Opinion on the notification for prior checking from the Data Protection Officer of the European Investment Bank (EIB) regarding the Gestion du Temps (GDT) (Time Management) dossier.

Brussels, 26 June 2006 (Case 2004-306)

1. Procedure

1.1. On 20 July 2004, the European Data Protection Supervisor (EDPS) sent a letter to the Data Protection Officers (DPOs) asking them to prepare an inventory of data processing operations that might be subject to prior checking by the EDPS as provided for by Article 27 of Regulation (EC) No 45/2001 (hereinafter referred to as "the Regulation"). The EDPS requested notification of all processing operations subject to prior checking, including those that commenced before the Supervisor was appointed and for which checking could never be regarded as prior, but which would be subject to "ex post" checking.

1.2. On the basis of the inventories received from the Data Protection Officers, the EDPS identified priority issues, including files containing health data.

1.3. On 10 November 2005, the EDPS requested an update of the inventory and notification of processing operations involving priority topics.

1.4. On 2 February 2006, the EDPS received notification for prior checking of data processing in the context of the EIB's "Gestion du Temps" dossier.

1.5. On 3 February 2006, the EIB's DPO was asked for further information. The DPO replied on 16 February 2006.

1.6. On 10 March 2006, the EDPS requested an information meeting on the "Gestion du Temps" application. The meeting took place on 18 May 2006 and was attended by Mr Burré of the EIB and Ms Louveaux of the EDPS.

1.7. On 20 June 2006 the EDPS suspended the time limit for delivering its opinion for 10 days to enable the controller to provide additional information and the EDPS to incorporate it.

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

2. Examination of the case

2.1. The facts

Under the Staff Regulations of the EIB, the working week for staff working full time is 40 hours based on a daily average of 8 hours. Part-time work is covered by pro rata provisions. There are provisions on time off in compensation for overtime worked.

The EIB has introduced a "Gestion du Temps" (GDT) system to enable the bank and its staff to manage attendance and absence, including overtime, leave, sick leave and other absences, on a semi-automatic basis.

All EIB staff, except members of the Management Committee, clock in and out on an electronic system using their service cards. Every operation is registered as "entry" or "exit". Where a staff member forgets to clock in or out, that identification is reversed and the time recorded as time worked will then not be accurate. Such errors are automatically recognised by the system and require manual correction by the data subject via the GDT application on his/her PC. When a correction is made, the system automatically adjusts hours worked accordingly. The application also makes it possible to record the working hours staff members spend carrying out other tasks for the EIB for which they are absent from the office (TEX: travail à l'extérieur).

Staff members can also submit applications for leave, sick leave (without a medical certificate) and time off in compensation for overtime. Leave applications and applications for time off in compensation for overtime have to be approved by a hierarchical superior. As soon as an application is made it appears on the hierarchical superior's screen. If approved, it will show "OK", if not approved, it will show "NO". Sick leave without a medical certificate does not require the hierarchical superior's approval.

The GDT application provides every staff member with a monthly chart of time worked/not worked showing: the hours to be worked in the month concerned, the number of hours carried over from previous months, the total hours worked each day, the total hours worked over the month and the excess or deficit at the end of the month. The screen will show the basic leave allowance, the days carried over from the previous year, additional leave (for example on grounds of age, for missions, on grounds of centre of interest).

GDT also enables the data subject and the hierarchy to see the average number of hours worked in excess of standard working hours over a period of four months. The maximum overtime allowed is 20 % over a given period. A person who exceeds 20 % is alerted to the fact. The same applies to the hierarchy. This facility is intended to encourage hierarchical superiors to be vigilant about overtime in excess of a given ceiling in the interests of promoting welfare at work and reconciling professional and family life.

The "Présent/absent" facility makes it possible to check whether a person is at work or not at a specific time or on a particular day and whether he/she can be reached by telephone. Every staff member has access to the "Présent/absent" data for colleagues in his/her division. The application uses a colour code to show the reason for absence (annual leave, leave, sickness, maternity leave, mission, other).

