Insurance Scheme. Additional follow up data processing operations will depend on the type of claim made by the EU staff member (i.e., occupational diseases or accidents and subsequent claim for reimbursement).

Finally, the EDPS confirms that the processing is carried out by a Community institution, in this case by the Sickness and Accidents Insurance Unit, of the Office for the Administration and Payment of Individual Entitlements, which is part of the European Commission, in the framework of Community law (Article 3.1 of the Regulation (EC) No 45/2001). Therefore, clearly all the elements that trigger the application of the Regulation exist in the management of the Accidents and Occupational Disease Insurance:

Assessment of whether the data processing operations fall under Article 27 of the Regulation: Article 27.1 of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS *"processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes"*. Article 27.2 of the Regulation contains a list of processing operations that are likely to present such risks. This list includes, under paragraph (a), the processing of data relating to heath. The data collected in connection with the management of the Insurance Scheme clearly relates to the health of individuals and is therefore health data. Therefore the processing operations must be prior checked by the EDPS.

Ex post prior checking: Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have already been established. This is not a serious problem as far as any recommendations made by the EDPS may still be adopted accordingly.

Notification and due data for the EDPS Opinion: The Notification was received on 9 March 2007. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within

[8] *Ex* Article 3.2 of Regulation (EC) No 45/2001.

which the EDPS must deliver an opinion was suspended for a total of 78 days. The Opinion must therefore be adopted no later than 27 July 2007.

2.2.2 Lawfulness of the processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. As pointed out in the Notification, the grounds that justify the processing operation are based on Article 5 a), pursuant to which data may be processed if the processing is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

In order to determine whether the processing operations comply with Article 5 a) of Regulation (EC) No 45/2001 two elements must be taken into account: First, whether either the Treaty or other legal instruments foresee the data processing operations carried out by PMO.3, and second, whether the processing operations are necessary for the performance of a task.

Relevant legal grounds in the Treaty or in other legal instruments.- In ascertaining the legal grounds in the Treaty or in other legal instruments that legitimise the processing operations that take place in the context of the management of the Accidents and Occupational Disease Insurance, the EDPS takes note of Article 73 of the Staff Regulations. As illustrated below, this Article sets forth the EU officials' entitlement to accidents and occupational disease insurance, subject to rules drawn up by agreement.

In particular, Article 73.1 of the Staff Regulations establishes 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. Such rules shall specify which risks are not covered*". Article 25 of Annex X of the Staff Regulations establishes that *"The spouse, children and other persons dependent on the official shall be insured against accidents occurring outside the Community in the countries appearing on a list adopted for this purpose by the appointing authority*".

Section 2 of Article 73 sets forth the benefits payable to EU staff members in the event of death, total or permanent invalidity. Article 73 also establishes that some services and products[9] will be covered under the same Scheme however, where the amount paid under Article 72 does not fully cover the expenditure incurred. Article 72 refers to the Sickness Insurance Scheme, which has been prior checked by the EDPS[10]. The EDPS further notes that in accordance with the above Article 73, on 13 December 2005 the Institutions adopted Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease. The Rules entered into force on January 2006. Among others, the Rules define what is to be considered an accident, an occupational disease, defines the exclusions from cover, the benefits, and the procedures to ensure the reimbursement of expenses.

[9] Medical, pharmaceutical, hospital, surgical, prosthesis, radiography, massage, orthopaedic, clinical and transport expenses and any other similar expenditure incurred as a result of the accident or occupational disease.
[10] EDPS Opinion of 10 July 2007 on a notification for prior checking related to management of the sickness insurance scheme (Case 2004-238).

The above legislation which refers to active Officials of EU institutions is complemented by Article 28 of the Conditions of employment *of other servants* of the European Communities which applies to temporary agents. In particular, Article 28 establishes that *"Articles 72 and 73 of the Staff Regulations, concerning sickness and accident cover, shall apply by analogy to temporary staff during the period of employment, during sick leave an during the periods of unpaid leave referred to in Articles 11 and 17..."*.

Furthermore Article 85a of the Staff Regulations establishes that " *where the death, accidental injury or sickness of a person covered by these Staff Regulations is caused by a third party, the Communities shall, in respect of the obligations incumbent upon them under the Staff Regulations consequent upon the event causing such death, injury or sickness, stand subrogated to the rights, including rights of action, of the victim or of those entitled under him against the third party"*.

