Opinion on the notification for prior checking from the European Ombudsman's Data Protection Officer regarding the "disciplinary proceedings and administrative investigations" dossier

Brussels, 17 October 2007 (Case 2007-0413)

1. Procedure

By letter received on 19 June 2007 the European Ombudsman's Data Protection Officer (DPO) served notification within the meaning of Article 27(3) of Regulation (EC) No 45/2001 on "disciplinary proceedings and administrative investigations". This notification is accompanied by a copy of the implementing arrangements for disciplinary proceedings and administrative investigations.

Further information was requested from the DPO on 26 July 2007. A reply was sent on 21 September 2007. The opinion was sent to the DPO for comments on 11 October 2007. Comments were received on 16 October 2007.

2. The facts

Under Article 86 of the Staff Regulations of officials of the European Communities, "any failure by an official or former official to comply with his obligations under these Staff Regulations, whether intentionally or through negligence on his part, shall make him liable to disciplinary action". Disciplinary rules, procedures and measures and the rules and procedures covering administrative investigations are laid down in Annex IX to the Staff Regulations.

Articles 49, 50, 50a and 119 of the Conditions of Employment of other servants of the European Communities lay down a similar mechanism for temporary and contract staff members.

Under Article 2(3) of Annex IX to the Staff Regulations of officials of the European Communities, "the institutions shall adopt implementing arrangements for this Article, in accordance with Article 110 of the Staff Regulations". The European Ombudsman has adopted general implementing provisions (GIP) governing disciplinary proceedings and administrative investigations relating to disciplinary proceedings and they became applicable as from 1 May 2004. Those general implementing provisions are published on the European Ombudsman's Intranet site. They apply to all the European Ombudsman's statutory personnel (officials, temporary staff and contract staff).

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

Administrative investigations

Before initiating disciplinary proceedings, heads of units may ask the Appointing Authority to open an administrative investigation. The Appointing Authority may also open an administrative investigation on its own initiative. The decision to open an administrative investigation must specify its object and scope and assign one or more officials or other servants to conduct it.

In cases of alleged financial fraud for which OLAF has launched an investigation or intends to do so, the Appointing Authority may postpone the launch of an administrative investigation and/or where appropriate, disciplinary proceedings until OLAF has completed its investigation (Article 1(4) of the GIP).

The official or other servant responsible for the investigation is empowered to obtain documents, request information from anyone he/she sees fit to question and carry out on-the-spot checks.

Conclusions referring to an official or other servant of the institution by name may not be drawn at the end of the investigation unless that person has had the opportunity to express an opinion on all the facts which relate to him or her in the presence of the official or other servant responsible for the investigation.

At the end of the investigation, the official submits a report to the Appointing Authority. That report sets out the facts and circumstances in question; it establishes whether the rules and procedures applicable to the situation were respected; it takes note of any aggravating or mitigating circumstances; it details the extent of the damage suffered by the Institution and makes a recommendation on action to be taken. Copies of all relevant documents and records of any hearings are attached to the report.

The Appointing Authority informs the official concerned when the investigation ends and communicates to him the conclusions of the investigation report and, on request and subject to the protection of the legitimate interests of third parties, all documents directly related to the allegations made against him (Article 2(3) of the GIP and Article 2(2) of Annex IX to the Staff Regulations of the European Communities).

On the basis of the investigation report and after the official concerned has been notified of all evidence in the file, he/she is heard at a preliminary hearing. The record of the hearing is forwarded to the official concerned by registered letter with acknowledgement of receipt, for signature. The official forwards the signed record and/or his comments and remarks within 15 calendar days of receipt. Failure do to so within that period will result in the record being considered as approved.

If, in accordance with Article 3(1)(a) of Annex IX to the Staff Regulations, the Appointing Authority decides that no case can be made against the official or other servant concerned, it will inform him/her by registered letter with acknowledgement of receipt. The official may request that a copy of this letter be inserted in his personal file (Article 4 of the GIP).

