Opinion on a notification for prior checking received from the Data Protection Officer of the Commission related to management of the Sickness Insurance Scheme

Brussels, 10 July 2007 (Case 2004-238)

1. Proceedings

On 6 March 2007, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of the Commission a notification for prior checking ("the Notification") regarding the data processing operations related to the management and reimbursement of the Sickness Insurance Scheme ("Sickness Insurance Scheme") carried out by the Office for the Administration and Payment of Individual Entitlements ("PMO").

The EDPS requested complementary information on 4 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 Sickness Insurance Scheme. On 14 June 2007 the EDPS sent the draft Opinion to the PMO for comments. PMO staff and the EDPS staff met again on 22 June 2007. During the meeting PMO staff gave their comments to the EDPS on the draft Opinion which were later on reflected in the paper version of the draft Opinion on 29 June 2007.

2. Examination of the matter

2.1. The facts

Overview of the Sickness Insurance Scheme: The Sickness and Accidents Insurance Unit of the PMO ("PMO.3") is responsible, among others, for the management of the Sickness Insurance Scheme for officials, temporary agents and retired staff of EU institutions ("EU staff members"). Spouses/partners, children and dependents may also be covered by the insurance ("insured parties")[1].

The Sickness Insurance Scheme was established pursuant to Article 72 of the Staff Regulations of Officials of the European Communities and Article 28 of the Conditions of employment of other servants of the European Communities[2]. The Notification concerns the data processing operations relating to the management of the Sickness Insurance Scheme.

[1] In this Opinion we will use the term "EU staff members" to refer to officials, temporary agents and retired staff of EU institutions which are entitled to accidents and occupational disease insurance under Article 72 and 28 of the Staff Regulations and the Conditions of employment of other servants of the European Communities respectively. We will refer to "insured parties" to include also spouses/partners, children and assimilated dependents. References will be made to members or insured parties, as appropriate.

[2] Adopted by the Council on 22 March 2004. These two documents will be referred respectively as "Staff Regulations" and "Conditions of Employment" or sometimes together as "Staff Regulations".

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

In order to manage the Sickness Insurance Scheme and reimbursements under the scheme, certain rules were established to complement Article 72 of the Staff Regulations. Among others, the rules determine the exact percentage to be reimbursed, which depends on the nature of services, the type of sickness, the procedures for the reimbursement, and other factors. According to these rules, in general, EU staff members of the Sickness Insurance Scheme pay the fees related to the use of medical services and pharmaceutical products upfront. Subsequently, EU staff members must complete standardised forms claiming the reimbursement of their expenses and forward them in paper form to the Settlement Office within PMO.3. The forms must be accompanied by the original invoices and medical prescriptions. In the event of hospitalisation, EU staff members can request from the Settlement Office to accept direct billing of the hospitalisation costs.

For certain treatments, prior authorisation is required from the Settlement Office before commencing the therapy or medication. In such cases, EU staff members have to provide to the Settlement Office specific information regarding the treatment as well as a medical prescription indicating, among others, the diagnosis of the illness requiring the treatment. Similar procedures apply for the recognition of serious illnesses, which are reimbursed at a higher percentage than regular illnesses.

Upon receipt of the claims for reimbursement, staff from the Settlement Office scans the documents received, enters the scan and any additional information into a computer and processes the claim. The software database used is ASSMAL. The Office periodically draws up payment lists and the payment orders which are transferred to DG BUDGET for the payment via the members' bank account.

The overall ***purpose of the processing*** of the data is to manage and ensure the reimbursement of the medical expenses that result from membership in the Sickness Insurance Scheme, in accordance with Article 72 of the Staff Regulation and its implementing rules.

The primary ***responsibility for the data processing*** lies within PMO.3, as explained above. Most of the data processing operations carried out within the scope of the management of the Sickness Insurance Scheme are performed by the Settlement Office within PMO.3. In addition, the medical officers attached to PMO.3 also perform certain data processing operations.

