Opinion on the notification for prior checking from the Data Protection Officer (DPO) of the European Parliament regarding the REMEDE dossier

Brussels, 14 November 2006 (Case 2006-301)

1. Procedure

Notification within the meaning of Article 27(3) of Regulation (EC) No 45/2001 concerning the REMEDE dossier (2006-301) was sent on 19 June 2006 to the European Data Protection Supervisor (EDPS) by the Data Protection Officer (DPO) of the European Parliament.

Since the "REMEDE" processing operation is already in place, it cannot be subject to prior checking and must therefore be checked "ex-post".

The EDPS identified certain priority topics and selected a number of processing operations subject to prior checking ex-post that required notification. These included processing operations relating to medical data.

On 6 July 2006 the EDPS requested further information on the processing operation in question. An answer was given on 28 September 2006. On 8 November 2006, the EDPS extended the time limit for delivering his opinion by 7 days to enable the DPO to forward his comments and to provide any additional information. Comments were forwarded on 10 November 2006.

2. Examination of the case

2.1. The facts

The processing operation under review concerns the administration of reimbursements of the medical expenses of Members of the European Parliament and their families. The data subjects are therefore MEPs and members of their families (spouse or stable non-marital partner and dependent children).

The legal basis for the REMEDE processing operation is to be found in the rules on the expenses and allowances of Members of the European Parliament, specifically Article 21, supplemented by Annex IV.

The data processed are the following: the personnel number, data concerning the health of the MEP – in the form of bills for medical treatment (name of doctor, nature of treatment) –, the MEP's family, bank account, social security data, administrative data relating to requests for reimbursement of medical expenses (request number, amount, beginning/end dates for validity of reimbursements, parity coefficients, treatment codes, summary of reimbursements, reference tables, etc.). These data are the administrative data necessary for the processing of medical

expenses. They are collected in part via the SIDEP database, which centralises data on current and former MEPs.

The data processing is partially manual and partially automated. The paper files contain only prescriptions and bills relating to medical care or treatment. The medical reports are sent in sealed and confidential envelopes to the institution's medical officers for their opinion. The medical reports are not retained by the REMEDE department.

The computer data in the REMEDE database are retained for an indefinite period. The paper files contain accounting documents, and are subject to Article 49 of the Implementing Rules of the Financial Regulation. The latter article establishes a retention period of at least 5 years from the European Parliament's discharge for the financial year to which the documents relate (except for operations not definitively closed). After that time limit, the files relating to former MEPs are destroyed by an approved company which certifies their destruction. The data for current MEPs are kept for the duration of their term of office, even if they are re-elected.

Data may be occasionally transferred to the Settlements Office of the Joint Sickness Insurance Scheme to obtain the medical officer's opinion or opinions on fees.

The European Parliament plans to inform the data subjects by means of a specific communication. This communication has not yet been drafted.

The paper files of MEPs are kept in locked cupboards in the REMEDE department. The paper files of former MEPs are kept in locked cupboards in the Social Rights and Special Expenses Unit. The electronic files are stored in the central ITD server and are accessible via a connection restricted to officials from the MEPs' pensions and insurance office. Members of the ex-ante verification department (from Directorate A and DG Finance) also have access. Each member of the department has a personal password to access the database. Different levels of access are established for management staff. The database is logged; access to the database and to operations is controlled. A daily backup is made by the ITD.

2.2. Legal aspects

2.2.1. Prior checking

The notification received by the EDPS on 19 June 2006 relates to processing of personal data within the meaning of Regulation (EC) No 45/2001 ("any information relating to an identified or identifiable natural person" – Article 2(a)). The data are processed by a Community institution and the processing is carried out in the exercise of activities falling within the scope of Community law (Article 3(1)). It involves the collection, recording, organisation, storage, retrieval, consultation, etc. of personal data (Article 2(b) of Regulation (EC) No 45/2001) relating to the administration of reimbursements of the medical expenses of Members of the European Parliament and their families. These activities constitute partially automated and partially manual processing. When processing is manual, the processed data form part of a filing system, i.e. the MEP's paper files (Article 3(2)). The processing therefore falls within the scope of Regulation (EC) No 45/2001.

Article 27(1) of Regulation (EC) No 45/2001 requires prior checking by the EDPS of all "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".

Article 27(2) of the Regulation contains a list of processing operations likely to present such risks. The REMEDE processing operation must be subject to prior checking by the EDPS under Article 27(2)(a) of the Regulation because it contains data relating to health.

