Opinion on the notification for prior checking received from the European Investment Bank's Data Protection Officer regarding data processing in the framework of the disciplinary procedure

Brussels, 25 July 2005 (Case 2005-102)

1. Procedure

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

1.2. On the basis of the inventories received from the Data Protection Officers, the EDPS identified priority topics, namely data processing operations in disciplinary, staff evaluation and medical files.

1.3 On 15 April 2005 the EDPS wrote a letter to the DPO of the European Investment Bank (EIB) asking to be notified of data processing operations which fell within the scope of the priority topics.

1.4 On 28 April 2005 the EDPS received the notification for prior checking regarding data processing in the framework of disciplinary procedures and penalties at the EIB and the EIF.

1.5 On 2 May 2005 the EDPS requested further information on the procedure itself and a copy of the EIB Staff Regulations. On 8 June 2005 the EDPS received the additional information.

1.6 On 28 June 2005 the EDPS requested further information. That information was received on 30 June 2005.

1.7 On 18 July 2005 the EDPS made a final request for further information. That information was received on 19 July 2005.

Postal address : rue Wiertz 60- B-1047 Brussels
Offices : rue Montoyer 63
E-mail : edps@edps.eu.int
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. Examination of the case

2.1 The facts

Under Article 1.5 of the EIB's Code of Conduct, members of staff who knowingly violate the obligations are liable, depending on the seriousness of the infringement, to the disciplinary measures provided for in the Staff Regulations or, where these do not apply to them, risk having the contract enlisting their services annulled by the Bank. Article 38 of the Staff Regulations provides that the following disciplinary measures may be taken against members of staff who fail to fulfill their obligations: written reprimand; a maximum of one year's suspension of incremental advancement; summary dismissal for grave misconduct, with or without severance grant; summary dismissal for grave misconduct with loss of severance grant and reduction of pension rights. In the event of dismissal, measures may be taken only after consultation of a Joint Committee in accordance with the procedure laid down in Article 40 of the Staff Regulations. The Committee shall not be required to deliver its opinion in the event of grave misconduct involving prosecution, when the member of staff concerned has been taken *in flagrante delicto*.

The Joint Committee is composed of the director of the General Administration Directorate, as non-voting chairman; the Head of Personnel and a director from a directorate other than that of the member of staff concerned; two staff representatives chosen by the member of staff concerned and a secretary who does not take part in the Committee's deliberations or vote.

The Joint Committee is convened by written instruction of the President addressed to the director of the General Administration Directorate. The member of staff concerned is simultaneously notified of that instruction and receives written notification of the charges against him at least fifteen days prior to the date set for the Committee's meeting.

The member of staff may, and if he so requests must, be heard by the Committee. He may enlist the aid of a counsel of his own choosing when appearing before the Committee.

The Joint Committee may, if it does not feel sufficiently well informed of the facts, hold any necessary enquiry and hear witnesses. The member of staff shall also be entitled to call witnesses.

The member of staff concerned shall not be present during the Committee's deliberations. The Committee shall deliver a reasoned opinion to the President of the Bank, to which each of its members shall be free to add his personal opinion. Those opinions shall, at the same time, be conveyed in writing to the member of staff concerned. The President shall give his decision within fifteen days following communication of the reasoned opinion.

Taking disciplinary measures in no way prevents the Bank from initiating any criminal proceedings considered necessary.

The information on any disciplinary penalties is entered in the official's personal file and also encoded in the HR information system (PeopleSoft application). This is an integrated application for human resources management. Hierarchical superiors do not have access to the data. All use of the data is subject to express authorisation by the Human Resources Manager. Queries allow authorised administrators (person responsible for HR reporting) to obtain a list of penalties imposed. That list gives the names of those concerned. It may be used in the

framework of staff management/mobility, for example, in the context of future assignment to a sensitive post.

All EIB/EIF staff members have access to their personal files, including the documents on disciplinary procedures or penalties concerning them.

Specific rules on access by members of the HR Department to documents contained in personal files were laid down by a decision of 16 December 2004. Those rules lay down a grid for access to documents depending on the type of document and the person from the HR Department requesting access: "paper" documents on disciplinary penalties are kept in the most confidential part of the personal file. All authorised persons who access the information will be responsible for the confidentiality of the information. Authorised persons may in no circumstances disclose data contained in personal files or relating thereto inside or outside the Bank. Other than HR Heads of Division or HR Managers, authorised persons must collect the documents they need personally and return them personally. Any HR staff member who does not have authorisation to access documents must make a specific request in writing to the Head of Division for each individual access. Such authorisation may be given by electronic mail. Personal files may be accessed only in the course of the normal activities of the HR Department. Copying or reproducing the documents contained in personal files is forbidden, unless exceptional permission is granted.

Access to the corresponding data in the HR information system (PeopleSoft application) is restricted to the Human Resources Manager, to his/her assistant and to the Head of the "HR coordination" unit (also responsible for legal matters concerning the staff).

As part of the implementation of the Electronic Data Management project, all personal files currently kept in the HR archives will be scanned. This task has been given to an outside company. The sub-contractor was chosen following a call for tenders procedure. Contractual and practical measures have been taken to comply with the requirements of Article 23. The rules on access to documents will be adapted on the implementation of Electronic Data Management, (see above).

In principle, data are kept throughout the entire career of the official/person concerned and after the end of the career for an indefinite period. In certain cases, however, the penalty provides for its deletion from the personal file after a certain time if the official's behavior has changed. In that event, the reference to the penalty is also removed from the disciplinary file.

2.2. Legal aspects

2.2.1. Prior checking

The management of disciplinary files constitutes processing of personal data within the meaning of Article 3(2) of Regulation (EC) No 45/2001 insofar as it consists of collecting, consulting and retaining personal data. This processing operation constitutes manual processing within the meaning of Article 3(2) insofar as the data are intended for inclusion in a filing system within the meaning of Article 2(c) of the Regulation.

Implementation of the project on the electronic management of personal files involves the automatic processing of part of the data, i.e. penalties.

Under Article 27(1) of Regulation (EC) No 45/2001, "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" is subject to prior checking by the EDPS.

Article 27(2) of the Regulation lists processing operations which are likely to present such risks.
Disciplinary files must be subject to prior checking for a number of reasons. They may contain data on suspected offences, offences, criminal convictions or security measures, as laid down in Article 27(2)(a). In addition, the documents are intended to evaluate aspects of the personality of the persons concerned, in particular their conduct, and accordingly are covered by Article 27(2)(b).

Prior checking covers the processing of personal data as part of a disciplinary procedure. The aim is not to provide an opinion on the disciplinary procedure as such.

The disciplinary procedure of which notification has been given also applies to members of the European Investment Fund (EIF) pursuant to Articles 38 and 40 of the EIF Staff Regulations. For reasons of simplicity, we have referred only to the EIB in the text. It goes without saying that all recommendations apply to the EIF *mutas mutandis*.

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 facto*. However, this does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be introduced.

The notification of the DPO was received on 28 April 2005. Under Article 27(4), this opinion must be delivered in the two months which follow. The Supervisor will therefore deliver his opinion by 28 June 2005 at the latest. An information request suspends this deadline by 39+2+1 days. The opinion must therefore be delivered by 11 August 2005.

2.2.2. Legal basis and lawfulness of the processing operation

With regard to the lawfulness of data processing in the context of disciplinary files, it is justified on the basis of Article 5(a) of Regulation (EC) No 45/2001 only insofar as it is necessary for the legitimate exercise of official authority vested in the EIB as a Community institution. In the case in point, lawfulness results from the execution of a task performed pursuant to Articles 38 and 40 of the EIB Staff Regulations, which are the equivalent of the Staff Regulations of officials of the European Communities (Articles 38 and 40 of the EIF Staff Regulations).

Disciplinary files may contain data on offences and criminal convictions, which can be processed only if authorised by the legislative acts adopted on the basis of the Treaties, in accordance with Article 10(5) of Regulation (EC) No 45/2001. Article 1(5) of the Code of Conduct and Articles 38 and 40 of the EIB Staff Regulations (and 40 of the EIF Staff Regulations) must be considered as authorizing such data processing.

If in the course of an enquiry personal data revealing political opinions or union membership are processed as part of a disciplinary procedure and are relevant to the case and/or the way it

is being handled, Article 10(2)(b) shall apply. In such cases too, Articles 38 and 40 of the Staff Regulations could serve as a basis for the processing of such data.

The lawfulness of the lists of penalties encoded in the HR information system for verification purposes in the context of future assignment to a sensitive post is more questionable. While we do not challenge the legitimacy of verifying the absence of disciplinary measures for the purpose of filling a post which has been established in advance as sensitive, the EDPS does question the need to have a list of names in the light of Article 5 of Regulation (EC) No 45/2001. Indeed, since disciplinary measures are recorded in the disciplinary file and in the personal file, consultation of those files when appointing persons to sensitive posts could be sufficient for the purpose of verifying the absence of disciplinary measures. While entering a disciplinary measure in a list of encoded penalties is useful, one may nonetheless ask whether this processing operation is really necessary and proportionate.

2.2.3. Data quality

Article 4 of Regulation (EC) No 45/2001 sets out certain obligations regarding the quality of personal data. The 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)).

Personal data must also be accurate and, where necessary, kept up to date. The Regulation also provides that "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)).

There are no systematic rules on the type of data which may be included in a disciplinary file. The nature of the data depends to a large extent on the case in question. That being the case, rules should be drawn up on the criteria to be applied before entering evidence or data in a disciplinary file in order to ensure that only relevant data are kept. Staff responsible for processing disciplinary files must be informed of these rules and comply with them.

2.2.4. Retention of data

Regulation (EC) No 45/2001 provides that 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.

According to the information received in the notification for prior checking by the Data Protection Officer, data on disciplinary penalties within the institution are kept in the individual file and are also encoded in the HR information system (PeopleSoft application).

- Retention of data in the individual file of the official concerned

In principle, data are kept throughout the entire career of the official/person concerned and after the end of the career for an indefinite period. In certain cases, the penalty may provide for its erasure from the personal file after a certain time if the official's behaviour has changed. On the other hand, there are no systematic rules on the deletion of data from the individual file after a certain time lapse.

The EDPS would like a data retention period to be established in the light of Article 4(1) of Regulation (EC) No 45/2001 which, in itself, is the concrete application of a fundamental right.

- Retention of data in the disciplinary file

Data are kept in the disciplinary file indefinitely unless the penalty provides for its erasure from the personal file after a certain time if the official's behaviour has changed, since in that instance the reference to the penalty is also removed from the disciplinary file. However, in this case there are no rules on the other components of the disciplinary file.

The EDPS would like a data retention period to be established in the light of Article 4(1)(e) of Regulation (EC) No 45/2001.

- Retention of data in the HR information system

The EDPS wishes to express the following reservations concerning the retention of data in the encoded list in the HR information system. On the one hand, the retention of data in that list must be consistent with any deletion of data from the individual or disciplinary file. On the other hand, the reference to a person on this list must not be retained after the end of the career of the person concerned.

2.2.6. Compatible use

Article 4(1)(b) provides that data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes.

If data on disciplinary penalties are encoded in the HR integrated system there is a risk that they might be used for purposes other than those for which the data were originally intended. However, the fact that the data may not be used without the explicit authorisation of the Director of Human Resources acts as a safeguard against that risk. Appropriate security measures could strengthen that guarantee (Cf. 2.2.10).

2.2.7 The collection and transfer of data

Article 7 of the Regulation provides for rules to be observed both by the controller and by the recipient when data are transferred within or between Community institutions or bodies.

Furthermore, Article 2(g) of the Regulation provides that "recipient shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients".

Accordingly "in the framework of a particular inquiry" the persons to whom data are disclosed thus cannot be regarded as recipients, and Article 7 therefore does not apply to the transfers envisaged in the frame of an inquiry under disciplinary proceedings.

Moreover, the transfer of data in the course of appeal procedures is considered as the legitimate performance of tasks covered by the competence of the recipient, and as such complies with Article 7.

2.2.8 Information for data subjects

Principle

Articles 11 and 12 of Regulation (EC) No 45/2001 provide that the controller must provide the data subject with certain information. Article 11 provides that where data have been obtained directly from the data subject, the aforementioned information must be given at the time of collection. If the data are not obtained directly from the data subject, the information must be supplied either at the time it is recorded or, if disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Personal data contained in disciplinary files may be collected from the data subject, and also from third parties. Information must therefore be given either at the time of collection of the data or before it is first recorded or transmitted to a third party.

The information to be provided includes, inter alia, the identity of the controller, the purposes of the processing operation for which the data are intended, the recipients or categories of recipients, the existence of the right of access and the right to rectify the data, and where appropriate the right to have recourse at any time to the European Data Protection Supervisor.

The disciplinary procedure provides that the member of staff concerned shall simultaneously be notified of this instruction and shall receive written notification of the charges against him at least fifteen days before the date set for the Joint Committee's meeting. However, the data subject is not given any particular information on the processing of personal data. The EDPS considers that at least general information on the processing of personal data in the frame of disciplinary proceedings must be given.

Restrictions

Although in principle data subjects must be informed, Regulation No 45/2001 nevertheless provides for limits to that obligation in certain restricted cases. Article 20 of the Regulation provides for certain limits to that obligation, in particular "where such restriction constitutes a necessary measure to safeguard: (a) the prevention, investigation, detection and prosecution of criminal offences;… (c) the protection of the data subject or of the rights and freedoms of others". In principle, if the investigation is not into a criminal offence, the exception provided for under Article 20 of the Regulation (EC) No 45/2001 does not apply *sensu stricto*.

Nevertheless, the EDPS considers[1] that Article 20 has to be interpreted in the light of the *ratio legis* of the provision so as to provide for certain restrictions on the duty to inform the data subject in the course of a disciplinary investigation. That view is supported by the fact that Article 13 of Directive 95/46/EC provides for exceptions from and restrictions on certain rights "when such a restriction constitutes a necessary measure to safeguard ...d) the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions". Article 13(1)(d) of the Directive is far-reaching and extends from the prevention, investigation, detection and prosecution of criminal offences to breaches of ethics for regulated professions. Accordingly, although it is not stated explicitly, there is no

[1] Opinion of 21 March 2005 (Case 2004/0198) on a notification for prior checking received from the Data Protection Officer of the European Parliament on data processing in the context of disciplinary files.

reason to believe that disciplinary offences by public sector agents are not also included in this restriction.

Regulation (EC) No 45/2001 must be read in the light of Directive 95/46/EC. Indeed, the twelfth recital of the Regulation advocates "consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data". Furthermore Article 286 of the Treaty requires that Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data apply to Community institutions and bodies.

Nothing would therefore appear to stand in the way of the application of a similar restriction on the duty to inform and the corresponding right of access during a disciplinary investigation.

The withholding of information during the investigation period is also supported by the fact that no information need be provided concerning the "recipients" of the information during a particular inquiry (see above).

It should be underlined that the terms "not harmful to the investigation" suggest that the actual need to withhold that information must be clearly demonstrated and that the withholding of information can continue only for a defined period. A soon as it is no longer harmful to the investigation, the information must be given to the data subject.

Furthermore, the fair processing of personal data in disciplinary proceedings implies the exercise of the right of defence. In order to exercise that right, the official must normally be in a position to know when proceedings have been initiated against him. Any exception must therefore be strictly limited.

The EDPS therefore considers that it is legitimate for the EIB to provide for restrictions on the obligation to inform where that is strictly necessary for the requirements of a disciplinary investigation.

2.2.9 Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 provides that "the data subject shall have the right to obtain, without constraint, at any time within three months from the receipt of the request and free of charge from the controller:

a) confirmation as to whether or not data related to him or her are being processed;
b) information at least as to the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
c) communication in an intelligible form of the data undergoing processing and of any available information as to their source;
d) knowledge of the logic involved in any automated decision process concerning him or her."

According to the rules on HR archives and the organisation of personal files (Note to all staff, dated 16 December 1998) every member of staff is entitled to consult all the documents in his personal file. Every member of staff is also entitled to make copies of any document in his

personal file. The EDPS therefore does not have any comments to make regarding the data subject's right to access parts of his personal file concerning a possible disciplinary penalty.

However, if a file is compiled during the disciplinary proceedings there are no rules on access to documents in that file. It would appear, however, that not only is that right provided for in Regulation (EC) No 45/2001, but also it is essential to the exercise of the right to defence. Restrictions may, however, be made, since under Article 20 of Regulation No (EC) 45/2001, the right to access may be restricted, in particular where such restrictions constitute a necessary measure to safeguard "the prevention, investigation, detection and prosecution of criminal offences" or "the protection of the data subject or the rights and freedoms of others". The right to access the disciplinary file must therefore be recognized in the light of the restrictions possible under Article 20.

Under Article 14 of Regulation (EC) No 45/2001, the data subject has the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data. Although one cannot speak of the accuracy of certain data in a disciplinary file, the data subject should at least be given the right to contest or supplement certain information in his disciplinary file that he considers inaccurate or incomplete. The EDPS would like the data subject's right to do so to be recognized.

The storage of documents electronically using Electronic Data Management will not replace the Bank's hard copy archives but will facilitate and accelerate consultation. That therefore makes it easier for data subjects to consult their personal files including any possible references to disciplinary penalties in that staff will be able to consult their files directly on computer screens. That will help staff effectively to exercise their right of access as advocated in Article 13 and their right to rectify if appropriate.

2.2.10 Security

Under Article 22 of Regulation (EC) No 45/2001, appropriate security measures must be implemented to ensure a level of security appropriate to the risks represented by the processing and nature of the personal data to be protected. Such measures must be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

Furthermore, Article 21 of Regulation (EC) No 45/2001 provides that persons employed by an institution or body who have access to personal data may not process them except on instructions from the controller.

For that reason, section 3.2. of the EIB Code of Conduct provides that specific measures must be taken to ensure respect for the confidentiality of personal details concerning individual staff members. The members of the Human Resources Department are charged with implementing those measures.

While the present security measures seem to be adequate with regard to Regulation (EC) No 45/2001, the EDPS would point out that the Electronic Data Management (EDM) project increases the risk to data, owing to the fact that they have been computerised, and that security measures should therefore be changed, in particular for those documents in personal files that refer to disciplinary penalties.

Furthermore, if the codification of disciplinary penalties in the Human Resources information system is confirmed, the EDPS stresses that a high level of security must be ensured given the nature of the data stored and also the fact that it is an integrated Human Resources application.

2.2.11 Processing of personal data on behalf of controllers

Under the EDM (Electronic Data Management) project an external company has been given the task of scanning the personal files. That external company must be considered as a "processor" within the meaning of Article 23 of Regulation (EC) No 45/2001. Practical contractual measures have been taken in order to meet the requirements of Article 23. The EDPS would emphasize that there must be tighter security measures for personal files containing documents considered as sensitive, such as any reference to disciplinary penalties.

Conclusion

The processing proposed does not appear to entail any infringement of Regulation (EC) No 45/2001 provided that the observations made above are taken into account.

- While it is useful to include disciplinary measures on the list of codified penalties in the Human Resources information system, it is doubtful whether such processing is genuinely necessary and proportionate. Moreover, the storage of data in this list must be consistent vis-à-vis the possible deletion of data from the personal or disciplinary file, and a person may not appear on the list once his/her career has ended.

- Rules need to be devised on the criteria to be applied before evidence or data are added to a disciplinary file, so that only relevant data are stored. The staff responsible for handling disciplinary files must be made aware of these rules and abide by them.

- A time limit must be established for the storage of data in disciplinary and personal files under Article 4(1)(e) of Regulation (EC) No 45/2001.

- As the data subject is not given any specific information on the processing of the data, general information at least should be supplied on the processing of personal data in the framework of disciplinary proceedings. The EIB may nevertheless legitimately provide for limits on the obligation to inform where strictly necessary for the requirements of a disciplinary investigation.

- The right of access to a disciplinary dossier must be recognized in the light of possible restrictions under Article 20 of Regulation (EC) No 45/2001.

- Data subjects should at least have the right to contest or supplement certain information in their disciplinary files that they consider to be inaccurate or incomplete.

- The encoding of sanctions in the HR system calls for a high level of security given the nature of the data stored and given the fact that it is an integrated Human Resources application.

Brussels, 25 July 2005

Peter HUSTINX
European Data Protection Supervisor