Upon analysis of the above legal framework, the EDPS considers that the data processing that takes place in connection with the management of the Insurance Scheme is clearly carried out on the basis of the Staff Regulations (Article 73), the Conditions of employment of other servants of the European Communities (Article 28) and on the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease. These legal instruments foresee the EU active officials and other servants' entitlement to be insured against accidents and occupational diseases under certain conditions. In order to implement this obligation the Institutions have set up an Insurance Scheme whose management entails the processing of personal data. Clearly, the Accidents and Occupational Disease Insurance is legally based on the above legal instruments.

Necessity test .- According to Article 5 (a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. It is therefore relevant to assess whether the data processing that occurs in the context of the Insurance is "*necessary"* for the performance of a task, in this case, for the management of the Insurance Scheme.

As outlined above, under the Staff Regulations, EU active staff members are entitled to benefit from an insurance against accidents and occupational diseases, under the conditions set forth in this legislation. The Institutions have the obligation to provide this benefit to EU active staff members. To execute this obligation that is binding upon the Institutions it is consistent for the Institutions to set up an Accidents and Occupational Diseases Insurance. For an insurance scheme to function properly and to have sound administration, it is necessary for the managers of the scheme to engage in processing of personal data. This is because the proper management of the scheme requires, among others, to ensure that the persons covered by the scheme (and not others) are duly reimbursed. To this end, it is necessary to identify insured parties. Furthermore, to ensure that members are reimbursed according to the rules, the managers of the scheme must collect information about the occupational sicknesses/accident at stake. Only the collection of such information will enable the management of the Scheme; including ascertaining whether individuals are covered and if so the percentages. In sum, it is the EDPS's view that the data processing that takes place in the context of the Accidents and Occupational Disease Insurance is indispensable for the sound management of this Scheme.

2.2.3. Processing of special categories of data

Processing of personal data concerning health is prohibited unless grounds can be found in Articles 10.2 and 10. 3 of the Regulation. Article 10. 2 (b) of the Regulation establishes that

the prohibition shall not apply where the processing is "*necessary for the purpose 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*".

As explained above concerning the legal basis, the justification for processing personal data in the context of the Insurance Scheme, including health data, can be found in the Staff Regulations and the Conditions of employment of other servants of the European Communities. To this extent, this processing takes place as a result of the employer's obligation to provide accident/occupational disease insurance. Therefore, the processing clearly falls under Article 10.2 (b) and is therefore not prohibited.

As it is an exception to a general prohibition, Article 10 2 (b) must be interpreted strictly. In particular, as Article 10 2 (b) stipulates, in order for the exception to apply, the processing must be '*necessary*' for the purposes of complying with the specific rights and obligations in the field of employment law. Thus, the processing of sensitive data is permissible only insofar as it is relevant and necessary for the purposes of providing the Accidents and Occupational Insurance. The question of necessity is further addressed below, when applying Article 4 (1) (d) of the Regulation regarding data quality.

In addition to the application of Article 10 2 (b), the processing of health data carried out by doctors would also be exempted from the prohibition per application of Article 10.3 *"Paragraph 1 shall not apply 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"*. The same exception may apply to the staff working for PMO.3.001 per application of Article 24 of the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease*: "Staff assigned to administering these rules shall be required to observe confidentiality regarding medical documents and/or expenses which come to their attention in the course of the performance of their tasks. They shall continue to be subject to this obligation after their duties have ceased under these rules".* In this regard, the EDPS recommends that the PMO.3.001 should raise awareness among its non-medical staff regarding the application of medical secrecy. This is crucial for non-medical staff given that, as opposed to trained medical practitioners, they are only bound by the medical secrecy rules by virtue of Article 24 of the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease, and not on the basis of their professional title. This means that they are not subject to an external self-regulatory authority in matters of professional ethics, such as a national medical chamber. Neither do the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease provide for an elaborate set of rules on medical secrecy similar to what is available on the national level. Perhaps even more importantly, medical practitioners received comprehensive training on matters related to medical ethics, including medical secrecy. There is a world of difference between the knowledge and commitment to medical secrecy between, on one hand, a medical doctor who took the Hippocrates Oath and, on the other hand, accounting and administrative staff who never received formal training on medical secrecy issues and are subject only to requirements of medical secrecy by virtue of an Article of the 2006 Common rules on the insurance of officials against the risk of accident and of occupational disease that they may only perused in a cursory manner.

