Opinion on the notification for prior checking from the Data Protection Officer of the European Investment Bank regarding the partial subcontracting of the Bank's Health Insurance Scheme

Brussels, 16 September 2008 (Case 2008-323)

1. Procedure

On 27 May 2008, a notification for prior checking was sent by the Data Protection Officer (DPO) of the European Investment Bank to the European Data Protection Supervisor (EDPS) in relation to the partial subcontracting of the Bank's Health Insurance Scheme.

A number of questions were put to the DPO in an e-mail dated 20 June 2008. Answers were given on 7 July 2008. Additional questions were put on 10 July and the answers were given on 11 July. The opinion was sent to the DPO for comments on 9 September 2008. The comments were received on 15 September 2008.

2. The facts

The Bank decided to subcontract part of its Health Insurance Scheme (HIS). The chosen subcontractor, GMC (Garantie Médicale et Chirurgicale) of the Henner Group, is a French company registered with the French Data Protection Authority (CNIL).

Purpose: the purpose of the partial subcontracting is to give members the choice of continuing to submit their medical expenses to the Bank's own HIS[1] or of submitting their medical expenses to an external service provider: the reimbursement rates are the same in both cases but with the advantage in the latter case of swifter reimbursement and anonymity vis-à-vis the EIB in the electronic processing of data. The member will be able to rejoin the internal HIS but only once. In addition to ensuring compliance with the applicable legal, regulatory and administrative provisions, the subcontractor enters data, creates, classifies and archives files, pays reimbursements by bank transfer, draws up letters agreeing to direct billing of hospitalisation costs and provides the EIB's HIS with the necessary accounting figures.

Description of the category or categories of data subject: the procedure potentially concerns serving and retired members of staff and their dependants with primary or secondary HIS cover.

Description of the data or categories of data: if a member opts for the subcontractor, he has to complete a form with all the data required for the processing of his file (personnel number, date

[1] This has already been the subject of an opinion of the EDPS. See Opinion 2004-305 of 6 April 2005 on the EDPS website.

of birth, status as serving or retired official, date of entry into service, address, dependants and whether they have primary or supplementary cover, bank account number). The EIB's Human Resources Department is responsible for informing GMC of any changes in membership circumstances. In certain cases, the EIB's HIS has to provide GMC with file histories (e.g. in the case of glasses, orthodontist treatment, etc.) to enable GMC to reimburse the amounts authorised under the HIS's reimbursement ceilings within the time limits.

Information to data subjects: the rules governing reimbursement by the HIS are set out in Administrative Provisions, on the Intranet (Human Resources page) and in Service Notes. Information sessions for staff have been organised. The Human Resources department will publish a list of frequently asked questions, together with answers, on the Intranet. A member opting for the subcontractor must fill in and sign a form. The form includes a data protection clause[2].

Procedures safeguarding the data subjects' rights: the data are stored by GMC, which is registered with the French data protection authority (CNIL). For members opting for GMC, the same healthcare reimbursement rules apply but they can also keep track of their file and the procedures to be followed on the GMC website by means of a username and personal password. The form referred to in the previous point also mentions their right of access, opposition and rectification. In the interests of confidentiality, all consultations of dossiers in situ, on the GMC site, are carried out in the presence of authorised staff from the General Services Department.

Procedures for automated/manual processing: members who opt for the subcontractor can submit expenses to GMC electronically and send on the original documents later. Once the claims have been processed, GMC sends the member a reimbursement statement, either electronically or by post at the member's choice.

GMC has its own database and in no case can it connect to the Bank's internal servers. The data concerning EIB staff and their family members are those provided by the staff themselves on the membership request form upon joining GMC. The personal data are processed in Paris. No processing operations are carried out within the EIB itself.

Data storage medium: The data storage information supplied by GMC is essentially as follows:

1. The backup system architecture enables the entire content of the Group's servers (in Paris and the provinces) to be backed up and simplifies the management and

[2] These questions must be answered to join the healthcare reimbursement scheme of the European Investment Bank which is managed by GMC Services (GMC). The data are intended for GMC Services and GMC Gestion as the controllers, and for the European Investment Bank, solely for the purposes of managing your insurance and shall be processed in accordance with French Law No 78-17 transposing Directive (EC) 95/46 of 24 October 1995. They may be transferred to healthcare establishments abroad for the purposes of reimbursing healthcare received by you there. The transfer will be made only at your request and in your interests and solely where necessary for the operation of the healthcare reimbursement scheme. The data are intended to be kept while reimbursement is being processed and until all sums due have been paid in full. They may be stored in accordance with the applicable limitation rules and for the periods necessary to prepare statistics and control statements. You have a right to access, contest and rectify, which may be exercised at 10 rue Henner 75009 Paris; or by e-mail at info@henner.com. You may also have recourse to the European Data Protection Supervisor, rue Wiertz 60, MO 63 B-1047 Brussels, in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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, as well as to the French data protection authority (CNIL), 8 rue Vivienne, CS 30223, 75083 Paris Cedex 02, in accordance with French Law No 78-17 (the Data Processing and Freedoms Law).

