

Opinion on the notification for prior checking received from the Data Protection Officer (DPO) of the Council of the European Union regarding the "Decision on the conduct of and procedure for administrative investigations and the Disciplinary Board within the General Secretariat of the Council" dossier

Brussels, 16 May 2006 (Case 2004-250)

1. Procedure

In a letter received on 22 February 2006, the DPO of the Council of the European Union sent the European Data Protection Supervisor notification for prior checking regarding the draft Decision on the conduct of and procedure for administrative investigations and the Disciplinary Board within the General Secretariat of the Council and the draft Decision concerning the implementing rules for the processing of personal data in connection with administrative investigations and disciplinary proceedings. That procedure had already been identified by the EDPS in his inventory of processing operations which might be subject to prior checking in a letter dated 10 November 2005, under reference 2004/250.

The draft Decision on the conduct of and procedure for administrative investigations and the Disciplinary Board within the General Secretariat of the Council and the draft Decision concerning the implementing rules for the processing of personal data in connection with administrative investigations and disciplinary proceedings were attached to the notification for prior checking.

Questions were put to the Data Protection Officer by e-mail on 11 April 2006. Answers were given on 25 April 2006. Additional information was requested on 4 May 2006. An answer was given on 5 May 2006.

2. Examination of the case

2.1. The facts

Article 86 of the new Staff Regulations of Officials of the European Communities (Staff Regulations) and Articles 49 to 50a and 119 of the Conditions of Employment of Other Servants (CEOS) provide that any failure by an official, a member of temporary staff or a member of contract staff to comply with his obligations makes him liable to disciplinary action. Paragraph 3 of Article 2 (relating to administrative enquiries) of Annex IX (relating to disciplinary proceedings) to the Staff Regulations stipulates that the institutions are to adopt implementing arrangements for that Article, in accordance with Article 110 of the Staff Regulations. Furthermore, Article 30 of Annex IX to the Staff Regulations provides that each institution will, if it sees fit, adopt implementing arrangements for that Annex after consulting its Staff Committee. Section 2 of Annex IX to the Staff Regulations stipulates that a Disciplinary Board is to be established in each institution.

The General Secretariat of the Council (GSC) has adopted a draft Decision containing general provisions on the conduct of and procedure for administrative investigations and the Disciplinary Board within the GSC (hereinafter "the Decision") and a draft Decision concerning the implementing rules for the processing of personal data in connection with administrative investigations and disciplinary proceedings (hereinafter "the Decision concerning the implementing rules"). These data-processing operations have been submitted for prior checking.

The purpose of the data processing is to ascertain facts which may demonstrate failure to comply with obligations under the Staff Regulations or CEOS via an administrative investigation and, where appropriate, enable the Disciplinary Board to issue an opinion and the Appointing Authority (AA) to take disciplinary action in accordance with the Staff Regulations.

The data processing is mainly manual. The data are kept in files (investigation report, personal file and disciplinary file). Processing operations can be carried out by automatic means where computer text files are used. In such cases too, data are kept in a computer file.

The data subjects are all persons who are or have been subject to the Staff Regulations and CEOS.

The categories of data processed are as follows:

- the administrative data of the official or other staff member;
- the personal file of the official or other staff member;
- where applicable, the offences and criminal convictions of the official or other staff member;
- the data used to determine whether there has been failure to comply with the official or other staff member's obligations. It is worth noting with respect to this category that no data-processing operations relating to telephone call traffic – the data processed and stored to establish telephone calls – have been implemented by the GSC to date. Personal data processing in the context of internal telecommunications networks – monitoring of e-mail – is governed by the GSC's Staff Note No 9/03 of 11 February 2003 (Code of Practice for access to Internet services and the use of e-mail), and more specifically by Article 15 of the attached Code of Practice.

Data are liable to be supplied to the following addressees: the relevant department (the Advisers Unit), any person who is the subject of an investigation, the AA of the Council and, where applicable, the Disciplinary Board. In cases falling under their jurisdiction, data may be forwarded within the institution to the specialised financial irregularities panel, the internal audit department or the Security Office and, outside the institution, to the European Anti-Fraud Office (OLAF). The complete file is forwarded to the AA for a decision on further action – in particular in the light of Article 3 of Annex IX to the Staff Regulations – and to the Disciplinary Board should the AA decide to refer the case to it. The complete file is also liable to be forwarded to the above entities should the AA consider that the case falls within their jurisdiction. The complete disciplinary file is submitted to the AA for a decision once the Disciplinary Board has issued its opinion. In the event of a dispute, the file is liable to be referred to the Civil Service Tribunal.