As further described below, the manual and automated data processing operations are closely interrelated. Whereas some data processing operations such as the initial collection of information are manual, later on this information is invariably introduced in a software database and transferred electronically. The ***manual operations*** can be summarised as follows:

- Regarding claims for reimbursement of medical expenses, once the Settlement Office has received the claim to which the statement of fees, invoices and medical prescriptions are attached, staff of the Settlement Office proceeds to *scan* them. Then, staff from the Settlement Office *assesses* the nature of each expense and its tariff, based on the documents provided by the EU staff member. Following this assessment, this information is encoded in order to undergo further processing towards the final reimbursement of the expenses.
- Applications for prior authorisation including for dental treatments are received by the Settlement Office, which is the body in charge of receiving the forms and related documents. These additional documents include the medical prescription stating the reasons for the treatment, information on the treatment (type, number of sessions, likely

duration) as well as information regarding the diagnosis of the illness requiring the prescription. The staff within the Settlement Office sends such requests to the medical officer's office, which will introduce the information in ASSMAL. The medical officer will *assess* whether the request should be granted. His/her opinion will be reflected in a word document, saved in the software database ASSMAL. If the medical officer recommends the authorisation to be granted, the Settlement Office issues a formal authorisation, which is then delivered to the claimant.

- Applications for direct billing are *received* and *scanned* by the Settlement Office which afterwards *verifies* whether the claimant is entitled to it. If so, staff from the Office *drafts* a letter of direct billing which is sent directly to the member in paper form. An electronic version of the letter is kept in ASSMAL.
- Application for recognition of serious illnesses must be sent to medical officers, attaching a detailed medical report. The staff working for the medical officers *scans* the information in ASSMAL. Upon analysing the documents the medical officer issues an opinion *recommending or not* the authorisation to be granted. This opinion is stored in ASSMAL. The head of the Settlement Office issues a formal authorisation, which is then delivered to the claimant. Each authorisation is referenced with a number.
- Confidential Information Forms must be completed to assess whether spouses/partners have any entitlement under the Sickness Insurance Scheme. As the form currently stands, spouses/partners are requested to provide information on their employment situation, including name of employer and also whether they receive pension or income. Furthermore, they are asked to provide the annual income from employment, pension, etc., and to specify whether they can be covered under a legal or statutory primary Sickness Insurance Scheme other than that of the EC. This information is provided by members in paper form to the Settlements Office which will introduce some of the information in ASSMAL.

Whereas the above data processing operations have a manual component, all of them are reflected in electronic documents and are ***automated***. This includes the following:

- Electronic archiving in the software database ASSMAL of all the documents that are scanned upon reception, including claim forms, copies of the prescriptions from doctors, original statements of fees. Such archiving is done either by staff of the Settlement Office (claims for reimbursement of medical expenses) or by the staff working with the medical officer (recognition of serious illnesses and request for prior authorisation).
- Encoding of the expenses and their assessment according to tariffs; subsequent archiving in ASSMAL.
- Electronic archiving in the software database ASSMAL of recommendations/opinions from medical officers regarding prior authorisations and the recognition of serious illnesses.
- Drafting of payment lists and the corresponding payment orders which are then transferred electronically to DG BUDGET for the payment via the EU staff members' bank account.
- Electronic archiving of documents such as approvals of direct billings, confidential declarations, approvals for treatments, including dental treatments, authorisations of recognition of serious illnesses.

Access to ASSMAL is based on a need-to-know basis. For example, underlying medical information entered in ASSMAL by the medical officers cannot be accessed by staff of the Settlement Office. For example, as concerns the recommendations/opinions from medical officers regarding prior authorisations and recognition of serious illnesses, people other than

medical officers will only visualise in ASSMAL whether the recommendation was accepted or not (i.e. "yes" or "not").

Data subjects include the following: *(i)* members, officials of the EU institutions and agencies; *(ii)* temporary staff of the EU institutions and agencies; *(iii)* contract staff of the EU institutions and agencies, *(iv)* retired staff and, *(v)* Spouses/unmarried partners, children and persons treated as dependent child.

In addition to the above, other data subjects whose information is also processed include the names of external doctors, for example those who issue prescriptions, as well as medical officers of the Commission.

The ***categories of personal data*** collected include the following: *(i)* data related to the members of the Sickness Insurance Scheme: EU staff member number, institution for which he/she works, office address and home address if retired, data of birth, type of beneficiary (whether member, dependent children or equivalent or spouse); *(ii)* bank account information where payments must be made, *(iii)* salary information; and *(iv)* information related to the insured parties' health (prescriptions from doctors, statement fees related to the purchase of pharmaceutical products, medical reports, etc). Whether a particular category of data will be collected in each case will depend on the specifics of the case. For example, salary information is used only for the purposes of the application of Article 72.3 of the Staff Regulation[3].