For these reasons, the EDPS recommends that all PMO.3.001 staff and other non-medical staff with access to medical data should receive appropriate and comprehensive training on

issues of medical secrecy. They should also be required to acknowledge in writing that they have received such training and that they undertake to abide by their confidentiality obligations.

2.2.4. Data quality

Adequacy, relevance and proportionality.- Pursuant to Article 4.1.(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This is referred to as the data quality principle.

Some of the information requested from insured parties must be provided through standardised forms to be filled in and to be accompanied by prescriptions and/or medical reports. For example, this applies to the accident reports. The EDPS has not identified in this form any request for information that, in principle, would be irrelevant or excessive.

However, a great amount of information will be contained in the medical reports. In this case, whether the information provided is excessive will depend on each particular case. In order to ensure that inadequate, irrelevant and non excessive information is not provided in such reports, it may be appropriate to provide guidelines about the content of such reports and also what exactly must be provided to the PMO 3.001 by EU staff members and insured parties. For example, the list of items/information to be provided to the PMO 3 could be described in the forms themselves. The guidelines would constitute guidance for doctors in order to direct them about the information that is relevant for the scheme, thus, contributing to the provision of adequate and relevant information. On the other hand, the guidelines would also apply to insured parties in order for them to know which information is necessary and which information is not necessary. For example, a form for occupational diseases could be drafted listing, among others, the necessary content of the report to be attached describing the nature of the disease. Furthermore, if irrelevant information is nevertheless provided to support a particular request, the PMO 3 should instruct its staff that such information should not be inserted in ASSMAL. The EDPS also considers that it would contribute to the proportionality of the data processing if members of the scheme were required to provide the information in a sealed envelope marked "confidential" or "to be opened by addressee only" or similar. This is particularly important regarding the underlying medical reports that accompany requests for recognition of occupational diseases and accident reports. Individuals should be informed of the importance of following this practice. The EDPS considers that the website and privacy statement should be amended to request EU staff members to follow these guidelines when sending medical information. Furthermore, transfers of this information by the PMO 3. to doctors designated by the Appointing Authority, should also be transmitted in a sealed envelope.
In addition to the above, in order to ensure that access to the underlying medical reports is strictly limited, PMO 3. should ensure that access rights to ASSMAL are set up on a need-to-know basis and to set up strict procedures to avoid unauthorised access.

Finally, the adequacy, relevance and proportionality should also be assessed regarding the information that is transferred to the insurance companies. According to the Notification, the data transferred includes identification data, date of birth, private and work address, data of the accidents and occupational illness, and type of injury/occupational disease, and bank related information. The transfer of this information seems necessary in order for the insurance companies to execute their obligations under the reinsurance contract. The company, among others, will need identification information to determine the identity of the individual, whether he/she is covered by the insurance policy. It will need information on the

injury/occupational disease to verify the events at stake and assess the relevant tariffs. It appears to the EDPS that the information provided to the insurance companies is adequate and proportional to the purposes of the processing of such companies.

Fairness and lawfulness.- Article 4.1. (a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2.). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 2.2.7.

Accuracy.- According to Article 4.1. (c) 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 the data which are inaccurate or incomplete , having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified"*. In this case, the data include medical reports, prescriptions, receipts from medical expenses, etc. Given the nature of most of the data, it is not easy to prove accuracy. However, the EDPS emphasises that PMO 3 must nevertheless take every reasonable step ensure that data are up to date and relevant.

2.2.5 Conservation of data/ data retention

Pursuant to Article 4. 1. (e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data of data subjects for not longer than is necessary for which the data are collected and/or further processed.