If the Appointing Authority decides to take no disciplinary action or to address a warning to the official concerned, the latter is informed by registered letter with acknowledgement of receipt. A copy of this letter is not inserted in the official's personal file (Article 5 of the GIP).

The Appointing Authority may decide on the penalty of a written warning or reprimand without consulting the Disciplinary Board (Article 11 of Annex IX to the Staff Regulations). The decision is inserted in the official's personal file. A copy of the decision is forwarded to the official concerned by registered letter with acknowledgement of receipt (Article 6 of the GIP).

Disciplinary proceedings

If the Appointing Authority decides to initiate disciplinary proceedings before the Disciplinary Board, it must do so by means of a report submitted to the chairman of the Board. A copy of the report is forwarded to the official concerned.

The Disciplinary Board's opinion is forwarded to the Appointing Authority and to the official concerned.

Pursuant to Article 14 of Annex IX to the Staff Regulations, if, in the presence of the Chairman of the Board, the official concerned acknowledges misconduct on his part and accepts unreservedly the report referred to in Article 12 of that Annex, the Appointing Authority may withdraw the case from the Board. Where a case is withdrawn from the Board the Chairman delivers an opinion on the penalty considered. The official concerned must be informed before acknowledging his misconduct of the possible consequences of such acknowledgement. He may ask for a hearing or put his views in writing. The original of the Appointing Authority's decision is inserted in the official's personal file. (Article 7(3) of the GIP).

On receipt of the opinion of the Disciplinary Board and after hearing the official concerned, the Appointing Authority decides on the disciplinary penalty. The Administration and Finance Department is responsible for applying it. The original of the decision is inserted in the personal file of the official concerned. The official receives a copy by registered letter with acknowledgement of receipt.

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 such measure. The Appointing Authority decides whether to grant this request (Article 27 of Annex IX to the Staff Regulations).

Individual documents inserted in the investigation file and disciplinary files are stored for 50 years in order to cover the career of the person or persons to whom the investigation relates and to ensure that the institution is able to take account of all matters affecting the assessment of points (h) and (i) of Article 10 of Annex IX. That Article stipulates that "*the severity of the disciplinary penalties imposed shall be commensurate with the seriousness of the misconduct. To determine the seriousness of the misconduct and to decide upon the disciplinary penalty to be imposed, account shall be taken in particular of: ... (h) whether the misconduct involves repeated action or behaviour,* (i) *the conduct of the official throughout the course of his career*". The individual documents inserted in the data subject's personal file are stored until he reaches the age of 70.

[...]

In addition to the members of the department handling the files (Administration Sector, personnel team), data may be communicated internally in whole or in part to the Appointing Authority, to the Secretary-General and to Heads of Department; to the persons designated by

the Appointing Authority to carry out an investigation; to the Disciplinary Board and to the persons being investigated. They may also be communicated outside the institution to the persons being investigated; to OLAF; to the Civil Service Tribunal; to the European Parliament security service; to the competent national authorities where there is an infringement of national law.

3. Legal aspects

3.1. Prior checking

The notification received on 19 June 2007 relates to the processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2(a) of Regulation (EC) No 45/2001, hereinafter "the Regulation") by a Community body in the exercise of activities all or part of which fall within the scope of Community law. The management of data for disciplinary proceedings and administrative investigations involves the collection, recording, organisation, storage, retrieval, consultation, etc. of personal data (Article 2(b)). These activities constitute partly automated processing and the data are contained in a file within the meaning of Article 3(2). The data processing therefore falls within the scope of Regulation No 45/2001.

Article 27(1) of Regulation No 45/2001 requires prior checking by the EDPS of all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*".

Article 27(2) of the Regulation contains a list of processing operations likely to present such risks. Disciplinary files 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 documents are intended to evaluate personal aspects relating to the data subjects, including in particular their conduct (Article 27(2)(b)).