In principle, checks by the EDPS should be performed before the processing operation is implemented. In this case, as the EDPS was appointed after the system was set up, the check necessarily has to be performed *ex post*. However, this does not alter the fact that the recommendations issued by the EDPS should be implemented.

The notification from the European Parliament's Data Protection Officer was received on 19 June 2006. The EDPS therefore had to deliver his opinion by 20 August 2006 at the latest, as laid down in Article 27(4) of the Regulation. The period within which the opinion had to be delivered was suspended for 84 days by a request for further information. By an e-mail dated 8 September, the procedure was suspended for 7 days in order to enable the DPO to provide his comments and, where appropriate, additional information. The comments were received on 10 November 2006 and the opinion must therefore be delivered by 14 November 2006 (20 August plus the 86-day suspension).

2.2.2. Lawfulness of processing

Under the Regulation (Article 5(a)), the lawfulness of the processing is therefore based on the performance of a task carried out in the public interest on the basis of legal instruments adopted on the basis of the Treaties establishing the European Communities or in the legitimate exercise of an official authority vested in the Community institution. Recital 27 of the Regulation states that "Processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies". In the present case, the European Parliament processes the personal data relating to the REMEDE operation in order to perform one of its tasks: ensure the efficient administration of reimbursements of the medical expenses of Members of the European Parliament and their families. The lawfulness of the processing is based on Article 5(b) of Regulation, since the reimbursement of the medical expenses is a legal obligation. That being so, the processing operation proposed is therefore lawful.

The European Parliament is therefore justified in organising the system to reimburse medical expenses. The specific legal basis for the processing operation is to be found in Article 21 and Annex IV of the rules on the expenses and allowances of Members of the European Parliament. This article lays down the conditions governing the reimbursement of medical expenses. In the case under examination, the legal basis is particularly important because of the sensitive nature of the data being processed. The processing operation concerns a special category of data (see point 2.2.3 below).

2.2.3. Processing of special categories of data

The processing of data concerning health is prohibited (Article 10(1)) unless it is justified on the grounds set out in Article 10(2) and/or 10(3).

Article 10(3) of Regulation (EC) 45/2001 states that "Paragraph 1 [prohibition on the processing of data concerning health] shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health

professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". This applies in the current case.

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 an obligation of professional secrecy equivalent to that of health practitioners. The EDPS welcomes the fact that medical examinations are forwarded to the European Parliament's medical officer in sealed and confidential envelopes.

2.2.4. Data quality

In accordance with Article 4(1)(c) of the Regulation, personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". The medical data will obviously vary from case to case. Steps must be taken to ensure compliance with the principle of data quality. They could take the form of a general recommendation to the persons handling the files asking them to ensure that they comply with Article 4(1)(c).

Furthermore, the data must be processed fairly and lawfully (Article 4(1)(a) of Regulation (EC) No 45/2001). The matter of lawfulness has already been analysed (see section 2.2.2 above). Given the sensitivity of the subject, fairness warrants considerable attention. It is linked to the information that has to be forwarded to the data subject (see section 2.2.10 below).

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 procedure itself must ensure that data are accurate. The updating of the data is carried out by the controller who collects data with a reasonable assurance as to their accuracy; it must be possible for MEPs to exercise their rights of access and rectification in order to make the dossier as complete as possible. See section 2.2.9 concerning the rights of access and rectification of the data subjects.

2.2.5. Conservation of data

The general principle in the Regulation is that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Article 4(1)(e) of the Regulation). There is currently no limit on the storage period for electronic files. The EDPS considers that a storage period proportional to the purposes for which the data were collected should be established.

The paper files are subject to the requirements laid down in the Implementing Rules of the Financial Regulation. The EDPS considers that this storage period is reasonable in relation to the purposes for which the data are collected.

In relation to the daily back-ups made by the ITD, the EDPS notes that such data may only be stored in order to re-establish the stability of the system and ensure continuity of processing in the event of an accident. The storage period must be proportional to that purpose.

If the data are stored for historical, statistical or scientific purposes (Article 4(1)(b)), as envisaged in the notification, the data must kept in anonymous form.

2.2.6. Change of purpose/compatible use

Use of the MEP's personal number makes it possible to conclude that certain data are retrieved from the staff database (in this case, the SIDEP database). The processing operation being reviewed involves no general change of the specified purpose of the databases of MEPs and is not incompatible with that purpose. Accordingly, Article 6(1) of Regulation (EC) No 45/2001 does not apply in this instance and the conditions of Article 4(1)(b) of the Regulation are fulfilled.

In relation to back-ups, the EDPS recommends that ITD personnel with access to back-ups of the REMEDE system be informed that the recovery of back-up data (connected to the MEPs themselves) collected in order to restore the stability of the system and ensure continuity of processing in the event of an accident may not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences, as provided for in Article 6(2) of the Regulation.