In addressing the conservation/retention question regarding paper information, the EDPS understands from the privacy statement and from the Notification that PMO 3. keeps information in paper form for the lifetime of the EU staff member plus five years. The EDPS is told that the reason for keeping the information for this long period is to enable the EU staff member or those entitled under him to re-open the file, following an aggravation of the occupational sickness or outcome of the accident. For example, this would enable the EU staff member to claim further benefits. As a general rule as concerns conservation of medical data, the EDPS considers that a period of 30 years is the absolute maximum during which data should be kept, apart from some specific exemptions. However, in his recommendations issued on 26 February 2007 in case 2006-532 in response to the request of the Collège des Chefs d'administration regarding the application of Article 73 of the Staff Regulations, the EDPS agreed with the need to keep health data for longer periods. In this case, the EDPS considers that the benefits derived from keeping the data for the lifetime of the member plus five year may outweigh the threat to privacy and data protection. Indeed, it appears that the need to ensure that members are able to re-open a case and re-adjust their entitlements according to their final health situation justify the keeping of the information during all the time where members or descendants are entitled to exercise this right. The possibility to re-open a case is explicitly mentioned in Article 21 of the 2006 Common rules on the insurance of officials of the European Communities against the risk of accident and of occupational disease. However, the EDPS insists on the need throughout the conservation time to ensure that appropriate technical and organizational measures are implemented in order to avoid the unwanted/unlawful disclosure of the information.

Finally, the EDPS notes that the privacy policy only refers to the length of storage of information kept in paper, but is silent regarding electronic storage. The EDPS considers that the privacy policy should be complemented in order to describe the storage and retention period for the data kept in ASSMAL. This would not only provide the information on the

retention but, as further described below, it would also indicate that the information is not only kept in paper form, which is an important piece of information.

2.2.6 Transfers of data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made *ex* Article 7 to Community institutions or bodies, *ex* Article 8 to recipients subject to Directive 95/46[11], or to other types of recipients *ex* Article 9. The facts described in the Notification reveal that the information collected is transferred to two types of recipients:

(i) Community institutions and bodies: In particular, the information is transferred to *(i)* PMO Salaries and DG BUDGET to calculate salaries and execute the payment of amounts due via the EU staff members' bank account respectively, *(ii)* IDOC in the context of harassment cases. In addition, (iii) data may be transferred to DG ADM B2 in the context of appeals under Article 90 of the Staff Regulations. Because all these recipients are Community institutions or bodies, Article 7 of the Regulation applies.

(ii) To recipients other than Community institutions and bodies, this includes the following: *(i)* The two insurance companies established in Belgium and operating under Belgian law. The data transferred to the insurance companies includes identification data, date of birth, private and work address, data of the accidents of occupational illness, type of injury, and bank related information. *(ii)* External doctors designated by the Appointing Authority. Because these recipients are subject to Directive 95/46 Article 8 of the Regulation applies.

Application of Article 7 of Regulation (EC) No 45/2001.- The EDPS recalls that Article 7 of Regulation (EC) No 45/2001 requires that personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, PMO 3 must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary.

The EDPS considers that the transfers of information to DG BUDGET and to the PMO Salaries for the purposes stated above comply with requirements. In both cases, the recipients have the competence to perform the task assignment for which the data is transferred, i.e., to determine salaries and execute the payment of amounts due via the EU staff members' bank account. Also, in both cases, the data transfers will be necessary in order for the addressees to perform their tasks. The above applies as long as the data sent to DG BUDGET and PMO salaries are limited to the data necessary for the performance of their tasks. In both cases, the type of information to be transferred will be limited to identification information of the member, bank account information and salary information. No health related data should be transferred to PMO and DG BUDGET insofar as such information is not necessary for the performance of their tasks.

The EDPS has also analysed the data transfers to IDOC and agrees that it has the competences to carry out the tasks for which the data are transferred to it. The EDPS notes that the data processing carried out by IDOC was the object of an EDPS Opinion in 2005[12].

---

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[12] EDPS Opinion on the notification for prior checking relating to internal administrative inquires and disciplinary procedures within the European Commission, 20 April 2007 (Case 2004-187). The Opinion is available at:

Application of Article 8 of Regulation (EC) No 45/2001.- Article 8 establishes that personal data shall only be transferred to recipients subject to national law implementing Directive 95/46/EC if *(a)* the recipient establishes the fact that data are necessary for the performance of a task carried out in the public interests or subject to the exercise of public authority or *(b)* the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subjects' legitimate interests may be prejudiced.