The personal data storage policy is as follows: individual disciplinary decisions are kept in the data subject's personal file in accordance with Article 26 of the Staff Regulations, without prejudice to the possibility of removing these decisions pursuant to Article 27 of Annex IX to the Staff Regulations. Investigation files and disciplinary files are kept in the relevant department's secure archives, in a separate locked cupboard, for 20 years, without prejudice to the provisions of Article 27 mentioned above. The criteria referred to in Article 10, (h) and (i) of Annex IX to the Staff Regulations have been invoked to justify the storage of disciplinary

data during that period. Computer files created during an investigation or a disciplinary procedure may be kept for the same period. Files which are not followed up are kept for that period, in the relevant department's secure archives. On request by the person concerned, a copy of the AA's decision to discontinue the case may be inserted in that individual's personal file.

No deadline has been set for blocking and erasing data.

The data are kept for case-law and statistical purposes; a compendium of anonymised disciplinary decisions is kept for a further 20 years after the 20-year period mentioned above. Access to that compendium is restricted to the AA of the GSC, the Head of the Advisers Unit, officials who have obtained authorisation from the latter, and the Disciplinary Board.

The provisions for informing the data subject are as follows: the decision and the decision concerning the implementing rules are published in a Staff Note circulated to the entire staff. Both decisions are available on the GSC intranet. Any person who is the subject of an administrative investigation is informed at once that the investigation is being opened, except where informing that person may prejudice the investigation's aims. In accordance with Article 2(2) of Annex IX to the Staff Regulations, the Appointing Authority informs the complainant and the persons involved when the investigation ends, and communicates its conclusions and its decision.

During interviews or any other step taken during an investigation, persons called upon to take part are informed of the obligation to maintain the confidential nature of the information.

In the section on the rights of data subjects, the notification refers to the Council Decision of 13 September 2004 (2004/644)¹ adopting implementing rules concerning Regulation (EC) No 45/2001 and, in particular, to section 5 thereof: "Procedure for data subjects to exercise their rights".

Under point 15 of the GSC's Staff Note No 9/03 of 11 February 2006 ("Code of Practice for access to Internet services and the use of e-mail"), the GSC's Data Protection Officer must be informed when the competent departments access any files on the workstation of the data subject or monitor e-mail and Internet use on an individual/workstation basis.

The security measures are as follows:

- access to computer folders and files is severely restricted;
- any data processing is confidential;
- communication of the data is restricted exclusively to persons who need them to fulfil their duties;
- in accordance with Article 26 of the Staff Regulations, the decision taken at the end of the disciplinary procedure is inserted in the personal file of the person concerned. The paper dossiers of the data subjects are filed in the Advisers Unit's secure archives, which are accessible by magnetic cards available only to that Unit's members. Only the Head of Unit possesses a key to the cupboard containing the dossiers. Advisers Unit officials have access only to the dossiers they are responsible for;

¹ Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2004/644/EC).

- computer files relating to the handling of dossiers are kept on the Advisers Unit's server, access being restricted to officials specifically responsible for dealing with these dossiers and to the Head of Unit. Officials have access only to those dossiers they are responsible for.

Procedure relating to the conduct of administrative investigations

Opening of an investigation

The Appointing Authority may decide, on its own initiative or in response to a request or a complaint, to open an administrative investigation in order to ascertain the facts, particularly in the context of Articles 12a, 22a, 24, 86 and 90 of the Staff Regulations. The decision to open an administrative investigation must specify the object and scope of the enquiry. In the case where the Appointing Authority decides, on its own initiative or at the request of the official concerned, to open an administrative investigation for harassment, the person who feels he is suffering harassment may at any time indicate to the Appointing Authority his desire for the investigation to be discontinued. After taking into consideration the individual interests and the interests of the service, the Appointing Authority determines the follow-up to be given to the investigation. No administrative investigation can be conducted as long as OLAF is conducting its own inquiry into the same facts.