As far as ***conservation of data*** is concerned, paper files related to the underlying medical conditions of insured parties (such as documents provided to prove a serious illness) are kept during the member's lifetime plus five years. They are stored for a period of two years in the PMO.3 offices, after which they are stored in the central archives of the Commission, given the limited space available in the PMO.3 facilities. Paper files related to claims for reimbursement of medical expenses are destroyed after a total length of 7 years.

As explained above, in addition to paper form, all electronic files, including the claims for reimbursement of medical expenses are stored in the software database referred to ASSMAL, which is hosted in Luxembourg. Information contained in ASSMAL is kept for the lifetime of the member plus five years.

The data controller, PMO.3, may ***transfer personal data*** to the following types of recipients, all of which are Community institutions or bodies: *(i)* DG BUDGET who will make the payment of amounts due via the EU staff members' bank account; *(ii)* PMO Salaries to recover from salaries amounts that were advanced in the context of hospitalisation and *(iii)* the Medical Council, Management Committee and Unit ADMIN.B.2 in the context of the following two procedures, in particular:

(i) The Medical Council may be consulted by the Management Committee or the Central Office concerning any matter of a medical nature which arises in connection with the

[3] Article 72.3 establishes that where a total expenditure not reimbursed for any period of 12 months exceeds half the official's basic monthly salary or pension, special reimbursement shall be allowed by the appointing authority, account being taken of the family circumstances of the person concerned, in the manner provided for in the rules referred to in paragraph 1.

Sickness Insurance Scheme. In the context of a consultation, personal data may be transferred to the Medical Council by PMO 3[4].
(ii) Where a decision taken by PMO.3 in respect of the Sickness Insurance Scheme gives rise to a grievance, a complaint may be lodged under Article 90(2) of the Staff Regulations. In this case, in accordance with Article 16 of the 2004 Joint Rules on Sickness Insurance for officials of the European Communities ("Joint Rules on Sickness Insurance", further described in Section 2.2.2 below), the appointing authority must ask for the Management Committee's opinion before ruling on a complaint. The opinion, which is not binding for the administration, is sent simultaneously to the appointing authority and the complainant. In such cases, the Management Committee will receive the complaint as well as the underlying medical information from PMO.3. Such information may be complemented by information provided by the medical officer. Because DG ADMIN B 2 is in charge of managing the appeals under Article 90 of the Staff Regulations, it may also receive information directly from the member.

As far as the ***right to information*** is concerned, the Notification refers to a privacy statement which intends to provide information to members of the Sickness Insurance Scheme. The privacy statement is available in the Commission intranet, in the section that refers to the Sickness Insurance Scheme:
http://intracomm.cec.eu-admin.net/pers_admin/sick_insur/index_en.html.

The privacy statement contains information, among others, on the identity of the data controller, the purposes of the processing and the existence of a right of access. It also contains time limits for storing the data and the reference to the applicable legal basis. **The *right of access*** and the procedures to exercise it are recognised in the privacy statement. There are no references to the ***right of rectification***.

Security measures are implemented.

2.2. Legal aspects

2.2.1. Prior checking

This Prior check Opinion relates to the management of the Sickness Insurance Scheme carried out by the PMO, pursuant to Article 72 of the Staff Regulations and Article 28 of the Conditions of Employment. Accordingly, the Opinion will assess the extent to which the data processing operations described above carried out by PMO 3 are in line with 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 ("Regulation (EC) No 45/2001" or "Regulation").

[4] The role of the ***Medical Council*** is foreseen by Article 22 of the Joint Rules on Sickness Insurance. In particular, Article 22.2 establishes that "The Medical Council may be consulted by the Management Committee or the Central Office concerning any matter of a medical nature which arises in connection with this Scheme. It shall meet at the request of the Management Committee, of the Central Office or of the medical officers of the offices responsible for settling claims and shall deliver its opinion within such time as may be specified". The Medical Council is composed of medical officers from each institution and the medical officers from each office responsible for settling claims. The role of the ***Management Committee*** is foreseen by Article 18 of the Joint Rules on Sickness Insurance, which sets forth the members of the Committee and its functions. Among others, the Committee has the power to deliver opinions, on any matter arising directly or indirectly from the application of the provisions of the Staff Regulations concerning sickness insurance; it has also the power to deliver its opinion on the level of contributions and benefits, in particular where there is an appreciable change in the cost of medical treatment.

In accordance with the above, this Opinion will not deal with the data processing operations carried out by PMO 3 in the context of managing the Accidents and Occupational Diseases Insurance, pursuant to Article 73 of the Staff Regulations. This is the object of a different Opinion which the EDPS is currently analysing separately. Furthermore, this Opinion will not assess the data processing operations that may be carried out by other bodies/institutions that may receive information initially collected from PMO 3 in the context of the management of the Sickness Insurance Scheme and for which such bodies may be data controllers. For example, this is true regarding the processing carried out by DG ADMIN B 2 in the context of managing the appeals under Article 90 of the Staff Regulations or the Management Committee in the context of its attributions.

Applicability of the Regulation. Regulation (EC) No 45/2001 applies to the *"processing of personal data wholly or partly by automatic 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*"[5]. For the reasons described below, all elements that trigger the application of the Regulation are present:

First, the management of the Sickness Insurance Scheme 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 members who exercise their rights under the Sickness Insurance Scheme are collected and further processed. This includes information related to the health of EU staff members such as prescriptions from doctors, statement fees related to the purchase of pharmaceutical products, information regarding medical treatments, etc.

Second, 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.

Finally, the processing is carried out by a Community institution, in this case by PMO.3, which is part of the European Commission, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present in the management of the Sickness Insurance Scheme.

Grounds for prior checking. 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 Sickness Insurance Scheme constitutes 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

[5] See Article 3 of Regulation (EC) No 45/2001.

established. This is not an insurmountable problem provided that all recommendations made by the EDPS will be fully taken into account and the processing operations will be adjusted accordingly.

Notification and due date for the EDPS Opinion. The Notification was received on 6 March 2007. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the two-month period within which the EDPS must deliver an opinion was suspended for a total of 66 days. The Opinion must therefore be adopted no later than 11th 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 a public interest task, and second, whether the processing operations carried out by PMO.3 are indeed necessary for the performance of that task.

Legal basis. 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 Sickness Insurance Scheme, the EDPS takes note of Article 72 of the Staff Regulations. As illustrated below, this article sets forth the EU officials' entitlement to sickness insurance.

In particular, Article 72 of the Staff Regulations establishes that "*An official, his spouse {....}, his children and other dependants within the meaning of Article 2 of Annex VII are insured against sickness up to 80 % of the expenditure incurred subject to rules drawn up by agreement between the institutions of the Communities after consulting the Staff Regulations Committee*". Furthermore, Article 72 provides that "*This rate shall be increased to 85% for the following services: consultations and visits, surgical operations, hospitalisation, pharmaceutical products, radiology, analysis, laboratory test and prostheses on medical prescription with the exception of dental prostheses. It shall be increased to 100% in cases of tuberculosis, poliomyelitis, cancer, mental illness and other illnesses recognised by the appointing authority as of comparable seriousness, and for early detection screening and in cases of confinement. However, reimbursement at 100% shall not apply in case of occupational disease or accident having given rise to the application of Article 73".* The EDPS further notes that in accordance with the above Article 72, on 16 June 2004, the Institutions have adopted Joint Rules on Sickness Insurance for officials of the European Communities. These rules, among others, set forth the procedural rules to ensure the reimbursement of expenses, and the rules on the choice of practitioners, hospitals or clinics.

The above legislation which refers to officials of EU institutions is complemented by Article 28 of the Conditions of Employment. 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 and during the periods of unpaid leave referred to in Articles 11 and 17.... "Article 72 of the Staff Regulations, concerning sickness cover, shall apply by analogy to temporary staff in receipt*

of invalidity allowance and to recipients of a survivor's pension. Article 72 shall also apply to staff referred to in Article 39 (2) that are in receipt of a retirement pension".

Upon analysis of the above legal framework, the EDPS considers that the data processing that takes place in connection with the management of the Sickness Insurance Scheme is carried out on the basis of (i) the Staff Regulations (Article 72), (ii) the Conditions of Employment (Article 28) and (iii) the Joint Rules on Sickness Insurance. These legal instruments foresee the officials and other servants' entitlement to be insured against sickness under certain conditions. In order to implement this obligation, the Institutions set up a Sickness Insurance Scheme whose management entails the processing of personal data. In conclusion, the Sickness Insurance Scheme 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 Sickness Insurance Scheme is "*necessary"* for the performance of a task, in this case, for the management of the Sickness Insurance Scheme.

As outlined above, under the Staff Regulations, officials and other servants are entitled to benefit from an insurance against sickness, under the conditions set forth in this legislation. The Institutions have the obligation to provide this benefit to EU officials and other servants. To execute this obligation it is appropriate for the Institutions to set up a Sickness Insurance Scheme. For a scheme to function and to have sound administration, it is necessary for the managers of the scheme to process personal data. This is because the proper management of the scheme requires, among others, to ensure that the persons covered by the scheme are reimbursed. To this end, it is necessary to identify who are the members of the Scheme. Furthermore, to ensure that members are reimbursed according to the rules, the scheme must collect information about the sickness/treatments of the insured parties. Only the collection of such information will enable the management of the scheme, ascertaining whether insured parties are covered for certain risks/products and if so in what percentages. In conclusion, it is the EDPS's view that the data processing that takes place in the context of the Sickness Insurance Scheme may be considered as necessary 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 Sickness Insurance Scheme, including health data, can be found in the Staff Regulations. The processing takes place pursuant to the employer's obligation to provide sickness insurance. Therefore, the processing falls under Article 10(2)(b) and is not prohibited.

As it is an exception to a general prohibition, Article 10(2)(b) must be interpreted strictly. In particular, 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 Sickness Insurance Scheme. The question of necessity is further addressed below, when discussing Article 4(1)(d) of the Regulation regarding data quality.

The processing of health data carried out by medical officers, for example, in the context of prior authorisations or recognition of serious sicknesses is also exempted from the prohibition by virtue 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, including the Settlement Office pursuant to Article 20 of the Joint Rules on Sickness Insurance "*The Staff assigned to the offices responsible for settling claims and the Central Office shall be bound by medical secrecy with regard to the expenses and/or documents which come to their attention in the exercise of their duties ...".*

In this regard, the EDPS recommends that PMO.3 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 20.4 of the Joint Rules on Sickness Insurance, 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 Joint Rules on Sickness Insurance 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 the one hand, a medical doctor who took the Hippocratic 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 Joint Rules on Sickness Insurance that they may only have perused in a cursory manner.

For these reasons, the EDPS recommends that all PMO.3 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 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 they are collected and/or further processed. This is referred to as the data quality principle.

Some of the information requested from members of the Sickness Insurance Scheme 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 claims for reimbursement, accident reports, and requests for prior authorisation. The EDPS has not identified in the forms any request for information that would be *prima facie* irrelevant or excessive, with the exception addressed below (confidential declaration).

However, considering that sensitive medical information will be contained mainly in the medical reports and prescriptions, it will depend on each particular case whether the information provided is excessive. In order to ensure that inadequate, irrelevant and

excessive information is not provided in such reports/prescriptions, it may be appropriate to provide guidelines about the content of such reports/prescriptions. For example, such guidelines should list the items that are necessary for PMO.3 to respond, to proceed to make the payment or authorise a given treatment. Such guidelines would constitute guidance for doctors in order to direct them what information is required for the Sickness Insurance Scheme. This may contribute to the provision of adequate and relevant information. Furthermore, if irrelevant information is nevertheless provided to support a particular request, PMO.3 and the office of medical officers should instruct its staff that such information should not be introduced in ASSMAL.

The EDPS welcomes the practice followed in the request for recognition of serious illnesses. In this type of procedure, members of the Sickness Insurance Scheme are asked to send medical reports in paper form to the *medical officers*, not to other staff of PMO.3. The EDPS considers that a similar procedure should be followed regarding medical reports that accompany requests for prior authorisation. In order to ensure that this information is sent to medical officers and that the data reach their intended addressees and therefore do not undergo processing that would contravene the data quality principle, individuals should be required to provide the information in a sealed envelope marked "confidential", "to be opened by addressee only" or similar. This is particularly important regarding the underlying medical reports that accompany requests for prior authorisations and recognition of serious illness. Individuals should be informed of the importance of following this practice when sending their information to PMO.3 and medical officer. The EDPS considers that the web site and privacy statement should be amended to request EU staff members to follow these guidelines when sending medical information. Furthermore, if the Settlement Office receives information which is intended for the medical officer, and which is not marked as such, it should be further transmitted in a sealed envelope.

In addition to the above, in order to ensure that access to the underlying medical reports is strictly limited to medical officers, 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.

Confidential information form. The EDPS considers that the information contained in the confidential information form is relevant and adequate in order to assess whether spouses/partners may be covered by the EU Sickness Insurance Scheme. However, taking into account that having such coverage is not mandatory - i.e. it is up to partners/spouses to accept or decline the entitlements that arise from the Sickness Insurance Scheme - they should not be requested to provide any information in cases where no entitlement is sought (for example, the partner/spouse does not wish to benefit from any entitlement). Therefore, the EDPS recommends amending the form to specify that this information is only necessary if partners/spouses wish to benefit from their potential entitlements under the Sickness Insurance Scheme. On the other hand, if partners/spouses wish to benefit from the entitlements, they must complete the form. Because the form is completed and signed not by the spouse/partner but by the EU staff member, a question may arise as to whether this constitutes a lawful collection of such information. The EDPS considers that by providing this information in the form, EU staff members must have previously informed and obtained the consent from their spouses/partners. To ensure this outcome, the EDPS recommends amending the form to specify that PMO.3 understands that the partner/spouse is informed of the purposes of the processing of their information and has consented to its transfer and further processing by PMO.3.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data 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)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date"*, and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified"*. In this case, the data include medical reports, prescriptions, receipts for 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 to ensure that data are up to date and relevant. In this respect, see also Section 2.2.8.

2.2.5. Conservation of data

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 subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

The EDPS notices certain inconsistencies between the information provided in the Notification and the information contained in the privacy policy regarding the length of time during which data are retained.

The EDPS understands that PMO.3 keeps documents related to the underlying medical conditions of insured parties (documents provided to prove a serious illness and reports that support prior authorisation) in paper form for the lifetime of the EU staff member plus five years and deletes the claims for reimbursement of medical expenses and respective invoices after 7 years.

The EDPS considers the conservation period of seven years to be reasonable as this is the approximate period during which supporting documents are required to be kept by the Financial Regulation. Indeed, Article 49 of the Financial Regulation, as amended in 2007, establishes that *"The management systems and procedures concerning the keeping of original supporting documents shall provide for: (d) such documents to be kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the documents relate. Documents relating to operations not definitively closed shall be kept for longer than provided for in point (d) of the first subparagraph, that is to say, until the end of the year following that in which the operations are closed"*[6]. However, the EDPS would like to draw PMO.3's attention to the last paragraph of Article 49 of the Financial Regulation according to which *"Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes"* and ask PMO.3 to assess whether this case allows for the deletion of the personal data contained in supporting documents at earlier stages.

The EDPS is concerned about the practice of keeping certain information for the lifetime of the EU staff member plus five years. 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 in this context. The EDPS invites PMO.3 to evaluate to what extent and for what purposes the data it holds about EU staff members needs to be retained for the

[6] Commission Regulation (EC, Euratom) No 478/2007 of 23 April 2007 amending Regulation (EC, Euratom) No 2342/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, OJ L 111, 28.04.2007.

lifetime of the member plus five years. In this respect, the EDPS calls the PMO's attention to his recommendations issued on 26 February 2007 in case 2006-532 in response to the request of the "Collège des Chefs d'administration" to comment on the Collège's proposal of a uniform 30 year conservation period for all medical data across the Community institutions[7]. In his recommendation, the EDPS invited the Collège to reassess its initiative and examine, on a case by case basis, what conservation periods are necessary for specific medicals documents, considering that Article 4(3) of the Regulation requires that data should be kept no longer than is necessary for the purposes for which they are processed.

The privacy policy only refers to the storage length of information kept on paper, but is silent regarding electronic storage. Yet, all the data processed by PMO.3, even the data kept on paper which is deleted after 7 years is also stored electronically in ASSMAL and kept for the lifetime of the EU staff member plus five years. The EDPS considers that the data kept in ASSMAL should be subject to the same deadlines as the data saved in paper form. The reasons that justify keeping the data for a certain period of time are the same for paper and for electronic formats. Therefore, the conservations rules should be brought in line.

According to the above, both as far as paper data is concerned and electronically stored data, a system should be elaborated that allows destroying the information when a given time limit has been reached. This principle should be taken into account particularly in the context of ongoing development of the new ASSMAL.

Furthermore, the EDPS considers that the privacy policy should be complemented to describe the 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 kept in electronic and in paper form.

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 to (i) Community institutions or bodies (based on Article 7), (ii) recipients subject to Directive 95/46 (based on Article 8), (iii) or other types of recipients (based on Article 9).

According to the Notification the transfer of the information is limited to (i) DG BUDGET to execute the payment of amounts due via the EU staff members' bank account, (ii) PMO Salaries to recover from salaries amounts that were advanced in the context of hospitalisation, and (iii) the Medical Council, Management Committee and Unit ADMIN.B.2 in the context of appeals.

All transfers are made within or to Community institutions or bodies, thus, Article 7 of the Regulation applies. No data transfers are made to recipients subject to Directive 95/46 or to other types of recipients; therefore, Articles 8 and 9 of the Regulation do not apply.

Article 7 of Regulation (EC) No 45/2001 requires 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.

[7] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Adminmeasures/07-02-26_conservation_documents_medicaux_EN.pdf

The EDPS considers that the transfers of information to DG BUDGET and to PMO Salaries for the purposes stated above comply with these requirements. In both cases, the recipients have the competence to perform the task assignment for which the data is transferred, i.e. to execute the payment of amounts due via the EU staff members' bank account and to recover from salaries the amounts that were advanced in the context of hospitalisations. Also, in both cases, the data transfers are necessary for the addressees to perform their tasks. This is provided that the data sent to DG BUDGET and PMO salaries are limited to what is strictly necessary for the performance of their tasks. In both cases, the type of information to be transferred should be limited to identification information of the EU staff member, bank account information and salary information. No health related data should be transferred to PMO and DG BUDGET because such information is not necessary for the performance of their tasks.

Transfers of personal information may also take place to the Management Committee to the Medical Council and to DG ADM B 3 in the context of the appeals procedure foreseen by Article 90(2) of the Staff Regulation. The transfer of information to the Management Committee is foreseen in Article 16 of the Joint Rules on Sickness Insurance which establishes that the appointing authority must ask for the Management Committee's opinion before ruling on a complaint. It further establishes that the Management Committee can seek external advice. In this context, the Management Committee can also consult the Medical Council.

In order to issue an opinion, both the Management Committee and the Medical Council need to have a complete description of the facts. In this regard, the EDPS considers that Article 7 is complied with because the recipients of the information need to receive such information in order to perform the tasks for which they are competent. However, the EDPS questions whether the Management Committee need to have access to identification information in order to carry out its tasks. The transmission of identification information to persons who are not medical practitioners does not appear to be necessary to issue an opinion on procedural and administrative issues. At the same time, transmission of sensitive information, for example, information that an EU staff member is suffering from cancer or mental illness may deter submission for appeal of legitimate claims. The EDPS is aware that by not knowing the identity of the patient, theoretically members of the Management Committee may fail to identify potential conflicts of interest (for example, if the matter under their consideration is related to a family member of one of the Management Committees' members). On the other hand, in such cases, the member of the Management Committee would be likely to identify the patient, even without identification information.

In the light of the reasoning described above, the EDPS suggests that PMO.3 remove identifying information regarding the claimant before asking the Management Committee for an opinion under Article 16 of the Joint Rules on Sickness Insurance.

2.2.7. Right of access and rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to their source.

The privacy statement confirms that PMO.3 provides access to personal information. It further establishes the arrangements in this respect. The EDPS welcomes that PMO 3 allows access to the EU staff member's 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. Members 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 constraints, it may be appropriate to establish reasonable time limits.

The EDPS calls the attention of PMO.3 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[8].

Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data. This means that the insured party should be able to request that opinions by another medical officer or a Court decision are placed in his file so as to ensure that the files are accurate and complete. The EDPS urges the PMO to put in place appropriate procedures allowing insured parties to exercise the right of rectification.

2.2.8. Information to the data subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals 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.

In order to ensure compliance with these Articles, the EDPS was informed of the existence of a privacy statement made available to EU staff members through the Commission's intranet, in the section that deals with sickness insurance.

The EDPS accessed the intranet in order to verify whether the privacy statement is easily available to individuals who access the site to download the forms where information has to be filled in. The privacy statements are available in the first section which provides an introduction to the Sickness Insurance Scheme. Although the EDPS finds it appropriate to include the privacy statement in this section, this may not be sufficient. Individuals downloading the forms where information has to be filled in may bypass the first page and therefore miss the web page where the privacy statement is made available. For this reason, the EDPS suggests including a link to the privacy policy in the pages where the forms are available for downloading. This will provide direct access to the privacy statement from the web page where the EU staff member has to go through in order to download the form. In addition, inserting in the forms themselves the URL where the privacy policy is available would also contribute to the compliance with the information principle and transparency.

---

[8] 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."*

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001.

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. The EDPS considers that the privacy statement contains most of the information required under Articles 11 and 12 of the Regulation, however, he considers that several amendments would contribute to ensure full compliance with Articles 11 and 12, in particular:

(i) There is no reference to the fact that the data undergo automatic processing. The EDPS considers that to ensure the fair processing of information, the privacy statement should indicate that the information provided to the PMO is introduced into an electronic database. This is necessary taking into account that EU staff members are asked to send the information in paper form, thus, nothing indicates to EU staff members that the information they send are kept in 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 EU staff members could send questions regarding the privacy statement.
(iii) There is no reference to the right of rectification and the procedure to exercise it; this right should be added to the privacy statement.
(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.

2.2.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must 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 prevent all other forms of unlawful processing.

The EDPS considers that the security measures adopted by PMO.3 are adequate in the light of Article 22 of the Regulation. A described under Section 2.2.4, the EDPS finds it a good practice and an appropriate measure for ensuring the confidentiality of information, to use sealed envelopes marked 'confidential', 'to be opened by addressee only' or similar for the transmission of medical information. Furthermore, the EDPS considers that it would also be appropriate to retain log files in order to keep track of access (and detect unauthorized access) to ASSMAL.

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 non-medical PMO.3 staff regarding medical secrecy. This should include training and signing a specific confidentiality declaration.

- In order to ensure that inadequate, irrelevant and 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 the basis for prior authorisation to medical doctors, as is presently done for requests for recognition of serious illness.
- Instruct EU staff members to send medical reports that support requests for recognition of serious illness and requests for prior authorisation in sealed envelopes marked with the terms 'confidential' and/or 'to be opened by addressee only'. These instructions should be given in the website that deals with the Sickness Insurance Scheme.
- Modify the confidential information form as suggested in this Opinion.
- Ensure that access to medical reports contained in ASSMAL is limited to medical officers.
- Reassess the necessary conservation period for data related to medical conditions. 30 years should be an absolute maximum, for both paper and electronically stored data.
- Ensure that the retention periods for the information stored in the electronic database are the same as the paper based information.
- In the on-going efforts to develop a new version of ASSMAL, it should be taken into account that the system should be elaborated in a way that permits the deletion of information with the time limits set up above.
- Ensure that no health related data is transferred to PMO Salaries and DG BUDGET because such information is not necessary for the performance of their tasks.
- Limit the transfer of information to the Management of Committee in the context of the appeals *ex* Article 90 of the Staff Regulations. In particular, the EDPS recommends removing identification information as it is unnecessary in order for the Committee to provide its reports.
- Insert a link to the privacy policy 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.
- Establish reasonable time limits for dealing with requests from data subjects exercising their right of access and foresee a procedure to exercise the right of rectification.
- Ensure that medical reports that contain confidential information are always transferred in sealed envelopes marked 'confidential' or 'for the addressee only'.
- Retain log files in order to keep track of access (and detect unauthorized access) to ASSMAL.

Done at Brussels, 10 July 2007

Peter HUSTINX
European Data Protection Supervisor