As outlined above, data are transferred to insurance companies, which can be deemed to act both as data processors and data controllers. In acting as data processors, the insurance companies process the information received as requested by the data controller, the PMO 3., for the purposes specified by the data controller. The wording of the insurance contract between the Commission and the insurance companies partially and indirectly reflects the processing role, for example by defining clearly the procedures of the insurance company regarding each accident/occupational disease request. However, the EDPS notes that the above mentioned agreement was signed before Regulation (EC) No 45/2001 and its wording does not refer explicitly to data protection and to the processing role itself. However, the PMO indicated to the EDPS that a new agreement was in the process of being drawn up which introduces specific data protection provisions. The EDPS considers that it would be appropriate to include such a new provision.

In addition to the data processor role, the insurance company also acts as a data controller and this role is also reflected in the contract and in the practical arrangements between the companies and the Commission[13]. Under this role, the EDPS considers that Article 8 (b) is complied with insofar as the insurance company has the need to hold the information and the legitimate interests of the individual are not prejudiced. Indeed, the EDPS considers that the transfer of information to the insurance companies as a necessary measure to minimise the EU institutions financial impact of professional diseases. It is in the public interest to enter into an agreement with an insurance company to guarantee in relevant cases that the financial burden of a professional disease of an EU staff member will be covered by the insurance company. As discussed above under 2.2.4, the company will need identification information, among others, to determine the identity of the individual, whether he/she is covered by the insurance policy. It will need information on the injury/occupational disease to verify the events at stake and assess the relevant tariffs. The common principles of the law of contracts, as resulting from common European practice, include the right of the insurance company to have enough information on the professional sickness in order to exercise all rights and actions available to it.

As far as external doctors designated by the Appointing Authority are concerned, these play the role of data processors insofar as they process the information on behalf of the data controller, the PMO, for the purposes specified by the controller. The contractual arrangements between the external doctors and the PMO implicitly confirm this role, in different ways. It would be appropriate for the contract to be more explicit and for example introduce a clause similar to the one proposed for the new contract with the insurance companies.

---

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2005/05-04-20_Commission_IDOC_EN.pdf

[13] Such as is the direct payment of benefits to individuals who have suffered an accident or an occupational disease.

2.2.7 Right of access and rectification

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the data controller. According to Article 13 of Regulation (EC) No 45/2001, 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. The information can then be obtained directly by the data subject (this is the so-called "direct access") or, under certain circumstances, by a public authority (this is the so-called "indirect access", normally exercised by a Data Protection Authority, being the EDPS in the present context).

The privacy statement confirms that PMO 3. provides access to personal information and also the right of rectification. It further establishes the arrangements in this respect. The EDPS welcomes that the PMO 3 allows access to insured parties' files without any specific restrictions. The EDPS recalls that access cannot be limited to "justified cases" and must be allowed for any or no reason at all. Insured parties cannot be required to specify the purpose of the request. Furthermore, in order to ensure that access requests will be dealt with in a timely fashion and without constrains, it may be appropriate to set up reasonable time limits

The EDPS draws PMO 3's attention to the Conclusions 221/04 of 19 February 2004 of the Collège des Chefs d'administration, which aims at harmonizing certain aspects of access provisions across the Community institutions. This document emphasizes that access must be provided to health data to the maximum extent possible. The document provides, among others, that access should also be provided to data of psychological or psychiatric nature; although in such cases access may be granted indirectly, through the intermediary of a medical practitioner designated by the data subject. In this regard, the EDPS wishes to highlight that the general rule, in all cases, whether they concern mental or physical conditions, remains direct access. However, *ex* Article 20.1 (c) of Regulation (EC) No 45/2001, the access to data of psychological or psychiatric nature can be provided indirectly, if an assessment made on a case by case basis reveals that indirect access is necessary for the protection of the data subject, given the circumstances at stake[14].