monitoring of backup reports. The backup software uses advanced functions such as compression and time navigation to search more quickly for the data to be restored. It utilises a database containing all the information required for the management of tapes and rolls. The database is also backed up to tape every day.

2. The data to be backed up are distributed among a number of domains. A backup policy is applied to each of these domains, specifying:
    - the duration for which data are retained in the backup library,
    - the type of backup:
        - complete (all data),
        - complete incremental (rebuilding data from incremental backups),
        - incremental (backing up the differences between two backups).

The processing applications are based on software programmes (9 in all), comprising management applications, applications for statistical purposes, bank reconciliation software, general accounting and cash-flow monitoring software, and software for setting up new contracts (linking sales with management), for storing members' user names and passwords for Internet access, for making available to members 2 years' history of their statements and, lastly, for entering data on the basis of which direct billing can be authorised.

Processor: a contract was signed in April 2008 with GMC and the European Investment Bank, including the following clauses:

1. Article 7 – Data protection

Without prejudice to § 11 of the General Terms and Conditions, the Service Provider guarantees that the Bank will not, at any time, as a direct or indirect result of any act or omission by the Service Provider, be in breach of its obligations under Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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.

The Service Provider undertakes to comply with all requirements arising from conditions imposed on the Bank by the European Data Protection Supervisor (EDPS).

2. § 11. of Appendix C to the contract: Confidentiality and data protection

The Consultant shall treat as confidential all information which he receives, from the Bank or from any other person, while providing his services. The abovementioned obligation of confidentiality shall not apply, however, to any information which the Consultant was in possession of before commencing his services, or which subsequently entered the public domain, other than as a result of illegal disclosure by the Consultant. The Consultant shall not publicise his association with the Bank, or the existence or the terms of the contract, without the Bank's prior written permission.

The Consultant shall comply with the relevant provisions of Community legislation on the protection of personal data, especially Regulation (EC) No 45/2001 of 18 December 2000, and with the provisions of relevant national legislation implementing Directive No 95/46/EC of 24 October 1995. The Consultant shall obtain, from each of his employees assigned to the project and, if necessary, from each subcontractor, a written undertaking (Annex 3) which he shall return to the Bank, duly approved and signed.

3. Annex 3 to the contract concluded between GMC and the EIB concerning data protection rules

Annex 3 to the contract concerns the rules governing data protection. It sets out all the provisions on data protection applicable to all the Contractor's staff working on the subcontracted project. Staff is reminded of the obligation of confidentiality and non-disclosure and of the obligation to refrain from copying or transmitting data. The attention of staff is drawn to the fact that if they violate the abovementioned rules on confidentiality they may be held personally liable and the EIB may institute proceedings against them. The EIB requests that a copy of this Annex, duly approved by the undersigned and countersigned by the Contractor's legal representative, be sent to it by return.

Legal basis and lawfulness of the processing operation: the Staff Regulations; the Administrative Provisions; the Staff Pension Scheme Regulations; the contract between the EIB and GMC; the Management Committee decision.

Recipients to whom the data might be disclosed: certain data from the Health Insurance Scheme are disclosed to the Medical or Dental Officer. Files relating to serious illnesses, loss of independence, cures or reimbursement for certain medicines, and files requiring opinions, are submitted to the Medical Officer. Dental and orthodontic estimates are submitted to the Dental Officer. Where one of the Medical Officers' opinion is required on a file processed by GMC, the latter sends the file directly to the Medical Officer – not via the Health Insurance Scheme – in an envelope marked "strictly confidential".

Personal data retention policy: GMC is required to adhere to the same data retention periods as the Health Insurance Scheme (10 years). GMC has drawn up a note containing information on the retention period, the archiving method, archiving requests and requests to consult the archives.

Measures taken to ensure security of processing: [...]

IT security measures are covered in Annex 2 to the contract concluded between the EIB and GMC. [...]

3. Legal aspects

3.1. Prior checking

The notification received on 27 May 2008 relates to processing of personal data ("any information relating to an identified or identifiable natural person" – Article 2(a)). The data processing in question is carried out by an institution in the exercise of activities which fall within the scope of Community law (Article 3(1)). The processing is partly automated and reimbursement files are archived in paper copies intended to form part of a filing system. Article 3(2) is thus applicable in this case.

