Opinion on a notification for prior checking received from the Data Protection Officer of the European Investment Bank on the recording of telephone communications in trading rooms

Brussels, 8 May 2006 (Dossier 2006-102)

1. Procedure

1.1. On 20 July 2004 the European Data Protection Supervisor (EDPS) wrote to Data Protection Officers (DPOs) asking them to establish an inventory of the 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 "the Regulation"). The EDPS requested notification of all processing operations subject to prior checking, including those that commenced before the Supervisor was appointed, for which checking could clearly not be regarded as prior, but which would be subject to "*ex post*" checking.

1.2. On the basis of the lists received from the DPOs, the EDPS identified a number of priority areas.

1.3. On 10 November 2005 the EDPS asked for the lists to be updated and for notification of data-processing operations in the priority areas. He also broadened the latter to include data processing arising from electronic and telephone communications.

1.4. On 2 March 2006, the EDPS received a notification for the prior checking of data processing concerning the recording of telephone communications in EIB trading rooms.

1.5. A request for information was sent to the DPO 16 March 2006, to which the DPO provided an initial reply on 21 March 2006; the other replies were given over the 'phone by Mr LEMAIRE on 24 March 2006.

1.6. Additional information was requested on 5 April 2006 and provided on 6 April 2006.

2. Examination of the case

2.1. The facts

All financial transactions taking place in the front offices of the EIB's Capital Markets (FICAP) and Treasury (FITRE) Departments (lending operations and currency, security and deposit trading) are negotiated and concluded over the telephone. To avoid either party misinterpreting

the terms of an agreement, all telephone conversations taking place in those departments are recorded. The only telephones outside the recording system are those on which trading is not authorised, i.e. telephones used by the various secretariats, those in the five offices and the meeting room around the trading room. If need be, trading-room staff can use those 'phones for private calls. In the trading rooms, however, there is no means of limiting the recording of telephone conversations to trading transactions; private conversations on these 'phones are therefore recorded automatically.

The communication data are recorded on CD-ROM; in addition to the conversation itself, they comprise contextual data such as time and date. Those data are also noted in the operational file documenting the dealer's work.

The maintenance firm is authorised to access the system. Each operation to access the recording system must be entered in full in the logbook kept permanently beside the equipment. The entry comprises the date of the operation, the reason for the operation, the starting and finishing time of the job, and the name of the person(s) working on the equipment. In principle, it is not necessary to access the tracks of the CD-ROM for maintenance purposes. If such access proves essential, however, the manager[1] and the dealer[2] concerned must be present throughout the operation. If the dealer does not wish to be present throughout, this will be noted.

The recordings and the CD-ROMs containing them may be consulted for the sole purpose of verifying telephone transactions. Verification takes place if a transaction is challenged or if the management deems it necessary to monitor operations. It may be requested by the dealer concerned, his head of division, or his head of department. A dealer may not refuse a request from his superiors to verify a transaction.

The dealer concerned and the director of his department or his substitute must be present when the data are consulted. The dealer's head of division may be asked to attend. If necessary the Inspectorate-General, the legal departments, the Director of Human Resources or the Chief Compliance Officer (CCO) may also be invited to attend. After entering his password, the dealer directly involved in the disputed transaction localises the relevant section on his listening channel. If, for overriding reasons, a disputed transaction has to be consulted while the dealer concerned is absent for some period of time (on leave, sick leave, a business trip, etc.), the dealer's head of department will try to contact him to tell him of the need to listen to his channel. In that case the DPO is also informed. If the dealer concerned cannot be contacted, the recording will be listened to nevertheless, after the Director of Human Resources and the DPO have been notified. In that case, the Departmental Director (or his substitute) will use the dealer's personal password, a copy of which he has received from the dealer in a sealed envelope. A record of the proceedings will be drawn up and signed by all the persons present and a copy thereof given to the dealer concerned on his return to work.

In the event of a disputed transaction, the data may be communicated to the other party (bank or organisation concerned). In general, the other party will have its own recording of the transaction and should not need to request that the date be transferred. If the other party should ask to listen to the recording, however, it may do so only on EIB premises and in the dealer's

---

[1] The Director-General FI, the Directors of FITRE and FICAP Departments, the member of the FI Coordination and Financial Policies Division, responsible for technical questions.

[2] i.e. Every dealer whose communications are recorded.

presence. If necessary, the data may also be communicated to the Inspector-General, the legal department or the Director of Human Resources and to the Chief Compliance Officer (CCO).

All data subjects at the EIB were briefed in detail by their superiors when the procedure was introduced. The procedure is described in the Finance Directorate Front Office Manual, a copy of which is given to each new recruit to the Directorate. The Manual describes the scope of the recording system, relations with other parties, access to the secure room, the system maintenance procedure, the custody of the recorded CD-ROMs, the consultation of recordings and the back-up system. The Directors of Capital markets and Treasury Departments ensure that each counterparty is informed in the manner they deem most appropriate of the existence of a front office recording system at the EIB. In addition, conversations are recorded in accordance with the financial sector's code of professional ethics.

Adoption of security measures. [...]

2.2. Legal aspects

2.2.1. Prior checking

The recording of telephone communications on lending operations and currency, security and deposit trading in the Capital Markets (FICAP) and Treasury (FITRE) Departments is a data-processing operation. It is, moreover, a personal data-processing operation, because the conversations take place between two persons at least one of whom is identified or at least "identifiable". An identifiable person within the meaning of the Article 2(a) of the Regulation is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity". Since each dealer has his own channel, and it is there that conversations are recorded, he is an identified person. Moreover, the correspondent in the counterpart institution will very often also identify himself at the beginning of the conversation.

The data-processing operation in question is carried out by an institution in the exercise of activities which fall within the scope of Community law.

The recordings are made by automatic means (Article 3(2) of the Regulation) and are manually processed, being noted in the dealer's operational file forming part of a filing system within the meaning of Article 2 of the Regulation.

The data-processing operation therefore falls within the scope of the Regulation.

Article 27(1) of the Regulation makes 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" subject to prior checking by the European Data Protection Supervisor. Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

Specific data-protection issues are involved when data are processed in the context of internal communications networks; for this reason the Regulation devotes a special chapter to the subject (Chapter IV). Article 36 lays down the basic principle (examined below) of confidentiality of communications. On account of the specific risks inherent in the recording of trading-room conversations, Article 27(1) of the Regulation may be applicable.

In principle, checking by the European Data Protection Supervisor should take place prior to processing. In the present case, as the European Data Protection Supervisor was appointed after the system was set up, checking necessarily has to be performed ex post. This in no way alters the desirability of acting on the European Data Protection Supervisor's recommendations.

The DPO's notification was received on 2 March 2006. This opinion must therefore be delivered within two months of that date, as laid down in Article 27(4) of the Regulation. That period was suspended for nine days. The EDPS will therefore deliver his opinion no later than 11 May 2006.

2.2.2. Legal basis and lawfulness of processing

According to the DPO's notification, the processing of data collected when recording communications in the Capital Markets (FICAP) and Treasury (FITRE) Departments is based on the Staff Regulations and Annex 4 to the Finance Directorate's Front Office Manual, which describes the procedure in place. The EDPS takes this Manual to be the basis for the processing of data collected via recordings made for the purpose of verifying telephone transactions. "Such verification shall take place if a transaction is challenged or if management deems it necessary to monitor operations." (Manual, Part VI). Verification concerns the content of the transaction. The processing operation may not therefore be used for any other purpose.

Alongside the legal basis, the lawfulness of the processing operation as defined in Article 5 of the Regulation must also be considered. Article 5(a) stipulates that personal data may be processed only if "processing is 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". The preamble to the Regulation (recital 27) 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. The recording of trading-room communications in order to ensure the validity of the transactions may thus be considered necessary for the performance of the EIB's tasks.