Conduct of the investigation

The investigation is conducted by the Advisers Unit of Directorate DGA I B (hereinafter "the relevant department"). By decision of the Appointing Authority, a person external to the relevant department may be involved, if necessary, in the conduct of an investigation. That person may be chosen from inside or outside the institution and, for the purposes of the investigation, is regarded as being part of the relevant department.

The Head of the relevant department must make sure there are no conflicts of interest for persons responsible for conducting the investigation or who are involved in that department under the above paragraph. The investigation must be conducted in confidence and over a period of time which is proportionate to the circumstances and complexities of the case. The relevant department may, in an emergency, propose that the Appointing Authority immediately take the appropriate precautionary measures.

Investigations conducted at the request of a person who claims to be a victim of harassment are regarded as taking priority. To this end, the relevant department must try to present its report within three months after the investigation was referred to it. This period may be extended by the Appointing Authority where circumstances so warrant. The persons concerned are informed of the extension.

Any person who is the subject of an administrative investigation must be informed at once that it is being opened and must be heard in respect of the facts concerning him. He may send the relevant department comments in writing and/or other documents.

In cases where informing and/or hearing a person who is the subject of an investigation may prejudice the aims of that investigation, compliance with the obligation to inform and/or to hear him during the investigation may be suspended by decision of the Appointing Authority at the request of the relevant department. In any case, conclusions which implicate a person cannot be drawn unless that person has been able to express his opinion on the facts concerning him. The conclusions must set out this opinion.

All evidence, including documents and written comments submitted by the person concerned, must be inserted into the investigation file.

Means available to conduct the investigation

In order to establish the facts, the relevant department, subject to legal or statutory requirements, may carry out on-the-spot inspections, interview any person who may be able to clarify the facts, and have access to any kind of document and existing administrative data which proves necessary for continuing the investigation, especially personal files. It may also request the assistance of any department of the General Secretariat of the Council.

Information forwarded or obtained in the course of administrative investigations by the relevant department (for the purposes of ascertaining the facts), in whatever form, is subject to professional secrecy and enjoys the protection given by Regulation (EC) No 45/2001 and/or other provisions applicable to the Council.

Investigation report

At the end of the investigation, the relevant department submits an investigation report to the Appointing Authority. Copies of all the relevant documents are attached to the investigation report. The investigation report must set out the facts and circumstances in question, indicate whether the rules and procedures applicable to the situation were respected, determine if appropriate the individual responsibilities whilst taking account of aggravating or mitigating circumstances, formulate conclusions and propose, if appropriate, measures to be taken.

Such measures may include: closing the investigation with no further action; opening disciplinary proceedings, with or without the involvement of the Disciplinary Board and referral to the specialised financial irregularities panel, to OLAF, to the internal audit department or to the Security Office; or adopting staff management or departmental organisation measures.

The closure of the administrative investigation does not prevent the investigation from being reopened on the basis of new facts.

Follow-up of the investigation

The investigation report is examined by the Appointing Authority, which takes the measures it deems appropriate. In accordance with Article 2(2) of Annex IX to the Staff Regulations, the Appointing Authority informs the complainant and the persons involved when the investigation ends, and communicates its conclusions and its decision.

Disciplinary Board

The chairman of the Disciplinary Board is chosen from among the former or serving officials in grade AD 16 of the other European institutions or among the former members of those institutions. The chairman's alternate is appointed from among the serving officials in AD 16 or AD 15 who perform the duties of Director-General or Deputy Director-General.

Representation of the institution before the Disciplinary Board, as provided for in Article 16(2) of Annex IX to the Staff Regulations, is performed by a member of the Advisers Unit of Directorate DGA 1 B, designated by the Head of Unit.

Publication of the results of disciplinary cases

Disciplinary decisions adopted, or summaries thereof, must be published annually, making sure that no mention is made of the names of persons involved or any other information that might allow them to be identified. The Disciplinary Board may have access to a compendium, rendered anonymous, of disciplinary decisions at the GSC, insofar as this proves necessary for the adopting of an opinion in a particular case.

2.2. Legal aspects

2.2.1. Prior checking

The notification received on 22 February 2006 relates to the processing of personal data ("any information relating to an identified or identifiable natural person" – Article 2(a)) by a Community institution in the exercise of activities all or part of which fall within the scope of Community law. The management of data regarding administrative investigations and the Disciplinary Board of the GSC involves the collection, recording, organisation, storage, retrieval, consultation, etc. of personal data (Article 2(b) of Regulation (EC) No 45/2001). These activities constitute partly automated processing and, when processing is manual, the data are contained in a filing system – i.e. the investigation file, the disciplinary file where applicable and the personal file in the case of the decision taken at the end of the disciplinary procedure – within the meaning of Article 3(2) of the Regulation. The data 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 liable to present such risks. Administrative investigations and Disciplinary Board proceedings must be subject to prior checking for several reasons. They can contain data relating to suspected offences, offences, criminal convictions or security measures, within the meaning of Article 27(2)(a). Furthermore, these processing operations are intended to evaluate personal aspects relating to the data subjects, including in particular their conduct, and are therefore covered by Article 27(2)(b).

This prior checking exercise concerns the processing of personal data in connection with administrative investigations and disciplinary proceedings. The purpose is not to give an opinion on the administrative investigations and disciplinary procedures themselves.

The EDPS welcomes the provision in the Decision's Article 4(2) to the effect that information processed in the course of administrative investigations enjoys the protection given by Regulation (EC) No 45/2001. However, he regrets the fact that the above Regulation is referred to only in connection with the powers of the relevant department.

The DPO's notification was received on 22 February 2006. Under Article 27(4), this opinion had to be delivered within the following two months. The EDPS should therefore have delivered his opinion by 23 April 2006. Owing to two requests for additional information, the deadline was suspended for 13 + 1 days. In order to enable the DPO to provide the additional information and relevant comments, the deadline was suspended for a further ten days. The EDPS therefore had to deliver his opinion by 17 May 2006.

2.2.2. Legal basis and lawfulness of the processing operation

The legal basis for the data processing is the two planned decisions, which are yet to be adopted; these are themselves based on Article 86 of the Staff Regulations and Annex IX thereto (in particular Article 2(3) – "The institutions shall adopt implementing arrangements for this Article, in accordance with Article 110 of the Staff Regulations" – and Article 30 – "Without prejudice to Article 2(3), each institution shall, if it sees fit, adopt implementing arrangements for this Annex after consulting its Staff Committee"). These provisions apply by analogy to temporary and contract staff members (Articles 49 to 50a and 119 of the CEOS). The legal basis is therefore valid.

Alongside the legal basis in relation to Regulation (EC) No 45/2001, 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". Administrative investigations and disciplinary procedures which involve collecting and processing personal data relating to officials or other servants come under the legitimate exercise of official authority vested in the institution. The processing is therefore lawful. The legal basis found in the Staff Regulations of Officials of the European Communities (Article 86 and Annex IX) also supports the lawfulness of the processing operation.

2.2.3. Processing of special categories of data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning the health or sex life of an individual are liable to be processed in the course of administrative investigations and Disciplinary Board proceedings.

The EDPS wishes to give the controller a word of caution as regards use of such data. The processing must be "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" (Article 10(2)(b)). The other exemptions provided for in Article 10(2) could also apply. In the case in point, the GSC has an obligation to ensure that its staff members do not fail to comply with their professional obligations. Accordingly, if such data appear in the context of investigations, they must be relevant to the case and proportionate to the intended purpose. The processing operation must comply with Article 10(2) of Regulation (EC) No 45/2001.

Administrative investigation files and disciplinary files are liable to contain data relating to offences, criminal convictions or security measures; processing of such data is subject to authorisation in accordance with Article 10(5) of Regulation (EC) No 45/2001. The decisions implementing Article 86 of the Staff Regulations and, by analogy, Articles 49 to 51 and 119 of the CEOS should be regarded as an authorisation to process these data.

2.2.4. Data quality

Article 4 of Regulation (EC) No 45/2001 lays down certain obligations as regards personal data quality. These data must be "adequate, relevant and not excessive" (Article 4(1)(c)) in

relation to the purposes for which they are collected. The EDPS acknowledges that it is difficult to identify from the outset which data are relevant for the purposes of the investigation. There is no systematic rule regarding the nature of data which can be included in administrative investigation or disciplinary procedure files. The nature of the data to be kept in these files depends to a large extent on the case in point. Article 1(2) of the draft Decision on the conduct of administrative investigations stipulates that "the decision to open an administrative investigation must specify the object and scope of the enquiry". That is a significant provision given the extent of the data collected and stored in the course of the procedure. Article 4(1) of the draft Decision provides that the relevant department has access to documents and administrative data "which [prove] necessary for continuing the investigation". Given this – necessarily broad – access to documents, the EDPS considers that the inclusion of such data into the investigation files must be governed by instructions quoting Article 4(1)(c) of Regulation (EC) No 45/2001 with a view to encouraging greater caution with respect to collecting evidence or data in an investigation file. Staff called upon to conduct administrative investigations must be given these instructions and must follow them. The instructions applicable to investigation files should also be applicable to Disciplinary Board reports (Article 15 of Annex IX to the Staff Regulations) and to disciplinary files.

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, the issue of fairness warrants considerable attention. It is linked to the information to be given 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. In particular, a copy of all decisions of the Appointing Authorities should be inserted in the disciplinary file. Any subsequent amendments or corrections should also compulsorily be inserted in the file. Data subjects' right of access to their data is a further means of ensuring that the data are accurate and up-to-date (see section 2.2.9 below on right of access and rectification).

2.2.5. Confidentiality of communications

Under Article 36 of Regulation (EC) No 45/2001, "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".

Electronic communications which are tapped in the course of administrative or disciplinary investigations come under Article 36 of Regulation (EC) No 45/2001; any restriction of the confidentiality principle must be "in accordance with the general principles of Community law". The concept of "general principles of Community law" refers to the fundamental human rights enshrined in particular in the European Convention on Human Rights.

In practice, this means that any restriction on the principle of confidentiality of communications must be consistent with the fundamental human rights enshrined in the European Convention on Human Rights. Such restriction may take place only if it is "in accordance with the law" and "is necessary in a democratic society" in the interests of national security, public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The GSC has excluded the possibility of processing data relating to the content of telephone calls.

The fact that the GSC Data Protection Officer is kept informed² when the competent departments access any files on the workstation or monitor e-mail and Internet use on an individual/workstation basis is an additional guarantee of compliance with Article 36 of the Regulation. That point is particularly important; accordingly, the EDPS would invite the GSC to refer to the DPO's information requirement in one of the two decisions planned by the GSC.

The EDPS consequently considers that the confidentiality of communications can be infringed only in exceptional circumstances (in the course of inquiries within the framework of an administrative investigation where no other less invasive method could be used), that infringing the confidentiality principle should be an extraordinary procedure and that it must always be restricted to those data which are strictly necessary.

2.2.6. Data retention

Under Article 4(1)(e) of Regulation (EC) No 45/2001, 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.

Individual disciplinary decisions are kept in the relevant data subject's personal file in accordance with Article 26 of the Staff Regulations, without prejudice to the possibility of deleting these decisions pursuant to Article 27 of Annex IX to the Staff Regulations. As has been set out above, investigation files (whether followed up or not) and disciplinary files are kept for 20 years, without prejudice to the provisions laid down in Article 27 referred to above. Computer files created during an investigation or a disciplinary procedure have the same retention period. The EDPS is satisfied with the retention period set by the GSC for investigation files (whether followed up or not) and disciplinary files.

As regards cases which are not followed up, the EDPS welcomes the fact that, on request by the person concerned (in accordance with Article 29 of Annex IX to the Staff Regulations), a copy of the Appointing Authority's decision not to follow up the case should be inserted in his personal file.

Under Article 27 of Annex IX to the Staff Regulations, an official against whom a disciplinary penalty other than removal from post has been ordered may, after three years in the case of a written warning or reprimand or after six years in the case of any other penalty, submit a request for the deletion from his personal file of all reference to that measure. The Appointing Authority decides whether to grant this request. The disciplinary decision can therefore be deleted from the personal file, but at the discretion of the Appointing Authority. Accordingly, the data subject does not have an automatic right to deletion of the data after a certain lapse of time.

However, in the interests of fairness to the data subject, the Appointing Authority must justify the need to keep the data and any refusal to delete the data where an official submits a request to that effect under Article 27 of the Staff Regulations.

² See point 15 of Staff Note No 9/03 of 11 February 2003 (Code of Practice for access to Internet services and the use of e-mail).

Under Article 4(1)(e) of Regulation (EC) No 45/2001, data kept by the GSC beyond the period that is necessary for the purposes for which they were collected (the compendium of disciplinary decisions) must be rendered anonymous. Article 4(1)(e) is therefore complied with in this respect.

Article 37(1) provides for specific rules as regards storage of traffic data, i.e. data relating to calls and other connections on telecommunications networks. In principle, these data must be erased or made anonymous upon termination of the call or connection.

For the moment, the GSC does not process data relating to telephone call traffic but has not excluded that possibility. If the GSC were to process such data in future in the course of an administrative investigation, it would have to do so in accordance with Articles 20 and 37 of Regulation (EC) No 45/2001. Furthermore, as the processing of these data is particularly sensitive – Article 37 of the Regulation is devoted to that issue – the EDPS invites the GSC to consult him if operations are set up to process data relating to telephone call traffic.

However, the GSC does process data relating to Internet connections and use of e-mail. Article 20 of the Regulation provides for exemptions from Articles 4(1) and 37(1) in particular when the retention of data constitutes a necessary measure to safeguard "the prevention, investigation, detection and prosecution of criminal offences" or "the protection of the data subject or of the rights and freedoms of others". According to the EDPS's interpretation of these exemptions (see section 2.2.10 on information to be given to the data subject), they apply to administrative investigations and disciplinary measures.

2.2.7. Change of purpose/compatible use

Data are retrieved from or entered into the staff databases. The processing operation under review involves no general change to the stated purpose of staff databases, of which administrative investigations and disciplinary procedures are only one aspect. 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.

2.2.8. Transfer of data

The processing operation should also be scrutinised in the light of Article 7(1) of Regulation (EC) No 45/2001. The processing covered by Article 7(1) is the transfer of personal data 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".

For the purposes of Article 7(1), this prior checking concerns the transfer of personal data within the institution (relevant department, Appointing Authority, Director-General for Administration and Disciplinary Board) and between institutions (OLAF). However, the parties referred to are not recipients within the meaning of Article 2(g): they may receive data in the framework of a particular inquiry and are therefore included in the exemption provided for under that article. In this context, Article 2(g) must be understood as an exemption regarding the right to information (see section 2.2.10 on information to be given to the data subject) rather than as an exemption from Article 7.

Article 7(3) of the Regulation provides that "the recipient shall process the personal data only for the purposes for which they were transmitted". There must be an explicit guarantee that

no-one receiving and processing data in the context of an administrative investigation or disciplinary procedure within the GSC can use them for other purposes. The latter point is particularly important where a person from outside the relevant department is involved in the investigation. The European Data Protection Supervisor wishes the GSC to give particular attention to the fact that personal data should be processed strictly within the framework of administrative investigations and disciplinary procedures.

2.2.9. Right of access and rectification

Under Article 13 of Regulation (EC) No 45/2001, "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: (...) 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; [and] communication in an intelligible form of the data undergoing processing and of any available information as to their source". Article 14 provides that "the data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data".

While the right of access and rectification may be restricted, under Article 20, to safeguard the prevention, investigation, detection and prosecution of criminal offences and the protection of the data subject or of the rights and freedoms of others (see section 2.2.10 on information to be given to the data subject for the EDPS's interpretation of that restriction), it must first be ensured. Accordingly, the EDPS requests that the right of access, as provided for by Regulation (EC) No 45/2001, be explicitly granted to the data subject, within the limits of the exceptions set out in Article 20 (see section 2.2.10 on information to be given to the data subject). Article 3(5) and (6) of the Decision seem to provide implicit acknowledgement of that right of access; however, they do not clearly establish that the data subject does indeed have access to his investigation file.

As regards right of rectification, the data subject has the right to obtain from the controller rectification without delay of inaccurate or incomplete personal data (Article 14 of Regulation (EC) No 45/2001). The EDPS notes that, in the context of an "evaluation of conduct", it is hard to establish whether personal data are "inaccurate" or not. The fact that the data subject can send comments in writing and other documents (as provided for in Article 3(5) of the Decision) and that these comments and other documents are inserted in the investigation file is a means of ensuring the right of rectification. The right of rectification is therefore respected in the case in point.

Furthermore, the EDPS is satisfied with Article 3(6) of the Decision, which stipulates that "in any case, conclusions which implicate a person cannot be drawn unless that person has been able to express his opinion on the facts concerning him. The conclusions shall set out this opinion." That is a means of guaranteeing fair processing.

Lastly, the EDPS welcomes Article 24 of Section 5 of the Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2004/644/EC), which provides that the controller must consult the Data Protection Officer if he decides to restrict the rights provided for under Articles 13 to 17 of Regulation (EC) No 45/2001. That is an additional safeguard for the data subject.

The other persons involved in the investigation should also, as far as possible, be granted the right to rectify their personal data.

2.2.10. Information to be given to the data subject

Under Articles 11 and 12 of the Regulation, whenever personal data are processed, data subjects must be sufficiently informed about the operation. This information should usually be supplied at the latest when the data are obtained from the data subject if the data subject has not already been informed (Article 11). If the data are not obtained directly from the data subject (Article 12), the information must be supplied as soon as the data are recorded or, if the data are to be disclosed to a third party, when the data are first disclosed, at the latest.

Personal data in an investigation file can be obtained not only from the data subject but also from third parties. The information must therefore be provided when the data are collected, i.e. before they are registered or forwarded to third parties.

Under the decision, any person who is the subject of an administrative investigation must be informed at once that it is being opened, except if this may prejudice the investigation's aims.

Under Article 20 of Regulation (EC) No 45/2001, that obligation to inform may be restricted, in particular when such a restriction constitutes "a necessary measure to safeguard: (a) the prevention, investigation, detection and prosecution of criminal offences; (b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others."

Restriction on the grounds of possible prejudice to the aims of the administrative investigation is justified in particular to safeguard "the protection of the data subject or of the rights and freedoms of others" and "the prevention, investigation, detection and prosecution of criminal offences", but the scope is in fact far broader. It may be necessary to avoid informing the data subject not only to protect witnesses ("rights and freedoms of others"), but also to ensure that the investigation is conducted properly. If the investigation does not concern a criminal offence, Article 20 of Regulation (EC) No 45/2001 does not, *stricto sensu*, provide for an exemption.

Nonetheless, the EDPS considers that Article 20 should be interpreted in the light of the underlying principle of the provision in order to provide for certain restrictions to the obligation to inform the data subject in the course of an internal investigation. In support of that idea, Article 13 of Directive 95/46/EC provides for exemptions and restrictions regarding 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(d) of the Directive has a broad scope ranging from the prevention, investigation, detection and prosecution of criminal offences to breaches of ethics for regulated professions. Accordingly, and while that is not explicitly set out, there is no reason to suppose that disciplinary misconduct of public-sector officials and other staff members is not included in that restriction.

Regulation (EC) No 45/2001 should be read in the light of Directive 95/46/EC. Recital 12 of the Regulation calls for "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 the application to the

Community institutions and bodies of Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data. There therefore seems to be no reason not to apply a similar restriction to the obligation to inform and corresponding access right in the course of a disciplinary investigation. Non-disclosure of information during the investigation period is also supported by the fact that no information needs to be supplied as regards the recipients of the data in the course of a given investigation.

It is worth stressing that the phrase "where informing (...) may prejudice the aims [of the investigation]" suggests that the need to avoid giving the information must be clearly established and the non-disclosure of information may not last beyond a specific period. The information should be given to the data subject as soon as that can no longer prejudice the aims of the investigation.

The EDPS approves of the fact that, in accordance with Article 2(2) of Annex IX to the Staff Regulations, the Appointing Authority informs the persons involved and the complainant when the investigation ends, and communicates its conclusions and its decision.

The EDPS welcomes the fact that the persons who are the subject of an investigation relating to harassment are informed when the three-month investigation deadline is prolonged.

He commends the decision for clearly setting out the various time-limits for storing data in general. However, as regards investigation reports which are not followed up, the EDPS calls on the GSC to inform data subjects of the storage time-limit.