The prior check set out below concentrates on administrative investigations and disciplinary files. It applies to personal files only to the extent that those files include disciplinary measures. Moreover, the prior checking exercise concerns only the processing of personal data in connection with administrative investigations or disciplinary files. It is not its purpose to provide an opinion on the actual disciplinary proceedings.

In principle, checking by the EDPS 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 carried out ex-post. This does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented.

The DPO's notification was received on 19 June 2007. Under Article 27(4) this opinion must be delivered within two months. The deadline was suspended for 26 days, for the month of August and for 5 days for comments. The EDPS will therefore deliver his opinion by 21 October 2007. As that is a Sunday, the opinion must be delivered by 22 October 2007.

3.2. Lawfulness of the processing

The lawfulness of the processing operations must be examined in the light of Article 5(a) of Regulation (EC) No 45/2001, which provides that 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 in the legitimate exercise of official authority vested in the Community institution".

It is therefore necessary to determine whether the processing operation has been carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments on the one hand, and whether that operation is necessary in order to perform the task involved on the other.

Under Article 86(1) of the Staff Regulations, "any failure by an official or former official to comply with his obligations under these Staff Regulations, whether intentionally or through negligence on his part, shall make him liable to disciplinary action." Article 86(3) provides that "Disciplinary rules, procedures and measures and the rules and procedures covering administrative investigations are laid down in Annex IX"[1]. On the basis of Article 2(3) of Annex IX to the Staff Regulations, General Implementing Provisions governing disciplinary proceedings and administrative investigations have been adopted by the European Ombudsman. Processing is therefore based on a task to be performed in the public interest as provided for in the Staff Regulations and is necessary for the performance of that task. The legal basis therefore supports the lawfulness of the processing.

3.3. Processing of special categories of data

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, is prohibited in principle pursuant to Article 10(1) of the Regulation.

It is not possible to rule out the possibility of particular categories of data within the meaning of Article 10 of Regulation No 45/2001 being processed in the course of administrative investigations or disciplinary proceedings. In such cases the EDPS would stress that processing must be provided for under one of the exemptions in Article 10(2) of the Regulation, derogating from the prohibition. Article 10(2)(b) provides that the prohibition on processing sensitive data does not apply where processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof. Processing of personal data in connection with an administrative investigation or disciplinary proceedings may be based on Article 86 of the Staff Regulations and thus qualify for the exemption provided for in Article 10(2)(b) on condition that proof is provided that the data are necessary in the context of that investigation or those proceedings. The person responsible for the investigation must be reminded of the particularly sensitive nature of the data.

Processing of data is also covered by Article 10(5) of the Regulation insofar as the data may relate to offences. However, such processing is permitted only by virtue of the fact that it is based on a legal obligation as referred to in Article 86 of the Staff Regulations.

[1] Articles 49, 50, 50a, and 119 of the Conditions of Employment of other servants of the European Communities provide that these provisions also apply to temporary and contract staff.

3.4. Quality of the data

Article 4 of Regulation No 45/2001 sets out a number of obligations regarding the quality of personal data.

The data must be "*processed fairly and lawfully*" (Article 4(1)(a)). The lawfulness of the processing has already been discussed (see point 3.2 above). Fairness relates to the information given to the data subjects (see point 3.9 below on this point).

Personal 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(1)(c)). The EDPS recognises that it is difficult to determine, at the outset, which data are relevant to the subject of the investigation, but vigilance in this respect must be laid down as a general requirement.

Article 4(1)(d) of the Regulation stipulates that "*data must be (…) accurate and, where necessary, kept up to date*". The procedure itself must guarantee the accuracy of the data. The EDPS is satisfied that the data subject receives a copy of the conclusions of the investigation and, on request, all documents directly linked to the allegations made, subject to the protection of the legitimate interests of third parties, and is thus in a position to verify that the data are accurate and up to date.

The record of the hearing is also forwarded to the official concerned by registered letter with acknowledgement of receipt, for signature. The official forwards the signed record and/or his comments and remarks within 15 calendar days of receipt. That also contributes to ensuring that the data are accurate and kept up to date (we will return to that point in relation to the right of rectification in 3.9).