This processing therefore falls within the scope of Regulation (EC) 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. The processing operation is also covered by the provisions of Article 27(2)(a): "The following

processing operations are likely to present such risks: … processing of data relating to health …", which is the case here, since it concerns the reimbursement of healthcare, and is therefore subject to prior checking by the EDPS.

In principle, checks by the EDPS should be performed before the processing operation is implemented. In this case, where the contract was signed in April 2008, the EDPS regrets that this processing operation was not submitted to him before being put in place. The checking therefore necessarily becomes ex post. This does not make it any the less desirable that the recommendations issued by the EDPS be implemented.

The formal notification was received through the post on 27 May 2008. A number of questions were put to the DPO in an e-mail dated 20 June 2008. Answers were given on 7 July 2008. Additional questions were put on 10 July and the answers were given on 11 July. In accordance with Article 27(4) of the Regulation, the two-month period within which the EDPS must deliver an opinion was suspended. The opinion was sent to the DPO for comments on 9 September 2008. The comments were received on 15 September 2008. The EDPS will therefore deliver its opinion no later than 22 September 2008, since the 21st is a Sunday (28 July + the 24-day suspension + the month of August).

3.2. Lawfulness of the processing operation

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 other legal instruments adopted on the basis thereof 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.

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.

The legal basis for this processing operation derives from the regulations governing the institution's relations with its staff, the Administrative Provisions, the Staff Pension Scheme Regulations, the contract between the EIB and GMC and the Management Committee decision.

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

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

Lastly, in the context of the reimbursement of medical expenses, the data subject's file 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.

3.3. Processing of special categories of data

Under Article 10 of Regulation (EC) No 45/2001, the processing of personal data concerning health is prohibited unless it is justified on the grounds provided for in Article 10(2) and (3) of the Regulation. The present case very clearly relates to the processing of personal data on health.

Article 10(2)(b) applies to the present case: "Paragraph 1 (prohibiting the processing of data concerning health) 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 …". The European Investment Bank, in its capacity as employer, is complying with Article 10(2)(b) by processing the data submitted.

On account of their profession, the European Investment Bank's Medical and Dental Officers are subject to the obligation of professional secrecy and should be the sole recipients of these data. In this case, Article 10(3), which states 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*", has been complied with.

For the same reason, it should be emphasised that persons dealing with administrative files who are not health practitioners must be subject to an "equivalent obligation of secrecy". This evidently applies to all GMC staff whose duties involve processing healthcare reimbursement files. The European Data Protection Supervisor welcomes the fact that the EIB has laid down a specific confidentiality clause to be complied with by GMC's staff, in particular by establishing a specific Annex to the contract which must be signed by each GMC staff member whose duties involve processing EIB healthcare reimbursement files.

3.4. The controller and the processor

Pursuant to Article 2(d) of the Regulation, the controller is "the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data". The controller is responsible for ensuring that the obligations provided for in the Regulation are met (on information to be given to the data subject, ensuring the rights of the person concerned, the choice of processor, notification of the data protection officer, etc.). The processor is the "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (Article 2(e)).

Under Regulation (EC) No 45/2001, the EIB must be considered to be the controller in this case, in the context of the partial subcontracting of the Bank's Health Insurance Scheme.

The contractor (GMC) for the processing of healthcare reimbursements is considered as a processor when carrying out the tasks specified in its contract with the EIB.

The role of the processor, as such, is to assist the EIB with the reimbursement of healthcare for any EIB staff who so choose. Article 2(e) of the Regulation is therefore applicable.

Consequently, the statement "*(…) The data are intended for GMC Services and GMC Gestion as the controllers, and for the European Investment Bank, solely for the purposes of managing your insurance and will be processed in accordance with French Law No 78-17 transposing Directive (EC) 95/46 of 24 October 1995 (…)*" at the bottom of the form is inaccurate. GMC Services and GMC Gestion are processors acting on behalf of the EIB, on the basis of a contract concluded on 8 April 2008[3].

The EDPS recommends that this statement, on the healthcare reimbursement form to be returned by the data subject to GMC Services, be corrected.

3.5. 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. The EDPS considers that Article 4(1)(c) of Regulation (EC) No 45/2001 has been complied with in this respect.

Furthermore, the data must be *processed fairly and lawfully* (Article 4(1)(a) of Regulation (EC) No 45/2001). The question of lawfulness has already been considered (see section 3.2 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 3.9 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). The system itself also helps to ensure that data are accurate and up-to-date, since the data subject himself supplies the data which are processed. Moreover, the data subject has the right to access and rectify data, which helps ensure that they are kept up-to-date and that the file is as complete as possible. This is a second way of ensuring the quality of data. See point 3.8 below on the dual rights of access and rectification.

3.6. 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*".

In this respect, GMC applies the same retention period as the EIB in connection with the same processing operation[4]; the recommendations on this point apply in the same way to both. The system's backup architecture enables data to be retained in secured form.

However, the processing applications are based on the software programmes (9 in all) comprising management applications, applications for statistical purposes, etc. These applications must fulfil the conditions laid down in Article 4(1)(e) of Regulation 45/2001 ("*The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or*

---

[3] "*We refer to the above contract governing the assignment which your staff is due to undertake* ***on behalf of the Bank's*** *SG-JU-RH-RH/ADM Department under the health project*".

[4] See Opinion 2004-305 of 6 April 2005 on the EDPS website.

scientific purposes."). The EDPS therefore recommends that these data be anonymised or encrypted.

3.7. Transfer of data

Here, the question arises as to how transfers between GMC and the EIB should be considered. There are two situations in which a transfer of data can occur:

1. when accounting data are transferred – in this case, if the data are anonymised, no personal data are transferred;
2. when Medical Officers are asked to provide an opinion. Where one of the Medical Officers' opinion is required on a file processed by GMC, the latter sends the file directly to the Medical Officer – not via the Health Insurance Scheme – in an envelope marked "strictly confidential".

Such processing needs to be examined in the light of Article 8 ("*Transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC*"), with GMC acting on behalf of the EIB. In this case, such transfers are covered by Article 8(a), since "*the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority*", as the processor of the data. At present the processor is subject to the obligations laid down by Directive 95/46/EC.

3.8. Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 establishes a right of access – and the arrangements for exercising it – upon request by the data subject. Article 14 of Regulation (EC) No 45/2001 establishes the data subject's right of rectification. In the same way that the data subject has a right of access, he or she may also directly change personal data or have them changed, if necessary.

For the record, the rights of data subjects are guaranteed directly by the processor, which explicitly mentions the two options on its reimbursement form. For members opting for GMC, the same rules apply but they can also keep track of their file, and of the procedures to be followed, on the GMC Intranet website by means of a username and personal password.

Articles 13 and 14 of the Regulation have therefore been complied with.

3.9. Information to be given to the data subject

The notification states that the data subjects, in this instance the staff of the European Investment Bank, are informed by means of the Administrative Provisions, the Human Resources website and Service Notes. Information sessions for staff have been organised. The Human Resources department will publish a list of frequently asked questions, together with answers, on the Intranet.

The provisions of Article 11 on information to be given to the data subject are applicable in this case, and have been complied with, since the recommendations made by the EDPS concerning dossier 2004-305[5] have been implemented by the EIB. GMC, on its reimbursement form[6] , also sets out the information required by the data subject.

[5] See footnote 1.
[6] See footnote 2.

3.10. Processing of personal data on behalf of controllers

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

In this case the EIB has complied with its obligation, since the terms of reference of the invitation to tender require the contractor to ensure the confidentiality of personal data processed by the contractor for the sole purpose of fulfilling the framework contract, in accordance with the provisions of Regulation (EC) No 45/2001. This requirement is stipulated in the contract.

Reference must also be made to Article 23(2)(b) of Regulation (EC) No 45/2001, on the processing of personal data on behalf of controllers. The processor refers explicitly to the provisions concerning confidentiality and security measures set out in Articles 16 and 17(3) of Directive 95/46/EC. The processor refers explicitly to French Law No 78-17 transposing Directive 95/46/EC.

3.11. Security

Under Article 22 of Regulation (EC) No 45/2001 on the 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 EDPS considers that the full set of security measures and the other organisational and technical measures taken by both the controller and the processor, in particular as set out in Annex 2 to the contract, to ensure maximum processing security are such that they can be regarded as adequate within the meaning of Article 22 of Regulation (EC) No 45/2001.

Conclusion

The proposed processing operation does not appear to infringe the provisions of Regulation (EC) No 45/2001, subject to the comments made above. This implies, in particular, that the Health Insurance Scheme of the European Investment Bank should require the processor to implement the following recommendations:

- that the reference, on the healthcare reimbursement form to be returned by the data subject to GMC Services, to "*controllers*" be corrected;
- that data which may be included in statistics be anonymised or encrypted.

Done at Brussels, 16 September 2008

(Signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor