Opinion on the notification for prior checking from the European Investment Bank relating to procedures regarding the administrative management of medical expenses

Brussels, 6 April 2005 (Case 2004-305)

Procedure

Notification within the meaning of Article 27(3) of Regulation (EC) No 45/2001 was given by Mr Jean-Philippe MINNAERT, Data Protection Officer of the European Investment Bank, by letter dated 10 February 2005.

Facts

The staff responsible for the Health Insurance Scheme (HIS) must reimburse medical expenses in accordance with the provisions set out in Annex II to the Bank's Staff Rules.

The member provides the HIS staff with a statement of expenses form setting out the number of enclosures and the total amounts by heading (consultation, dentistry, hospitalisation, corrective glasses, tests/X-rays and physiotherapy). The original statements of fees must be attached. Each statement of fees is entered into the computer system on one or more lines. In the event of hospitalisation, a letter agreeing to direct billing of hospitalisation costs may be issued. In that case, the hospital sends its invoices to the HIS staff, which pays them directly.

The data are entered in several stages: first the personnel number of the staff member involved is keyed in; the personal circumstances of that member then appear on screen (name of each family member and mention of whether they have primary or supplementary HIS cover).

Each item of medical treatment is entered as a code (e.g. FM0107 for consultations, DI0102 for tests, DI0104 for X-rays, etc.), together with the date and relevant amount. The amount to be reimbursed then appears automatically on screen.

As regards the payment procedure, all lists relating to payment are generated and printed exclusively by HIS managers. The process comprises several steps:

- identification of all amounts to be paid;
- preparation of a list showing the payment amounts (identification report);
- verification of the list by HIS managers. A human resource manager then signs off the payment on the last page containing the total amounts;
- electronic transfer of amounts to be paid through the S-Multiline payment system of the *Banque et Caisse d'Epargne de l'Etat* in Luxembourg;
- print-out of a list of benefits pending;

- duplicate print-out of statements: one copy is automatically put in an envelope marked "confidential" and sent to the relevant staff members or retired staff members, the other is filed in the HIS file of the relevant staff members with the corresponding supporting documents. These files are kept under lock and key in the HIS offices for two years (current year and previous year) and are then sent to the Bank's central archives. The retention period of these medical files (on hard copy) is ten years.

A memorandum signed by the official in charge of the Human Resources/Administration Division is sent to the accounts department, mentioning the total amount of reimbursements, the amount of advance payments on submission of statement of expenses forms, the amount of advance payments for hospitalisation fees and the amount of the transfer sent to the *Banque et Caisse d'Epargne de l'Etat*. Copies of the page signed off for payment and of the statement of expenses forms are attached.

The data are of a medical nature and are mostly given in the form of codes: They include:

- the name and forename of the staff member;
- the staff member's personnel number;
- the nature of the expenses: consultations, medicines, dentistry, hospitalisation, corrective glasses, X-rays/tests or physiotherapy;
- the date of the services;
- the name and forename of the patient (if spouse or child);
- the amount of the expenses.

The information on data retention is as follows:

Administrative medical files containing data on the reimbursement of medical expenses together with the HIS statements and supporting documents are kept for a total period of ten years (two years in the HIS offices – current year and previous year –, then in the Bank's central archives). Only the HIS managers and staff involved have access to these files.

Letters agreeing to direct billing of hospitalisation costs are kept in the Bank's central archives for five years.

- *Print-outs of HIS payments are kept in the Bank's central archives for ten years.*

- *The computer data contained in databases (expenses entered and reimbursements) are kept for three to four years, depending on the type of treatment.*

A medical file for each staff member is kept by the European Commission Medical Service (that file contains the reports and test results relating to the annual medical examination, preventive medicine and any opinions issued by the Medical Officer in relation to the person involved).

Legal aspects

1. Prior checking

The notification received by e-mail on 10 February 2005 relates to processing of personal data ("any information relating to an identified or identifiable natural person" – Article 2(a)) and therefore falls within the scope of Regulation (EC) No 45/2001.

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

Processing is also subject to the provisions of Article 27(2)(a): "The following processing operations are likely to present such risks: processing of data relating to health …", which is the case here.

The notification from the European Investment Bank's Data Protection Officer was received by e-mail on 10 February 2005. The European Data Protection Supervisor therefore had to deliver his opinion by 10 April 2005 at the latest, as laid down in Article 27(4) of the Regulation.

2. Legal basis and lawfulness of the processing operation

Under its Statute, the European Investment Bank enjoys autonomy of decision-making within the Community institutional system. Pursuant to Article 29 of the Bank's Rules of Procedure, the Administrative Board adopts regulations concerning staff. The Staff Regulations lay down the general conditions governing the employment of staff.

In the case in point, the legal basis for the processing operation derives from the regulations governing the Bank's relations with its staff and the institution's Staff Rules and Staff Pension Scheme Regulations.

The Staff Pension Scheme Regulations were established by the European Investment Bank's Board of Directors in accordance with Article 36 of the Staff Regulations.

Alongside the legal basis in relation to Regulation (EC) No 45/2001, the lawfulness of the processing operation must also be considered. Article 5(a) of Regulation (EC) No 45/2001 stipulates that the processing must be "*necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities … or in the legitimate exercise of official authority vested in the Community institution"*. The reimbursement of medical expenses administered by the European Investment Bank's Health Insurance Scheme to the Bank's staff and retired staff and their dependants is part of the legitimate exercise of official authority vested in the institution and is necessary for the management of health services. The processing operation is therefore lawful.

Lastly, in the framework of the reimbursement of medical expenses, the file of the data subject may reveal data which Article 10 of Regulation (EC) No 45/2001 classes as "special categories of data". Data concerning health may come to light in the file.

Likewise, Article 10(2)(b) (whereby the provision that "*the processing of … data concerning health … [is] prohibited"* shall not apply where "*processing is necessary for the purposes of*

complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof …") applies in the case in point. The European Investment Bank, in its capacity as employer, is complying with Article 10(2)(b) by processing the data submitted.

Lastly, in the case in point, certain data (relating to the HIS in particular) are forwarded – in an envelope marked "confidential" – to the Medical or Dental Officer. Owing to the nature of the data involved, which concern health, Article 10(3) (special categories of data) of Regulation (EC) No 45/2001, which lays down that: "*Paragraph 1* [("*the processing of … data concerning health … [is] prohibited*")] *shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*", applies in the case in point. On account of their positions, the Commission Medical and Dental Officers (who compensate for the lack of a medical officer within the European Investment Bank) are subject to the obligation of professional secrecy and are the sole recipients of these data. In this instance, Article 10(3) of the Regulation is duly complied with.

For the same reason, it should be emphasised that persons dealing with administrative dossiers who are not health practitioners must be subject to an" equivalent obligation of secrecy".

The European Data Protection Supervisor recommends that the staff mentioned above be informed that they are subject to the obligation of secrecy.

3. Collection and transfer of data

Use of the official's personnel number means that certain data are taken from staff databases. The processing operation being reviewed involves no general change of the specified purpose of staff databases and is not incompatible with that purpose. Accordingly, Article 6(1) of Regulation (EC) No 45/2001 is not applicable to the case in point and the conditions of Article 4(1)(b) of the Regulation are fulfilled.

The European Investment Bank uses the personnel number. While the use of an identifier is, in itself, no more than a means (and a legitimate one in this case) of facilitating the task of the personal data controller, its effects may nevertheless be significant. This was why the European legislator decided to regulate the use of identifying numbers in Article 10(6) of the Regulation, which makes provision for action by the European Data Protection Supervisor. In the case in point, use of the personnel number may allow the linkage of data processed in different contexts. The point here is not to establish the conditions under which the European Investment Bank may process the personnel number, but rather to draw attention to that provision of the Regulation. In this instance, the European Investment Bank's use of the personnel number is reasonable because it is a means of facilitating the processing operation.

The processing operation should also be scrutinised in the light of Article 7(1) of Regulation (EC) No 45/2001. The processing covered by Article 7(1) is the transfer of personal data within or to other Community institutions or bodies "*if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient*".

The case in point concerns transfers within the same institution (Health Insurance Scheme, human resources, bank transfers, staff concerned, accounts department, central archives). It also concerns transfers between institutions since the medical file of each staff member is kept by the European Commission Medical Service, which, as the European Investment Bank has no medical service, also handles medical examinations prior to recruitment, annual medical check-ups and expert medical opinions.

Care should therefore be taken to ensure that the conditions of Article 7(1) are fulfilled; that is the case since the data collected are necessary for carrying out the processing and, furthermore, are "*necessary for the legitimate performance of tasks covered by the competence of the recipient*". In this case, the task is the responsibility of the European Commission and Article 7(1) is therefore duly complied with.

4. Data retention

Article 4(1)(e) of Regulation (EC) No 45/2001 lays down the principle that data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*".

Data are subject to long-term retention after having fulfilled their purpose (reimbursement of medical expenses under the Health Insurance Scheme):

- ten years in the case of administrative medical files containing data on the reimbursement of medical expenses and of the print-outs of HIS payments;
- five years in the case of letters agreeing to direct billing of hospitalisation costs;
- three to four years in the case of computer data contained in databases.

The ten-year period for the retention of administrative medical files and print-outs of HIS payments is mentioned in the procedures manual of the Human Resources Department, which is available on the European Investment Bank's intranet. So is the five-year period – which does not seem unreasonable – for letters agreeing to direct billing of hospitalisation costs.

There is no formal basis for the three- and four-year periods, but they are shorter than the ten-year period already in use; this appears to be reasonable in the light of Article 4(1)(e).

The notification excludes the possibility of storing data for historical, statistical or scientific reasons.

Nonetheless, the long-term retention of data should be accompanied by appropriate safeguards. The European Data Protection Supervisor recommends that appropriate safeguards be established regarding use of these data once medical expenses have been reimbursed.

5. Information for data subjects

The notification states that the data subjects, in this instance the staff of the European Investment Bank, are informed by means of the Staff Rules, the Human Resources intranet page and internal memoranda.

The provisions of Article 11 on information to be given to the data subject apply in this case. The provisions set out in subparagraphs (a) (identity of the controller), (b) (purposes of the

processing operation), (c) (recipients or categories of recipients of the data) and (d) (whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply) are indeed complied with.

However, there is no mention in either the notification or its annex (arrangements governing reimbursement of medical expenses by the Health Insurance Scheme) of the following possibilities: subparagraph (e) ("*the existence of the right of access to, and the right to rectify, the data concerning him or her*") and subparagraph (f) of the same Article which refers to information that is not compulsory *(legal basis for the processing operation, time-limits for storing the data, right to have recourse at any time to the European Data Protection Supervisor)*. This information – in particular the information referred to in subparagraph (e), which is compulsory – must be supplied to the person to be informed.

In view of these considerations, the European Data Protection Supervisor requests that the compulsory information ("*the existence of the right of access to, and the right to rectify, the data concerning him or her*"), as well as the information referred to in Article 11(1)(f) of the Regulation, be mentioned in every information medium (Staff Rules, the Human Resources intranet page, internal memoranda, etc.) and through any other appropriate means.

6. Right of access

Article 13 of Regulation (EC) No 45/2001 makes provision, and sets out the rules, for right of access at the request of the data subject. The notification makes no mention of staff members' entitlement to have access to their file.

The European Data Protection Supervisor requests that the provisions of Article 13 be complied with.

7. Data quality

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

Furthermore, the data must be *processed fairly and lawfully* (Article 4(1)(a) of Regulation (EC) No 45/2001). The matter of lawfulness has been reviewed above. Given the sensitivity of the subject, fairness is an issue which warrants considerable attention. It is linked to the information to be given to the data subject (see section 5 above).

Lastly, the data must be "*accurate and, where necessary, kept up to date; 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*" (Article 4(1)(d) of the Regulation). There does not appear to be any mention of rules concerning staff members' right to have data updated.

The European Data Protection Supervisor requests that the right of staff members to rectify their personal data be guaranteed.

8. Security

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

The security measures set out in the notification and the information subsequently received appear to be relatively adequate for the processing of sensitive data.

The notification states that only a very limited number of persons have access to each file. The accounts department, which reimburses the expenses, does not have access to medical data. File access must be restricted to authorised persons, with a distinction being made between strictly medical data and data relating to reimbursement of expenses.

The European Data Protection Supervisor requests that the two points set out above be expressly implemented and/or guaranteed.

Conclusion

There is no reason to believe there is a breach of the provisions of Regulation (EC) No 45/2001, providing that the following considerations are fully taken into account. This implies, in particular, that those responsible for the Health Insurance Scheme of the European Investment Bank should:

- inform staff handling files of their professional secrecy obligations;
- ensure that the long-term retention of data is accompanied by appropriate safeguards. The European Data Protection Supervisor recommends that appropriate safeguards be established regarding use of these data once medical expenses have been reimbursed;
- supply compulsory information ("*the existence of the right of access to, and the right to rectify, the data concerning him or her*"), together with information on the legal basis for the processing operation and the right to have recourse to the European Data Protection Supervisor, in the Staff Rules, on the Human Resources intranet page, in internal memoranda and through any other appropriate means.
- guarantee the right of access provided for by Article 13 of the Regulation;
- guarantee the right of all staff members to rectify personal data contained in their files;
- restrict file access to authorised persons, making a distinction between strictly medical data and data relating to reimbursement of expenses.

Brussels, 6 April 2005

Peter HUSTINX
European Data Protection Supervisor

Follow-up Note 6 November 2006

All acting measures have been taken on 27 October 2006.

The European Data Protection Supervisor