The "délégation d'accès" facility enables all staff members to delegate personal access to their data to a person of their choice. This facility makes it possible to modify data but does not

allow access to data relating to persons for whom the person delegating access has hierarchical responsibility.

In addition to having access to requests for approval of leave and compensatory leave, directors can also look at the individual time records of staff working under their authority. They may also see the schedule showing when staff working under them are available. Directors can also delegate the duty of authorising/approving leave applications and looking at the individual time records or schedules of staff working under their authority (e.g. to their Heads of Division).

The system administrator has access to all the data to which the data subject does not have access, i.e. adjustment of annual leave allowance (e.g. special leave) and introduction of dates of unpaid leave, parental leave, sick leave with medical certificate, maternity leave.

Where data are incomplete or inaccurate, the data subject can request a correction to his/her time record, directly via his/her individual PC or by sending an e-mail or a note through the internal mail to the system administrator or by delegating access to another trusted staff member.

GDT concerns only the application for the management of staff attendance and absence:

- recorded by the time clock;
- corrected by the data subject where necessary;
- approved by the directors.

The application concerns only attendance time, requests for time off in compensation for overtime and the introduction of sick leave of less than three days without a medical certificate. Other information is imported into GDT from other databases. Such data relate to missions, special leave and sick leave with a medical certificate. The GDT application does not forward data to other databases.

The GDT application stores data for 13 months on each individual PC. The system administrator stores them for 10 years for statistical purposes.

All GDT records are entered via the staff member's personal number.

When they take up their duties, all EIB staff receive an explanatory document on the GDT application. It explains how the system works. Among other things, it describes the types of data recorded in the system, the methods staff can use to record data and the access other people may have to the system.

Access to computer applications is secured via each staff member's individual PC access code. GDT maintenance has been subcontracted to a firm of consultants operating within the EIB. Maintenance relates solely to technical aspects. It is covered by a contract between the EIB and the firm of consultants.

2.2. Legal aspects

2.2.1. Prior checking

The notification received on 2 February 2006 relates to processing of personal data ("any information relating to an identified or identifiable natural person") under Article 2(a) of the Regulation. Data processing under the Gestion du Temps (GDT) application is carried out by an

institution in the exercise of activities which fall within the scope of Community law (Article 3(1)).

Moreover, the processing of personal data wholly or partly by automatic means comes within the scope of the Regulation under Article 3(2) thereof, which means that the application in question is covered, since most of the data-related operations are automatic.

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. Article 27(2)(b) identifies "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*" as processing operations likely to present such risks. Processing of personal data under the Gestion du Temps application comes under Article 27(2)(b) insofar as the information on presence and absence makes it possible to evaluate the person's conduct in relation to hours spent at the office. Indeed, since it calculates the hours worked, the application makes such evaluation possible.

Moreover, Article 27(2)(a) of the Regulation defines "the processing of data relating to health" as a processing operation likely to present such a risk. Since data on sick leave of less than three days can be entered in the time management system, Article 27(2)(a) also applies. In addition, information on sick leave with a medical certificate is also entered and can thus be viewed on the GDT screen.

The Gestion du temps application is therefore subject to prior checking by the EDPS.

In principle, checks by the European Data Protection Supervisor should be performed before the processing operation is implemented. In this case, as the European Data Protection Supervisor was appointed after the system was set up, the check necessarily has to be performed ex-post. This does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented.

The DPO's notification was received on 2 February 2006. Under Article 27(4), this opinion must be delivered within the following two months. The time limit was suspended for 13 + 69 + 10 days because further information was requested; the Supervisor therefore had to deliver an opinion by 3 July 2006 at the latest.

2.2.2. Legal basis and lawfulness of the processing operation

The legal basis for the data processing in question is Articles 25 to 28, 30, 31 and 33 of the EIB Staff Regulations, administrative provisions Nos 3 and 5 and Annex VI on part-time work.

Article 25 of the Staff Regulations sets the working week at 40 hours and specifies that working hours shall be determined accordingly.

Article 27 of the Staff Regulations requires all staff to inform the personnel department of all absences and the reasons for them. Staff members absent for more than three days in succession must provide a medical certificate as from the fourth day.

The Staff Regulations also provide that staff are entitled to 24 days of paid leave and special leave for particular reasons pursuant to special provisions. Staff may request unpaid leave for personal reasons for a period of three months which is renewable (Article 31).

In the event of prolonged or repeated absence not attributable to occupational disease or accident, the staff member's remuneration will be reduced in accordance with the criteria laid down in Article 33 of the Staff Regulations.

In addition to working hours, the GDT application manages absences and compensatory leave. It is also used to calculate and transfer data relating to overtime for which compensatory leave may be taken.

Alongside the legal basis, 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 other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution*".

The EIB exercises its right to organise working hours and manage leave and in so doing performs tasks carried out in the public interest on the basis of legal instruments adopted on the basis of the Treaties. The provisions of the Staff Regulations and the administrative provisions confirm the lawfulness of the processing.

2.2.3. Processing of special categories of data

The processing of personal data concerning health is prohibited unless it comes under Article 10(2) and/or (3).

Although the information recorded in the GDT system as sick leave does not contain any medical information as such, the data are "data concerning health" insofar as they provide information on the state of the data subject's health.

Article 10(2)(b) provides that the prohibition on processing such data does 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. Since the basis for processing data with the Gestion du Temps application is Article 27 of the EIB Staff Regulations, such treatment may be regarded as being necessary for the purposes of complying with the rights and obligations of the controller in the field of employment law.

2.2.4. Data Quality

Article 4 of the Regulation lays down certain obligations as regards the quality of personal data. Data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Article 4(1)(c)).

The presentation made at the meeting with the system administrator and the information received as set out under "facts" confirm that the data are adequate and relevant for the purpose declared.

The data must be processed fairly and lawfully (Article 4(1)(a)). Lawfulness has already been examined and the issue of fairness is linked to the transparency entailed by the information which must be transmitted to the data subject (see below).

Article 4(1)(d) stipulates that "data must be (…) accurate and, where necessary, kept up to date". Use of the personal number makes it possible to ensure that the data are accurate when they are

imported from another database. Data subjects' right to access and rectify their data is a further means of ensuring that the data are accurate and are updated if there is a clocking-in error (see below "right of access and rectification").

2.2.5. Retention of data

Under Article 4(1)(e) of the Regulation, personal data are to 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. If the data are stored for historical, statistical or scientific purposes, they must be kept in anonymous form or be encrypted.

The GDT application stores data for 13 months on each individual PC. The system administrator stores them for 10 years for statistical purposes. The data are not, however, kept in anonymous form.

The EDPS approves of the GDT application's 13-month time-limit for keeping data. On the other hand, the EDPS cannot agree to have the system administrator store data for a period of 10 years. As a general rule, a 5-year storage period may be appropriate provided that it corresponds to the period within which records of working hours or absences may be challenged or corrected and provided that the rights of the data subjects arising from these records are taken into account. A 5-year period can therefore be considered appropriate.

Data could be kept for the purposes of statistics on working hours; in that case they should be kept in anonymous form.

The EDPS therefore recommends that the long-term storage period be reviewed.

2.2.6. Transfer of data

Processing must also be examined in the light of Article 7(1) of the Regulation, which provides that personal data may only be transferred 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". Moreover, the recipient may process them only for the purposes for which they were transmitted.

Under the GDT system different users have different rights of access. These rights are clearly defined. Members of the same division have access to the schedule in order to check whether a member of the division is present or not. Directors have access to requests for approval of leave and leave in compensation for overtime and can also look at the individual time records of staff working under their authority. They may also see the schedule showing when staff working under them are available. Such access can be regarded as necessary for the legitimate performance of tasks covered by the competence of the data recipient.

Directors can also delegate the duty of authorising/approving leave applications and looking at individual time records or schedules (e.g. to their Heads of Division). Conditions should be set for such delegation to ensure that data are not processed for purposes other than the management of compensatory time.

Moreover, stricter measures should be set for the system administrator's access, since it makes it possible to draw up a relatively precise table of each staff member's absence/presence and overtime worked and to establish individual statistics. The EDPS would therefore advise setting specific conditions for such access.

2.2.7. Processing including the personal or identifying number

Under Article 10(6), the European Data Protection Supervisor "shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body".

This decision does not aim to establish the general conditions for using the personal identifying number, but only its use in the context of the GDT application. For the case in hand, use of the personal number for the purpose of recording data in the system is reasonable in that this number is used to identify the person in the system and thus helps ensure that the data are accurate.

2.2.8. Right of access and rectification

Article 13 of the Regulation provides for the data subject's right of access to data concerning him/her. Under Article 14 of the Regulation, the data subject has the right to obtain rectification of inaccurate or incomplete data.

The GDT system gives the data subject access to personal data via his/her personal PC.

As stated under "facts", where data are incomplete or inaccurate, the data subject can request a correction of the time record, directly via his/her individual PC or by sending an e-mail or a note through the internal mail to the system administrator or by delegating access to another trusted staff member. That arrangement thus enables the data subject to exercise his/her right of access and rectification.

2.2.9. Information to be given to the data subject

Articles 11 and 12 of Regulation (EC) No 45/2001 provide that the data subject must be informed where his or her personal data are processed and lists a series of specific items of information that must be provided. In the present case, some of the data are collected directly from the data subject and others from other sources. Both articles therefore apply.

As stated under "facts", when they take up their duties, all EIB staff receive an explanatory document on the GDT application. It explains how the system works. Among other things, it describes the purpose of the system, the types of data recorded in it, the methods staff can use to enter data, the opportunity to correct inaccurate data and the access other people may have to the system (data recipients). In the light of the provisions of the Regulation, the EDPS would like staff members covered by the system also to be informed of the identity of the controller, the legal basis for processing and the time limit for keeping data. They should also be informed that they can have recourse at any time to the European Data Protection Supervisor.

2.2.10. Security

In accordance with Articles 22 and 23 of the Regulation, the controller and the processor are required to implement the 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, accidental loss or alteration, and prevent all other forms of unlawful processing.

Access to computer applications is secured via each staff member's individual PC access code. Given the relatively low sensitivity of the data relating to each staff member, the EDPS considers that sufficient.

2.2.11. Processing of personal data on behalf of the controller

Article 23 sets out the obligations to be met by the controller where a processing operation is carried out on its behalf: the controller must choose a processor providing sufficient guarantees in respect of the technical and organisational security measures; the carrying out of processing must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor may act only on instructions from the controller; the obligations set out in Articles 21 and 22 are also incumbent on the processor. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 must be in writing or in another equivalent form.

GDT maintenance has been subcontracted to a firm of consultants operating within the EIB. Maintenance relates solely to technical aspects. It is covered by a contract between the EIB and the firm of consultants.

The contract binding the processor to the EIB should be checked to ensure that it lists the processor's obligations regarding security (Articles 21 and 22 of the Regulation) and stipulates that the processing firm may act only on instructions from the EIB. The EDPS requests that this check be made and recommends that, if necessary, these specific provisions be inserted in the body of the contract.

Conclusion

The proposed processing operation does not appear to infringe the provisions of Regulation (EC) No 45/2001, provided that the comments made above are taken into account. This means in particular that:

- the long-term storage period must be reviewed;
- if data are kept for the purposes of statistics on working hours, they must be made anonymous;
- conditions must be set for delegation by directors of the duty of authorising/approving leave applications and looking at individual records or schedules in order to ensure that data are not processed for purposes other than the management of compensatory time;
- conditions must be set to ensure that the system administrator's access to all data cannot be used for purposes incompatible with the purposes of the GDT application;

- staff members covered by the system must also be informed of the identity of the controller, the legal basis for processing, the time limit for keeping data and their right to have recourse to the European Data Protection Supervisor;

- the contract binding the processor to the EIB must mention the processor's obligations regarding security and stipulate that the processing firm may act only on instructions from the EIB.

Done at Brussels, 26 June 2006

Peter HUSTINX
European Data Protection Supervisor