2.2.3. Data quality

Under 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". In order to avoid either party misinterpreting the terms of an agreement, all telephone conversations made in the departments concerned are recorded. However, there is no means of limiting the recording of trading-room telephone conversations solely to trading transactions. The data concerned are therefore all the data in the recordings of the communications. As the recording process cannot be restricted, private conversations made on those telephones may possibly be recorded.

Since the purpose of the processing is to monitor transactions made over FICAP and FITRE trading-room 'phones, it would be difficult, indeed undesirable, not to record all calls made over those departments' 'phones, as it is hardly possible to distinguish as a matter of course between private and professional incoming calls to telephones intended to be used for transactions. It is therefore relevant and not excessive in relation to the purpose for which the data are collected that all communications should be recorded. It must also be stressed that the Front Office

Manual asks staff of the departments concerned to use designated 'phones - outside the recording system - for their private calls.

The data surrounding the communication but not forming part of its content are necessary in this case so that, for example, the content can be linked to a specific recipient or the communication given a date and time. This contributes to the accuracy of the data.

Article 4(1)(d) stipulates that the data must be "accurate and, where necessary, kept up to date". The fact that conversations are recorded live ensures compliance with this principle. Moreover, in the event of system failure, an alert is sent to both the technical services of the FM division and the trading room.

2.2.4. Confidentiality of data

Under Article 36 of the Regulation "Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law".

It should be noted in this connection that the principle of the confidentiality of communications is based on Article 5 of Directive 97/66/EC, which stipulates that Member States must prohibit listening, tapping and storage or other kinds of interception or surveillance of communications and the related traffic data without the consent of the users concerned, except when legally authorised, in accordance with the principles of Community law. That Directive has since been replaced by Directive 2002/58/EC, but the principle remains unchanged: if the parties to a conversation give their consent, there is no breach of the principle of the confidentiality of communications. The EDPS considers that Article 36 of the Regulation must be interpreted in the light of these provisions.

FICAP and FITRE front-office dealers are informed of the recording procedure in Annex 4 to the Front Office Manual, which is distributed to every new recruit to those departments. As far as the data subjects in the counterparty are concerned, the Directors of the Treasury and Capital Markets Departments ensure that each counterparty is informed, in the manner which they deem most appropriate, that such a recording system is in operation in EIB front offices. In this connection, care should be taken to check that not only the counterparty as an institution but also that persons whose data are being recorded are informed of the system.

If the recordings have to be consulted, the dealer involved must be present. Should the dealer concerned by absent for any length of time, his head of department will try to contact him in order to tell him of the need to listen to his channel. Only if the dealer cannot be contacted will the recording be listened to without his knowledge. Strict rules apply to the listening procedure in accordance with the principles of Community law. The consultation of a recording at the EIB automatically implies that the counterparty institution must do the same and, therefore, that the latter has been notified.

2.2.5. Conservation of Data

In principle personal 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" (Article 4(1)(e)).

Article 37(1) lays down specific rules on the storage of traffic data, i.e. the data surrounding a communication including the data necessary to establish the call. In principle, traffic data should be erased or made anonymous upon termination of the call.

Under Article 37(2) traffic data may be stored for a maximum of six months for the purpose of telecommunications budget or traffic management, including the verification of authorised use of the telecommunications systems. However, it is not necessary to rely on this provision as grounds for storing data when the call is over, because Article 20 also authorises restrictions on the application of certain principles of the Regulation in specific cases.

Article 20 allows exceptions to Article 4(1) and Article 37(1), in particular when the storage of data constitutes "a necessary measure to safeguard an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters".

Traffic data are processed as part of the recording procedure. All the data are stored for one year unless a transaction is challenged, in which case the CD-ROMs may be kept for more than one year and until the problem is resolved.

Data are kept for this period on grounds of security, as proof of transactions and in order to comply with the practices of the bank's various counterparties on the international financial markets; the period is specific to the nature of the markets on which the EIB operates. The procedure can be justified on the basis of Article 20, in that it can be considered as "necessary to safeguard an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters".

2.2.6. Transfer of data

Pursuant to the notification received from the DPO, in the event of a dispute data may be communicated to the counterparty (bank or institution directly concerned) and, if necessary, to the Inspector-General, the legal service or the Director of Human Resources and to the Chief Compliance Officer (CCO).

In-house transfers of data must comply with the rules laid down in Article 7 of the Regulation, which provides that data may be transferred only if they are necessary for the legitimate performance of tasks covered by the competence of the recipient. The EDPS would query whether the data need to be transferred to the Director of Human Resources if the sole aim of the data-processing operation is to verify transactions, as the notification and the Manual both state.

In the event of a dispute, the data are not transferred but are made available to the counterparty by the EIB. This point will consequently be dealt with in the section on right of access.

2.2.7. Right of access and rectification

Under Article 13 of the Regulation the data subject has, *inter alia*, the right to obtain, without constraint from the controller communication in an intelligible form of the data undergoing processing and of any available information as to their source. Under Article 14 of the Regulation the data subject has the right to obtain rectification of inaccurate or incomplete personal data.

The Finance Directorate Front Office Manual (Annex 4) permits the dealer to have access to the recording system. Any right of rectification could apply only to the contextual data: the communication itself cannot be erroneous, having been recorded live.

As regards right of access and rectification by counterparties, since the counterparties themselves record the communications, they do not, as a rule, need to exercise right of access to EIB recordings. However, should the counterparty not have its own recording system, or should the system fail, the EIB permits counterparty dealers to consult recordings concerning them, such consultation to take place at the EIB's head office. The same limitations apply to right of rectification *mutatis mutandis*.

2.2.8. Information to be given to data subjects

Articles 11 and 12 of the Regulation relate to 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, certain 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 that information. Since in this case the data are collected directly from the data subject, the information in question must be given to him at the latest when the data are recorded.

The information to be provided to data subjects under Article 11 concerns the identity of the controller; the purposes of the processing operation; the recipients or categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the right of access to, and the right to rectify, inaccurate or incomplete data concerning him or her. Any further information, such as the legal basis of the processing operation, the time-limits for storing the data and the right to have recourse at any time to the EDPS may also be given insofar as such further information is necessary to guarantee fair processing in respect of the data subject.

As mentioned earlier (Facts), data subjects receive this information from Annex 4 of the Finance Directorate Front Office Manual, a copy of which is given to each new recruit to the Directorate. The Manual describes the recording procedure in detail, but it does not include all the information specified in Article 11. The controller is not identified, and there is no mention of the data subject's right to have recourse to the EDPS at any time.

As far as information to counterparties is concerned, according to information received the Directors of the Treasury and Capital Markets Departments ensure that each counterparty is informed, in the manner which they deem most appropriate that such a recording system is in operation in EIB front offices. In this connection, care should be taken to check not only that the counterparty as an institution but also counterparty staff whose data are being recorded are informed of the system.

2.2.9. Security

Under Article 22 of the Regulation, the data controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

Having carefully examined the security measures adopted, the EDPS considers them to be adequate in the light of Article 22 of the Regulation.

Conclusion

The proposed processing operation does not appear to involve any breach of the provisions of Regulation (EC) No 45/2001 provided that account is taken of the comments made above. That means in particular that:

- Annex 4 to the Front Office Manual must identify the data controller and specify that recourse can be had to the EDPS at any time;

- Consideration must be given to whether the data need to be transferred to the Director of Human Resources in view of the purpose of the transaction verification system as set out in the notification and Annex 4 to the Front Office Manual;

- Checks should be made as far as possible to ensure that information on the data-processing operation is received not only by the counterparty as an institution, but also by the individuals whose data are being recorded.

Done at Brussels, 8 May 2006

Peter HUSTINX
European Data Protection Supervisor