2.2.7. Transfer of data

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

In the current case, data is transferred within an institution (medical officer, DG Finance). It is also a transfer between institutions, since personal data may occasionally be transferred to the Settlements Office of the Joint Sickness Insurance Scheme.

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 various departments of the European Parliament and the Settlements Office of the Joint Sickness Insurance Scheme. As regards transfers, only relevant data must be transferred. Such transfers are therefore indeed lawful insofar as the purpose is covered by the competences of the recipients. Article 7(1) is therefore duly complied with.

2.2.8. Processing including the personal or identifying number

The European Parliament 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, such use may have significant consequences. That is why the European legislator made the use of identifying numbers subject to the provisions of Article 10(6) of the Regulation which requires the European Data Protection Supervisor to intervene.

Here, it is not a case of establishing the conditions under which the European Parliament may process the personnel number, but rather of drawing attention to this point in the Regulation. In this instance, the European Parliament's use of the personnel number is reasonable because it is a means of facilitating the processing task, in particular archiving.

2.2.9. Right of access and rectification

According to Article 13 of the Regulation, the data subject shall have the right to obtain, without constraint, from the controller, communication in an intelligible form of the data undergoing processing and any available information as to its source. Article 14 provides that the data subject has the right to obtain from the controller rectification without delay of inaccurate or incomplete personal data.

The EDPS considers that the rights of access, rectification, blocking and erasing (Articles 15 and 16 of the Regulation) must be granted to the data subject of the paper and electronic files.

2.2.10. Information to be given to the data subject

Articles 11 and 12 concern the information to be given to data subjects in order to ensure transparency in the processing of personal data. Article 11 provides that when the data are obtained from the data subject, the information must be given at the time of collection. When the data are not obtained from the data subject, the information must be given when the data are first recorded or disclosed, unless the data subject already has it (Article 12).

In this instance, data related to medical expenses, for example, may be collected from the data subject. Identification data can also be collected from a third person through other databases (SIDEP) or through the medical officer. Articles 11 and 12 therefore apply in this case.

The EDPS notes that so far no arrangements have been made to provide information to the data subjects. The EDPS requests a system for providing data subjects with full information be introduced. That information must meet all the requirements of Articles 11 and 12 of Regulation (EC) 45/2001.

2.2.11. Safety

Technical and organisational measures have been taken to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Following a careful examination of the security measures in place, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

Conclusion

Certain aspects of the proposed processing operation do not take account of the provisions of Regulation (EC) 45/2001. In order to ensure compliance with Regulation (EC) 45/2001, the EDPS recommends that the foregoing comments be taken into account, in particular:

- Staff responsible for the processing operation should be informed that they are subject to a professional secrecy obligation equivalent to that of medical practitioners.

- A general recommendation requesting compliance with Article 4(1)(c) should be addressed to persons dealing with the dossiers.

- A storage period proportional to the purposes for which the data were collected should be established for the electronic files.

- The storage period for back-up files should be proportional to the purpose for which the data were collected – restoring the stability of the system and ensuring continuity of processing in the event of an accident.

- If the data are stored for historical, statistical or scientific purposes (Article 4(1)(b)), as envisaged in the notification, they should be kept in anonymous form.

- In relation to back-ups, the EDPS recommends that ITD personnel with access to back-ups to the REMEDE system be informed that the recovery of back-up data (linked to the MEPs themselves) collected in order to restore the stability of the system and ensure continuity of processing in the event of an accident may not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences, as provided for in Article 6(2) of the Regulation.

- The rights of access, rectification, blocking and erasure should be granted to the data subjects of the paper and electronic files.

- Comprehensive information should be provided to the data subject. That information must meet all the requirements of Articles 11 and 12 of Regulation (EC) 45/2001.

Done at Brussels, 14 November 2006

Peter HUSTINX
Supervisor

Executive summary

The REMEDE personal data processing operation administers reimbursement of the medical expenses of Members of the European Parliament and their families. The system is independent of the system for EU officials. In addition to the personal particulars of MEPs, medical prescriptions and bills for medical treatment are the main data collected and processed in order to determine the amounts of reimbursements. The EDPS reviewed the system because it contains data relating to health. The EDPS made a large number of recommendations, emphasising that some aspects of the processing operation do not take account of the provisions of Regulation 45/2001. This is particularly true of the provisions relating to data subjects' rights of access and rectification and of information to be given to them. The EDPS also made a recommendation regarding the storage period for electronic data.