3.5. Confidentiality of communications

Although the notification does not mention tapping of communications, the GIP empower the official or other servant conducting the investigation "to obtain documents, to request information from any person he/she sees fit to question and to carry out on-the-spot inspections" (Article 2(2) of the GIP). There is thus a possibility that the official or other servant responsible for conducting the investigation may seek to intercept telephone calls or e-mails in order to obtain the information required for the investigation.

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".

Tapping of electronic communications in the course of administrative or disciplinary investigations comes under Article 36 of Regulation (EC) No 45/2001 and any restriction of the confidentiality principle must therefore 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 or 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 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. He therefore wishes those restrictions to be taken into account in the conduct of administrative investigations and disciplinary proceedings. He recommends that a procedure be clearly established for the conduct of any tapping of electronic communications.

3.6. Storage of data

Under Article 4(1)(e) of Regulation 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*".

Data relating to administrative investigations and disciplinary proceedings are stored for 50 years in the data subject's investigation file and disciplinary files and the individual documents are inserted in the data subject's personal file and are stored until he reaches the age of 70.

- *Storage in the data subject's personal file*

In accordance with the GIP, the personal file will include all decisions taken in the context of disciplinary proceedings except for decisions by the Appointing Authority not to take any disciplinary action (unless an official requests otherwise), and any warnings addressed to the official.

The institution justifies the storage of these data in the personal file throughout an official's career on the basis of Article 10(h) and (i) of Annex IX to the Staff Regulations which provide that "the severity of the disciplinary penalties imposed shall be commensurate with the seriousness of the misconduct. To determine the seriousness of the misconduct and to decide upon the disciplinary penalty to be imposed, account is taken in particular of … (h) whether the misconduct involves repeated action or behaviour; (i) the conduct of the official throughout the course of his career".

Pursuant to 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 references to such measure. The Appointing Authority decides whether to grant this request. Certain information may therefore be removed from the personal file, but this is done 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, it follows from the data protection rules that the Appointing Authority must justify the need to store the data and any refusal to delete them if an official requests deletion under Article 27 of Annex IX to the Staff Regulations.

Points (h) and (i) of Article 10 are also invoked to justify storing disciplinary data in the personal file *after* the end of the career of the official or other servant, until he reaches the age of 70. The EDPS does not, however, consider that storing such information in the personal file until the data subject reaches the age of 70 is justified in the event of early retirement. In such cases, data in personal files should be stored only for a period of ten years after the end of service or the last pension payment.

The EDPS would therefore recommend that the period of storage of data in the personal file be reviewed to bring it into line with Article 4(1)(e) of the Regulation.

- *Storing data in disciplinary files*

The data in the disciplinary files are stored for 50 years, whether or not they have been deleted from the personal file. In most cases, this involves duplication of information, and the Court of First Instance has already banned the keeping of parallel files[2]. Moreover, the storage of all data in the disciplinary file for 50 years must be evaluated in the light of the principle of necessity as established in Article 4(1)(e) of the Regulation.

The EDPS therefore invites the European Ombudsman to review that data storage period. Once the time limit for appeal has passed, the intended purpose needs to be determined since the purpose of storing data in the disciplinary file in addition to the personal file might conflict with the principle of double jeopardy.

- *Storage of traffic data*

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.

If the European Ombudsman were to process data relating to Internet connections and the use of e-mail or the telephone in the course of an administrative investigation or disciplinary proceedings, he would have to do so in accordance with Article 37 of Regulation (EC) No 45/2001.

Article 20 of the Regulation provides for exemptions from the erasure of data relating to calls and other connections as provided for in Article 37(1) in particular when the storage 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". The EDPS interprets the restriction constituting "a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences" (Article 20(1)(a)) as applying to administrative investigations and disciplinary measures[3]. That provision therefore allows traffic data to be stored if necessary during a specific administrative investigation or specific disciplinary proceedings.