The EDPS welcomes the fact that the decision mentions the legal basis for the data processing. However, in the case in point, the legal basis for the processing is split among several documents (Staff Regulations, Annex IX to the Staff Regulations, Decision and Decision concerning the implementing rules). The EDPS invites the GSC to draw up a document – an informative note – describing the processing as a whole in a single document so as to ensure fair processing of data for the data subjects.

He also approves of the fact that the decision should mention the possibility, under Article 27 of Annex IX to the Staff Regulations, for an official against whom a disciplinary penalty has been ordered, after three years in the case of a written warning or reprimand or after six years in the case of any other penalty, to submit a request for the deletion from his personal file of all reference to that measure.

There is no need to give information regarding the transfer of the file within the institution specifically to the data subject because the institution's authorities are not recipients within the meaning of Article 2(g) of the Regulation. The EDPS welcomes the fact that the general information should be in the Decision, thus ensuring that the procedure is transparent.

The EDPS wishes data subjects to be informed of their right of access within the limits of the exemptions provided for under Article 20. The Decision concerning the implementing rules is an excellent means of supplying that information. It would also be desirable to refer to Section 5 of the Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2004/644/EC).

The EDPS would also call on the GSC to refer to Council Staff Note No 9/03 of 11 February 2003 on the code of practice for access to Internet services and the use of e-mail.

To ensure that the data are processed fairly, Article 12 of the Regulation stipulates, *inter alia*, that the data subject must be informed of the categories of data concerned. In the case before us, no mention is made of the processing of data relating to internal telecommunication networks despite the fact that the GSC has drawn up specific rules in this respect. The above Staff Note contains a point 15, devoted to investigative rights.

The EDPS requests that the Decision concerning the implementing rules should mention the right to have recourse at any time to the European Data Protection Supervisor, as being necessary to ensure that data subjects are duly informed of all means at their disposal.

2.2.11. Security

Following in-depth examination of the security measures in place, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) No 45/2001.

The EDPS is gratified that organisational measures are taken to ensure a level of security appropriate to the risks represented by the processing and to the nature of the personal data to be protected, in particular by issuing strict rules regarding confidentiality. The technical security measures also appear to be appropriate.

Conclusion

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

- The GSC should give particular attention to the use of specific categories of data; these must be relevant to the case and proportionate to the intended purpose so as to comply with Article 10(2) of Regulation (EC) No 45/2001.
- Instructions quoting Article 4(1)(c) should be drawn up to encourage greater caution with respect to inserting and collecting evidence or data in an investigation file. Staff called upon to conduct administrative investigations must be given these instructions and follow them. The instructions applicable to the investigation files should also be applicable to Disciplinary Board reports (Article 15 of Annex IX to the Staff Regulations) and to disciplinary files.
- A copy of all decisions of the Appointing Authority should be inserted in the disciplinary file. Any subsequent amendments or corrections should also be inserted in the file.
- If the GSC were in future to process data relating to telephone call traffic for the purposes of an administrative investigation, it would have to do so in accordance with Articles 20 and 37 of Regulation (EC) No 45/2001. Furthermore, the EDPS must be consulted if operations for the processing of data relating to electronic communications traffic are set up in future.
- Mention should be made in one of the two decisions planned by the GSC of the fact that the Appointing Authority must inform the DPO whenever it instructs the competent departments to monitor electronic communications.

- Right of access, as provided for by Regulation (EC) No 45/2001, should be explicitly granted to the data subject, within the limits of the exemptions set out in Article 20.
- Other persons involved in the investigation should, as far as possible, be granted the right to rectify their personal data.
- The GSC should provide data subjects with information regarding the time-limits for storing investigation reports which are not followed up.
- The GSC should draw up a document – an informative note – describing the processing as a whole in a single document so as to ensure fair processing of data for data subjects.
- Data subjects should be informed of their right of access within the limits of the exemptions provided for under Article 20. It would also be desirable to refer to Section 5 of the Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2004/644/EC).
- Reference should be made to Council Staff Note No 9/03 of 11 February 2003 on the Code of practice for access to Internet services and the use of e-mail.
- The Decision concerning the implementing rules should mention the right to have recourse at any time to the European Data Protection Supervisor, as that is necessary to ensure that data subjects are duly informed of all means at their disposal.

Done at Brussels, 16 May 2006

P. HUSTINX
European Data Protection Supervisor