2.2.7 Information to the data subject

Pursuant to Article 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals to whom the data refers of the fact that their data are being collected and processed. Individuals are further entitled to be informed of, *inter alia*, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The Notification was accompanied by a privacy statement which is supposed to be made available to EU staff members through the Commission's intranet, in the section that deals with occupational diseases and accidents. The privacy statement would therefore serve to comply with the above Articles. The EDPS has accessed the intranet in order to verify whether the privacy statement is easily available to individuals downloading the forms where information has to be filled in and has not been able to find the privacy policy. The PMO 3 has informed the EDPS that the privacy statement that informs about the data processing at

[14] Article 20.1 (c) of Regulation (EC) No 45/2001 reads as follows: The Community institutions and bodies may restrict the application of Article 4.1, Article 11, Article 12.1, Articles 13 to 17 and Article 37.1 where such restriction constitutes a necessary measure to safeguard: (c) the protection of the data subject or of the rights and freedoms of others.

point is provided together with the privacy statement for a different data processing, that of the Sickness Insurance Scheme. This was confirmed.

The EDPS considers that the privacy statement for the Insurance Scheme should be placed separately from the privacy statement for the Sickness Insurance Scheme. In particular, the EDPS considers that the statement should be included in the web page that deals with the Accidents and Occupational Disease Insurance, which is entitled *"What if I have an accident?*", on web page http://intracomm.cec.eu-admin.net/pers_admin/sick_insur/accident/index_en.html. This would make the privacy statement easy to find. It will also avoid the current confusion where two privacy statements regarding different data processing are mixed up together. When uploading the statement, the EDPS suggests including a link to the privacy policy on the pages where the forms are available for downloading. This will provide direct access to the privacy statement from the web page where the member has to go through in order to download the form. The URL where the privacy statement is available should also be printed in the form to report accidents.

The EDPS has checked the content of the information provided in the privacy statement to check whether the content is in line with requirements of Article 11 and 12 of Regulation (EC) No 45/2001.

The EDPS notes that the privacy statement contains information on the identity of the data controller, the purposes of the processing and how the data is processed, the conditions for the exercise of the right of access, the time limits for storing the data and the legal basis for the processing operations for which the data are intended. The EDPS considers that the privacy statement contains most of the information required under Article 11 and 12 of the Regulation, however, it considers that several amendments would contribute to ensure full compliance with Article 11 and 12, in particular:

(i) It is observed that there is no reference to the fact that the data undergoes automatic processing. The EDPS considers that to ensure the fair processing of information, the privacy statement should indicate that if not all, most of the information provided to the PMO 3 is inserted in an electronic database. This is particularly necessary taking into account that members are asked to send the information in paper form, thus, nothing indicates to insured parties that the information they send are kept in an electronic form.
(ii) In order to ensure full transparency and fair processing, it would be appropriate to add a contact address (that of the data controller or someone from his Unit) where insured parties could send questions regarding the privacy statement.
(iii) The section that deals with data transfers should be complemented to indicate that data may be transferred to IDOC for the purpose of the inquiry in case of harassment.
(iv) As outlined above, the information regarding time limits for storing the data only concerns paper information. References to the time limits that apply to information stored in ASSMAL should be added.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations in this Opinion are fully taken into account. In particular, PMO 3. must:

- Raise awareness among PMO 3. staff regarding the application of medical secrecy of all the staff members, not only to medical officers. This should include training and signing a specific confidentiality declaration.
- In order to ensure that inadequate, irrelevant and non excessive information is not provided in medical reports there should be guidelines about the content of such reports
- Instruct EU staff members to send medical reports that support requests for recognition of occupational diseases in sealed envelopes marked with the terms 'confidential' and/or 'to be opened by addressee only'. These instructions should be given in the Web site that deals with the Accidents and Occupational Disease Insurance.
- Ensure that access to medical reports contained in ASSMAL is limited to individuals on a need to know basis.
- Include explicit data protection provisions in contractual arrangements with insurance companies and external doctors designated by the Appointing Authority.
- Upload the privacy statement in the appropriate web page and insert a link to the privacy statement in the web page where the forms for downloading are available and insert a link to the policy in the forms themselves.
- Amend the privacy policy as recommended in this Opinion.
- Put time limits for the exercise of the right of access.
- Retain log files in order to keep track of access (and detect unauthorized access) to ASSMAL.

Done at Brussels, 27 July 2007

Joaquín BAYO DELGADO
European Data Protection Assistant Supervisor