---

2 See Baltsavias v Commission, T-39/93 and T-553/93.

3 See EDPS opinion of 21 March 2005 on data-processing in the context of European Parliament disciplinary files (2004-0198).

3.7. Compatible use/Change of purpose

Data are retrieved from or inserted in the personal files. The processing operation under review involves no general change in the stated purpose of staff databases, administrative investigations and disciplinary proceedings being an aspect of the management of the official or other servant's career. Accordingly, Article 6(1) of Regulation No 45/2001 does not apply in this instance and the conditions of Article 4(1)(b) of the Regulation are fulfilled.

3.8. Transfer of data

The processing operation should also be scrutinised in the light of Article 7(1) of Regulation (EC) No 45/2001 relating to the transfer of personal data within or to other Community institutions or bodies. Such transfers can take place only if "*necessary for the legitimate performance of tasks covered by the competence of the recipient*".

In this instance, the data circulate between various people in the Ombudsman's Office, i.e. the Appointing Authority, the Secretary-General and the Heads of Department; the persons designated by the Appointing Authority to carry out an investigation; the Disciplinary Board and the persons being investigated. They may also be communicated outside the institution to the persons being investigated; to OLAF; to the Civil Service Tribunal; to the European Parliament security service[4]. Where data are transferred within or between Community institutions or bodies, Article 7 is applicable. That being so, the EDPS is satisfied that the transfers are necessary for the legitimate performance of tasks covered by the competence of the recipients.

Article 7(3) of Regulation (EC) No 45/2001 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 proceedings within the European Ombudsman's Office 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 recommends particular attention to the fact that personal data should be processed strictly within the framework of administrative investigations and disciplinary proceedings.

The EDPS would also draw attention to the fact that he himself may also be considered as the recipient of data on the basis of Regulation (EC) No 45/2001. For example, on the basis of Article 33 (complaints by Community staff) or of Article 47(2)(a), he has the right to obtain from a controller or Community institution or body access to all personal data and to all information necessary for his enquiries.

It may also happen that data are transmitted to the competent national authorities where there is an infringement of national law. In such instances, Article 8 of the Regulation is applicable and provides that personal data may be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC only if "*the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the*

[4] In that case, data are transmitted only where, in the light of the facts prompting the administrative investigation and/or disciplinary proceedings, there is reason to believe that the security services may be able to contribute to the investigation, provide security, undertake surveillance or contribute to prevention. The data transmitted are only those essential for the performance of the security service's task.

exercise of public authority". If data are transferred at the request of a national authority, it must therefore establish the "necessity" for the transfer. If, on the other hand, data are transferred on the sole initiative of the European Ombudsman, it will be for him to establish the "necessity" for the transfer in a reasoned decision.

However, it should be noted that the parties to whom the data are transmitted 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 3.10 on information to be given to the data subject) rather than as an exemption from Articles 7 and 8.

3.9. 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, and 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, the 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*".

Right of access and rectification is granted under Regulation (EC) No 45/2001 to all subjects of personal data, within the limits of the possible exemptions set out in Article 20. In the context of administrative investigations and disciplinary proceedings, those rights are granted not only to the person who is the subject of the investigation ("the suspect") but also to all other persons whose personal data are processed in the course of the investigation or disciplinary proceedings.

The EDPS therefore requests that right of access, as provided for by Regulation No 45/2001, be explicitly granted to the data subject, within the limits of the exemptions set out in Article 20. The EDPS is satisfied that in the case of an administrative investigation Article 2 of the GIP allows the data subject to request all documents directly linked to the allegations made, subject to the protection of the legitimate interests of third parties. He is also satisfied that the record of the prior hearing provided for in Articles 3 and 11 of Annex IX to the Staff Regulations is sent to the official or other servant heard (Article 3 of the GIP). The EDPS is pleased that in the case of proceedings before the Disciplinary Board the official concerned has the right to obtain the complete file concerning him/her and to copy all documents relevant to the proceedings, including exonerating evidence (Article 13 of Annex IX to the Staff Regulations).

However, the EDPS would stress that right of access must also be granted to all persons mentioned in the investigation report or disciplinary file, within the limits of the exemptions set out in Article 20. Restricting the right of access to protect third parties (see 3.4 above Quality of data) is in accordance with Article 20 of Regulation (EC) No 45/2001 which allows right of access to be restricted in order protect interests, notably if this restriction constitutes a necessary measure to safeguard the protection of the data subject or of the rights and freedoms of others. It must, however, be balanced against the person's right of access in relation to his right of defence.

As regards the 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 GIP) 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 for the interested party is therefore respected in the case in point. The other persons involved in the investigation should also, as far as possible, be granted the right to rectify their personal data.

3.10. 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 of the operation. This information should usually be given at the latest when the data are collected from the data subject if the data subject has not already been informed (Article 11). If the data are not collected directly from the data subject (Article 12), the information must be provided as soon as the data are recorded or, if the data are to be communicated to a third party, when the data are first communicated, 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. Data subjects (officials and other servants of the European Ombudsman) must be informed of the processing of personal data in the context of administrative investigations and disciplinary proceedings in general. Moreover, in the event of a specific administrative investigation and/or specific disciplinary proceedings against an individual, the principle of fair processing would seem to require that the individual be informed of the opening of proceedings relating to him and of the resulting processing of personal data.

According to the notification received, the GIP are published on the European Ombudsman's Intranet site. Although the EDPS considers that such publication does contribute to complying with the obligation to inform provided for in Regulation (EC) No 45/2001, it is not entirely satisfactory since not all of the items specified in Articles 11 and 12 are mentioned. There is no reference to information regarding the identity of the controller, the purposes of the processing operation or the existence of the right of access to, and the right to rectify, the data in general (see 3.9 above: Right of access and rectification), the time-limits for storing the data or the right to have recourse at any time to the European Data Protection Supervisor.

Information must also relate to the recipients of the data in general. With regard to the recipients of data, as pointed out above (3.8. Data transfers), authorities which may receive data in the framework of a particular investigation are not regarded as recipients. That therefore removes the obligation to provide information about such recipients in the context of a specific investigation but does not remove it in the context of general information on investigations and disciplinary proceedings.

The EDPS therefore recommends that information be provided on the processing of personal data.

The GIP stipulate that the official or other servant concerned be informed of the decision to open disciplinary proceedings and that the preliminary allegations made be specified. Moreover, the official or other servant must be heard before the end of the investigation.

Finally, the conclusions and, subject to certain reservations, the documents used to reach those conclusions, must be forwarded to the official or other servant concerned. The EDPS is satisfied that the person concerned is kept informed of the progress of the investigation or disciplinary proceedings but wants specific information relating to the processing of personal data also to be made available to the data subjects, subject to the restrictions in Article 20 of Regulation No 45/2001 as interpreted by the EDPS (see above).

3.11. Security measures

[...] The EDPS considers that these measures are adequate in the light of Article 22 of the Regulation.

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 means in particular that:

- a general instruction be adopted to ensure that only adequate and necessary data are processed in the course of administrative investigations and disciplinary proceedings.
- a procedure must be clearly established for the conduct of any tapping of electronic communications;
- anyone receiving and processing data in the context of administrative investigations or disciplinary proceedings within the European Ombudsman's Office process them solely within the framework of administrative investigations or disciplinary proceedings;
- the period of storage of data in the personal file and in the disciplinary file be reviewed in the light of Article 4(1)(e) of the Regulation.

- right of access and right of rectification also be granted to all persons mentioned in the investigation report or disciplinary file, within the limits of the exemptions set out in Article 20;

- provision must be be made for the supply of general information on the processing of personal data in the context of administrative investigations and disciplinary proceedings and for the supply of specific information on the processing of data in the context of a specific administrative investigation or specific proceedings within the limits of Article 20 of Regulation No 45/2001.

Done at Brussels, 17 October 2007

(Signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor