Opinion on a notification for prior checking received from the Data Protection Officer of the European Commission on security investigations

Brussels, 2 October 2008 (Case 2007-736)

1. Procedure

On 17 December 2007, the European Data Protection Supervisor (EDPS) received a prior checking notification from the Data Protection Officer (DPO) of the European Commission, on security investigations carried out by the Administrative Requisitioning section of DG ADMIN/Security (ADMIN/DS/RA).

On 1 February 2008, the EDPS asked the European Commission's DPO for additional information. The answers were received on 3 March 2008. The opinion was sent to the DPO for comments on 7 March 2008. Comments were received on 10 July 2008. The controller's response gave rise to other questions, which were sent to the European Commission's DPO on 11 July 2008; his reply was received on 15 July 2008. Further questions were sent to the European Commission's DPO on 25 July 2008. The answers were received on 1 October 2008.

2. The facts

ADMIN/DS/RA has three main functions, which are as follows:

measures in response to criminal acts concerning the buildings occupied by the Commission, the people who work in or for various reasons have access to those buildings, and any other acts which may be harmful to the institution. This includes collecting and keeping evidence and taking various investigative steps to gather such evidence, technical reporting, and collecting statements from victims, complainants, witnesses and where appropriate perpetrators of acts, without prejudice to the rules governing the actions of the Investigations and Discipline Office (IDOC) and the European Anti-Fraud Office (OLAF).

- providing technical assistance to other Commission departments which approach the Security Directorate in the context of occasional activities which come under their competence. This mainly means the ADMIN/IDOC Directorate, OLAF, the welfare and medical services, and DG BUDG. The section is also responsible for collecting, keeping and forwarding to the judicial authorities various items of evidence and information as requested by them, doing so strictly in compliance with internal procedures.

- exercising the institution's duty of care towards its officials and other staff, mainly in cases of some urgency.

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

These activities take various forms, including if necessary the drawing up of a detailed report on the incident which is forwarded to ADMIN/IDOC, OLAF and sometimes the police or judicial authorities, in accordance with internal procedures in this area.

2.1. Categories of data subjects

The categories of data subjects involved in this processing activity are the following: all officials, other agents and contract staff who are currently working; former officials, other agents and contract staff; service providers, contractors, visitors; people from outside the institution who contact the Commission and its staff, by mail, e-mail, phone or fax; people who are the victims, witnesses or perpetrators of an offence, a breach or event harmful to the institution or to its staff; and any member of staff in respect of whom the Commission must exercise its duty of care.

2.2. Data categories

The categories of data processed are: surnames, first names, possibly the date and place of birth, address, and phone contact details of the data subjects, the nature of the event, the place and time at which it took place, any items of evidence discovered and the link between those items and the persons involved.

The notification form, explicitly confirmed on this point by the DPO, specifies that special categories of data (those referred to in Article 10 of the Regulation) are not processed in the context of investigations conducted by the ADMIN/DS/RA section. However, very exceptionally, there may be ad hoc circumstances where, due to the subject-matter under investigation (e.g. access to health-related data in connection with the reimbursement of expenditure by the sickness and accident insurance office), such data may be processed.

In any event, data *"relating to offences, criminal convictions or security measures"* (referred to in Article 10(5) of the Regulation) are involved in this case.

The personnel number of an official under investigation is included in the final report in order to be absolutely certain that the person under investigation is identified clearly and with absolute certainty.

2.3. Data collection and storage

Any incident reported to ADMIN/DS/RA is recorded in a **computer database** with a whole range of information including the name of the official responsible for the dossier, the time and place where the incident took place, the nature of the incident, the details of the requesting department or individual, the names of all other persons involved, the nature of the damage suffered and some details of what happened. Each incident automatically receives a dossier number.

This has a twofold purpose: firstly, given the large number of dossiers handled, it makes it possible to respond rapidly and efficiently to any person or department who contacts the section about any past incident and wishes to add any further details, ask about follow-up or send the dossier to a higher level; it allows comparable data to be extracted (particularly as regards the time, place and nature of incidents) to help identify the perpetrator(s); it makes it possible to find details about the incident and have speedy access to relevant information to help solve a subsequent case rapidly. Annual statistics are drawn up on the basis of this information.

Any incident recorded in the computer database is also the subject of a **physical file** containing all the relevant documents such as the initial request, working and procedural documents, evidence (materials, photos or documents), statements and reports. All these are filed under the dossier number allocated by the computer database.

At the conclusion of an investigation, the investigator in charge must prepare a final report, presenting the findings and conclusions of the investigation.

Sometimes certain incidents result in access to one of the Commission buildings having to be prohibited for a particular individual, either urgently - as for example if someone presents an immediate risk to the security of the institutions' staff, property or information - or because a formal administrative decision to that effect has been made by the authorised body, or because the connection between a contractor and one of its employees has been broken and that person still possesses a service badge or a badge giving access to the buildings.

ADMIN/DS/RA draws up the **list of persons not allowed access to buildings occupied by the Commission.** This takes the form of a table indicating the surname, first name, date of birth, administrative status, and the building(s) which that person is not allowed to enter, as well as the corresponding dossier number in the computer database and physical files. The reason why the measure is being applied is not mentioned in this table.

In its investigations, ADMIN/DS/RA has **access to various databases**, both public and internal to the institution, from which it is able to collect information which is useful to it in handling its dossiers. The following databases are consulted;

- Argus

This database is maintained and updated by the ADMIN/DS4 unit, in its work to establish documents on and rights of access to buildings occupied by the institution. It contains the identity and photograph of persons holding access rights, the nature and duration of that right, the details of any vehicles, and the requesting department.

- Sysper

This database is used by DG ADMIN and contains various data about staff currently or previously employed by the Commission under the Staff Regulations.

- Sysper "pensioners"

This database is used by the PMO and contains various data about retired staff formerly employed by the Commission under the Staff Regulations.

- Recording of video images by surveillance cameras

This is a series of databases used by the ADMIN/DS4 unit which contains recent recordings of images filmed by the various surveillance cameras installed in and around some of the buildings occupied by the Commission[1].

- Leave and absences

Investigations conducted by ADMIN/DS/RA under its own authority sometimes require the consultation and/or use of data relating to leave requests or certificates of inability to work presented to DG ADMIN by a member of staff, when there is concern because that person has disappeared and there has to be an urgent preliminary check before any investigation is launched, in the interests of the person concerned. These checks relate only to the existence of such a document, not to its content.

[1] This data processing operation was the subject of a separate notification (EDPS Case 2007-271)

- Third-party files

This database of third-party files used by DG BUDG includes any entity which receives payments from the institution and its bank details. It is used when there is an urgent need to send the judicial authorities the bank details of someone whose disappearance is causing concern.

- Computer and phone investigations

Technological development has been such that many offences (threats, scams, slander and lies, leaks of sensitive information) are committed anonymously or under a false name by computer, phone, or fax. Investigations to discover the origin of such acts requires the consultation of records of telephone traffic on lines used or paid for by the institution (exclusively the identification of numbers and the time and duration of calls, and not their content), e-mail traffic passing through the Commission's IT network, connections to the internet from the Commission's internal network, and the use and content of the various databases used within the Commission. The same applies when ADMIN/DS is asked to carry out such investigations by authorised bodies such as ADMIN/IDOC or OLAF or on a formal request by the judicial authorities. A special procedure has been established specifically in the context of the authorisation of such investigations involving a request addressed to DG DIGIT or, if necessary, any other Directorate-General. A written request is first sent to the Commission's DPO, who has access to the data justifying the request for an investigation.

Following written authorisation by the DPO, the justified request is presented by the Director of ADMIN/DS to the ADMIN Director-General. The investigations only take place once the latter's written authorisation has been received, on the basis of the request asking that this procedure be followed. These investigations may result in a request being addressed to DG DIGIT and/or the Office for Infrastructure and Logistics in Brussels (OIB), as well as any other DG concerned[2].

In its investigative activities, ADMIN/DS/RA may make copies of hard disks for the purposes of data analysis. The procedure laid down in Administrative Notice No 45-2006 of 15 September 2006 applies. A specific "protocol" governing this activity has not been put in place.

- Database of access to buildings and areas equipped with computerised access control

Access to the various buildings occupied by the Commission is subject to controls, either by guards or electronically. Some access controlled by guards is recorded in ad hoc registers by office messengers or guards, on the responsibility of ADMIN/DS4. This mostly involves access by visitors, approved service providers (technicians, cleaners, guards etc), and authorised building trades (various companies). Such controls involve access to the building itself or to certain locked premises within that building, by withdrawing a key against proof of identity, and also access by officials outside normal office hours. Some specific areas within the buildings occupied by the Commission have computerised access control, with a database recording recent movements. This database is maintained by ADMIN/DS4.

- Database of the sickness and accident insurance office.

The PMO maintains a database of action by the sickness and accident insurance office for Commission staff. Investigations by the "Administrative Requisitioning" section under its own authority sometimes require it to request information contained in that database, for example the

[2] For investigations of ICT services (use of e-mail, internet, computer equipment, phone, fax or mobile phone), the conditions for acceptable use and the control and investigation methods are described in Administrative Notice No 45-2006 of 15 September 2006.

existence and use of false documents by a beneficiary seeking reimbursements to which they are not entitled. Except in the special case of a request from the judicial authorities with a view to the formal identification of a person who has lost their memory or died, the consultation of the database in question excludes any medical data.

- Technical action in buildings

The Offices for Infrastructure and Logistics in Brussels and Luxembourg (OIB and OIL) maintain databases containing information about the various technical activities carried out in the buildings occupied by the Commission.

2.4. Conservation of data

The data contained in the computer database and in the physical files may be kept by ADMIN/DS/RA for a maximum period of ten years after closure of the file. This time-limit corresponds to the period beyond which the law generally allows criminal cases to lapse. Staff dealing with dossiers may be called on to give evidence before the competent authorities.

The data on the list of those not allowed access to buildings occupied by the Commission are kept for the time strictly necessary to apply the measure prohibiting access, and in any case for not more than five years after the measure has been applied.

In order to allow for the comparison of precedents and the compilation of statistics, final reports of internal investigations may be rendered anonymous and kept for 50 years.

2.5. Transfers of data

The report and supporting documents are forwarded for follow-up to the competent body, i.e. OLAF, IDOC, the competent judicial authorities of the Member States and/or third States or international organisations, or to the medical or welfare services, the OIB (insurance section), or finally to any department responsible for taking the necessary action on the report's conclusions. In the latter case, it is possible only to forward part of the report.

The data included in the report and forwarded depend on the case. There is no "standard report". Usually the report contains a summary of the facts and observations (sometimes including photos), a description of the action taken, sometimes a legal evaluation of the facts, and recommendations.

2.6. Information provided to the data subjects

2.6.1. Method

- Person who is the subject of an investigation

ADMIN/DS/RA provides information to the person who is the subject of an investigation when their statement is taken.

Every statement is preceded by the following text: *" I am aware that I am in no way obliged to make this administrative statement and that if I agree to do so I may request a copy. You have informed me that the information I give will be subject to data processing. You have informed me that I will subsequently be able to make an additional statement if I want to change or add to this information to which I retain a general right of access.*
The personal data concerning me which will be collected in connection with this case are protected by Regulation 45/2001, available from www.cc.cec/security/index_en.html, where I can

also consult the privacy statement on the protection of data contained in the database used by the "Administrative Requisitioning" section of the ADMIN/Security Directorate.
The rights of access, information and rectification (see Articles 13 to 17 and Article 37 of that Regulation) are in this case restricted on the one hand by the necessities of the prevention, investigation, detection and prosecution of criminal offences, and also by the protection of the rights and freedoms of others (Article 20). I am aware of my right to contact the European Data Protection Supervisor, who will carry out a verification in the cases covered by Article 20. I declare that I have received a copy of the privacy statement relating to the protection of data contained in the database used by the "Administrative Requisitioning" section of the ADMIN/Security Directorate. The personal data may be processed for the purposes for which they were transmitted."

Where, because of the circumstances of the case, it is not possible to contact the data subject when the case is being processed (physical impossibility, for example as regards individuals who have disappeared or run away), this opportunity is offered as soon as contact is subsequently made with them and it becomes possible.

If the department does not collect the written statement and has no contact with the person before forwarding the data to another department (OLAF, IDOC, national authorities), the data subject is not provided with information by ADMIN/DS/RA. The only information available is that contained on the internet site of the Security Directorate.

Those who are prohibited from having access to Commission buildings receive prior notification of that decision. In the case of staff employed by the Commission under the Staff Regulations, DG ADMIN is responsible for notifying the person concerned of the Appointing Authority's decision, and the information is only added to the database after that notification has been given, unless this is physically impossible (for example because the person has run away and is evading justice). Visitors, service providers or outsiders (for example members of the families of staff employed under the Staff Regulations) are only included on the database on due grounds if there is an imminent danger or if the person holds an access card which they have not returned or have refused to return, and only after the person has if possible been given notice of the measure, either directly by ADMIN/DS/RA or via the employer in the case of a service provider.

- Informants, whistleblowers and witnesses

Anyone who contacts ADMIN/DS/RA to report an incident or request technical or personal assistance, and anyone contacted in connection with investigations, is advised - either orally or in writing, depending on the nature of their contact with members of the section - that the information they provide will be entered in a database, and that if they so wish they are at liberty to contact their interlocutor again to make subsequent additions or changes to that information.

Any statement is preceded by a text identical to that relating to a "Person who is the subject of an investigation" (see above).

Where, because of the circumstances of the case, it is not possible to contact the data subject when the case is being processed, this opportunity is offered as soon as contact is subsequently made with them and it becomes possible.

2.6.2. Content of the information

If the information is sent by e-mail the following response (in French and English) automatically generated: *"Your message has well been recorded and will be processed as soon as possible. It is brought to your attention that the given information will be subject to data processing. You have the opportunity to modify or supplement this information at a later date by the same way. The personal data are protected by Regulation 45/2001 (see "www.cc.cec/security/index_en.html").*

The application can be restricted where such restriction constitutes a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences, or to insure the protection of the data subject or of the rights and freedoms of others (art. 20 of the Regulation)." Dominique Baudoux, Raf Philips, ADMIN/Security Directorate - Administrative Requisitioning".

According to the controller, the automatic response will shortly read as :
Your message has been recorded and will be processed as soon as possible. It is brought to your attention that the information you have given will be subject to data processing. Through the same channels, you may modify or supplement this information to which you retain a general right of access. The personal data are protected by Regulation 45/2001, available from www.cc.cec/security/index_en.html, where the privacy statement on the protection of data contained in the database used by the "Administrative Requisitioning" section of the ADMIN/Security Directorate may also be consulted.
The rights of access, information and rectification (see Articles 13 to 17 and Article 37 of that Regulation) are in this case restricted on the one hand by the necessities of the prevention, investigation, detection and prosecution of criminal offences, and also by the protection of the rights and freedoms of others (Article 20). I am aware of my right to contact the European Data Protection Supervisor, who will carry out a verification in the cases covered by Article 20. I declare that I have received a copy of the privacy statement relating to the protection of data contained in the database used by the "Administrative Requisitioning" section of the ADMIN/Security Directorate. The personal data may only be processed for the purposes for which they were transmitted.

If the information is provided when the written statement is made, the data subject receives the "Privacy statement - Data protection - Databases used by the Administrative Requisitioning section of the ADMIN/Security Directorate". This document contains information on the identity of the data controller, the purposes of the processing operation, the data recipients, the existence of a right of access and rectification, storage periods and security measures, and the right to address the EDPS in the context of a request for access to the data.

2.7. Right of access and rectification

In principle, ADMIN/DS/RA does not communicate the reports and other documents connected with the investigation, either to persons who are the subject of an investigation or to informants or witnesses. The reason for this is to avoid committing any blunder which might jeopardise the procedures launched by the competent bodies (IDOC/OLAF/national judicial authorities). According to the notification, communication of the content of the reports drawn up by ADMIN/DS/RA is their responsibility in the context of the procedures governing their activity.

However, data subjects are able to correct the information they have provided or which is provided to them, either immediately or subsequently, by making and sending in an additional statement which will be an integral part of their file. This possibility is always mentioned during contacts with data subjects and is set out on the ADMIN/Security Directorate site. According to the data controller, this procedure ensures that data can be rectified and updated depending on subsequent developments.

According to the data controller, data which are not communicated directly by the data subject come within the exceptions mentioned in Article 20 of Regulation (EC) No 45/2001. Anyone may therefore contact the European Data Protection Supervisor for him to check the lawfulness of the processing operation. A data subject may always contact the Commission's Data Protection Officer, who may check the data concerning that person and have them modified or erased if a legitimate reason is given.

2.8. Security

Security measures have been adopted in order to protect both paper and electronic files.

[...]

3. Legal aspects

3.1. Prior checking

This prior check relates to the processing of personal data in the context of internal security investigations carried out by ADMIN/DS/RA. This is processing by a European institution, in the framework of Community law. The personal data processing operation is carried out partly by automatic means, and the manual processing concerns data which forms or is intended to form part of a filing system. As a consequence, the Regulation is applicable.

Article 27(1) of the Regulation subjects to prior checking by the EDPS 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 that are likely to present such risks.

Article 27(2)(b) of the Regulation stipulates that operations intended to *"evaluate personal aspects relating to the data subject, including his or her (...) conduct"* shall be subject to prior checking by the EDPS. In this case, the conduct of the persons involved is analysed by ADMIN/DS/RA.

Furthermore, under Article 27(2)(a) of the Regulation, processing operations relating to *"suspected offences, offences, criminal convictions or security measures"* shall be subject to prior checking by the EDPS. In this case, the processing operation could include this type of data.

Since the data controller draws up a list of persons prohibited from having access to buildings occupied by the Commission, Article 27(2)(d) on *"processing operations for the purpose of excluding individuals from a right, benefit or contract"* also applies.

Insofar as the data controller may analyse the hard disks of computers containing private data, the EDPS, in conformity with the settled interpretation of the Regulation, considers that Article 27(1) of the Regulation is applicable.

Since prior checking is designed to address situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. However, in this case the processing operation has already begun. On the other hand, this is not a serious problem, in that any recommendations made by the EDPS may still be adopted accordingly.

The DPO's notification was received on 17 December 2007. According to Article 27(4) the present opinion must be delivered within two months following receipt of the notification. The procedure was suspended for 197 days and during the month of August 2008. The opinion will therefore be delivered no later than 3 October 2008.

3.2. Lawfulness of the processing

The lawfulness of the processing operation must be examined in the light of Article 5(a) of the Regulation which stipulates that personal data may be processed only if: *"processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties*

establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed".

The processing of data in the context of internal administrative investigations is based on the Commission Decision of 19 September 1994 on the tasks of the security office and on Commission Decision No 844/2001 of 29 November 2001 on security measures.

Those instruments indicate that administrative investigations conducted by ADMIN/DS/RA are missions in the public interest (combating crime, protecting persons and property, etc). Furthermore, ADMIN/DS/RA carries out those activities in the legitimate exercise of official authority and thus complies with its legal obligation to investigate matters within its competence.

The EDPS would draw attention to the fact that the wording *"combating crime"*, which implies the use of force by the State, is not really appropriate in the light of the legal basis for the processing operation. The data controller has informed the EDPS that this wording will be replaced, in the texts in which it appears, by the following phrase: *"investigations relating to any criminal and/or administrative offence, if it occurred in Commission premises, if members of Commission staff were harmed or involved, or if the Commission itself was involved or harmed"*.

The "necessity" of the processing has to be analysed in concrete terms. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the investigations has to be proportional to the general purpose of the processing operation (investigating criminal offences, protecting people and property, etc) and to the particular purpose of the processing operation in the context of the case (considering, for instance, the seriousness of the incident under investigation, the sort of data needed to clarify the facts, etc.). Thus, the proportionality of the processing operation has to be evaluated on a case-by-case basis.

3.3. Processing of special categories of data

Article 10(5) provides that: *"Processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor."* In this case, the data processing operation is authorised by the legal instruments mentioned in paragraph 3.2 above.

Apart from that, according to Article 10(1) of the Regulation, the processing of special categories of data (that is *"data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life"*) is prohibited. The Regulation provides for certain exceptions in Article 10(2). However, it seems very likely that, if any exception were to apply, only those in sub-paragraphs (b) or (d) would possibly be relevant.

Indeed, the type of data described in Article 10(1) would only be processed in exceptional circumstances. However, consultations of the files of the EU's sickness insurance scheme could for example reveal data relating to health. If this happens, the general rule laid down in Article 10(1) has to be complied with; otherwise, there must be a restrictive examination of whether an exception is necessary. In any case, ADMIN/DS/RA staff in charge of the files must be aware of this rule that exceptions must remain exceptional, and must avoid the inclusion of special categories of data unless one of the circumstances provided for in Article 10(2) is present in the particular case or unless Article 10(4) has to be applied.

3.4. Data quality

According to Article 4(1)(c), personal data must be *"adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."*

Even though certain standard types of data such as the name and date of birth will always be present in the investigation files, the precise content of a file will of course vary depending on the case. However, guarantees must be established to ensure that the principle of data quality is respected. This could take the form of a general recommendation to the persons handling these files, reminding them of the principle and asking them to ensure that it is respected.

The data controller has sent a written instruction, to be signed in acknowledgement, to staff in the "Administrative Requisitioning" section, reminding them of the principle of data quality and requesting them to respect it.

The EDPS also recommends that whenever access to personal data appears to be necessary for the purposes of the investigation, such access should respect appropriate guarantees, taking into account any potential risk of inadmissibility of the evidence in a possible future criminal case, which could arise if the fundamental rights to privacy and personal data protection were not respected when the evidence was collected. Particular attention must be paid to respecting these principles when access to files which are manifestly of a private nature seems necessary for the purposes of the investigation.

These principles also apply to processing operations involving the forensic examination of computers. Specific precautions should be taken regarding access to the contents of a computer belonging to a Community institution, since it may also contain files used by the data subject for private purposes (for instance in the folder "My documents", or e-mails marked as "private"), or files which are not relevant or which are excessive for the purposes of the investigation. Such forensic examinations of computers must be subject to particular authorisation mechanisms. In this respect, the EDPS recommends the adoption of formal "Standard Operating Procedures" for the conduct of forensic examinations of computers, which will also help to ensure that the principle of data quality is respected[3].

According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date"*, and *"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"*. The procedure in place gives sufficient cause to believe that the data are accurate and kept up to date. This principle is very closely connected to the exercise of the rights of access, rectification, blocking and erasure (see paragraph 3.8 below).

Data must also be *"processed fairly and lawfully"* (Article 4(1)(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, considerable attention must be paid to this in the context of such a sensitive subject. It concerns the information provided to the official who is the subject of an investigation (and other data subjects), and the speed with which this information is provided, so that the right of defence can be respected.

3.5. Conservation of data

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. The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in*

[3] See the EDPS opinion of 23 June 2006 on a notification for prior checking received from the Data Protection Officer of the European Anti-Fraud Office (OLAF) on OLAF internal investigations (Case 2005-418).

anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes" (Article 4(1)(e) of the Regulation).

The data contained in the computer database and in the physical files is kept for ten years after closure of the file. This time-limit corresponds to the period beyond which the law generally allows criminal cases to lapse. Staff dealing with dossiers may be called on to give evidence before the competent authorities.

The data on the list of those not allowed access to buildings occupied by the Commission is kept for five years after the ban is applied. In order to allow for the comparison of precedents and the compilation of statistics, final reports of internal investigations may be rendered anonymous and kept for 50 years.

The EDPS finds that this data storage policy complies with the Regulation.

3.6. Data transfer

3.6.1. Transfer of personal data between or within Community institutions or bodies

Article 7(1) of the Regulation stipulates that: *"Personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".*

This means that the reports and/or related documents (personal data) are only transferred if this is "necessary" for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor has to be considered in this regard, taking into account, for instance, the nature of the data collected and further processed, and the competence of the recipient.

In any case, in accordance with Article 7(3) of the Regulation, the recipient must be informed that personal data can only be processed for the purposes for which they were transmitted. Following this recommendation, the data controller has decided to add the following footnote on page 1 of any report forwarded: *"Personal data may only be processed for the purposes for which they were transmitted."*

3.6.2. Transfer of personal data to Member States

Two scenarios can be observed in the Member States:

(a) those Member States where the national data protection law adopted pursuant to Directive 95/46/EC covers every sector of the national legal system, including the judicial sector;

(b) those Member States where the national data protection law adopted pursuant to Directive 95/46/EC does not cover every sector, and in particular not the judicial sector.

As to the first scenario, Article 8 of the Regulation provides that: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, (a) 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 exercise of public authority, or (…)".*

Thus, even if judicial authorities do not fall within the scope of application of Directive 95/46/EC, if the Member State, when transposing Directive 95/46/EC into internal law, has extended its application to these public authorities, Article 8 of the Regulation has to be taken into account.

For those countries that have not extended their implementation of Directive 95/46/EC to their judicial authorities, Article 9 of the Regulation has to be taken into consideration. In those countries, Council of Europe Convention 108, which in this case can be considered as providing an adequate level of protection, is in any case applicable to judicial authorities.

3.6.3. Transfer to third country authorities and/or international organisations

Article 9(1) of the Regulation provides that *"personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out"*. Thus transfers to States which do not offer an adequate level of protection are, in principle, not possible.

However, Article 9(6) stipulates that derogations are possible, in particular if *"the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims"* (Article 9(6)(d)) Since this provision is an exception it must be strictly interpreted. This derogation cannot be used systematically. Its use may only occasionally be accepted, where the transfer is particularly necessary in relation to the purpose of the processing operation. In any event, the use of Article 9(6) may not bring about a situation in which the fundamental rights of the data subject are violated.

Another form of derogation is provided for in Article 9(7) which states that the EDPS may authorise the transfer *"where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights"; such safeguards may in particular result from appropriate contractual clauses*". When the data is transferred, the data controller must provide the recipient with information on the principles of data protection and must ensure that the privacy and fundamental rights and freedoms of the data subject are guaranteed by the recipient.

By virtue of Article 9(8), the ADMIN/DS/RA section must inform the EDPS of categories of cases where they have applied Articles 9(6) and 9(7). The EDPS recommends that a register of occasional transfers carried out by virtue of the derogations in Articles 9(6) and 9(7) should be set up for this purpose. The register could contain the following information: the purposes of the transfer, the data subjects, the categories of data, whether data subjects have been informed (if appropriate), rights of access (direct or indirect), the legal basis and legality of the transfer, the data recipients, an indication of how long the data will be kept by the recipient, etc. This register should always be available to the EDPS.

The data controller informed the EDPS while the opinion was being drafted that a footnote would be added to the first page of every document transmitted: *"Personal data may only be processed for the purposes for which they were transmitted."* In addition, there will be a mention of the principles of data protection and of the need to respect the privacy and fundamental rights and freedoms of the data subjects, which is a principle which the recipient of the report must respect.

The data controller has also undertaken to keep a computer register of these transfers, including the dossier number, the date of transmission, the recipient, the purpose of the transfer, the data subjects, the categories of data, whether information has been provided to the data subjects, rights of access (direct or indirect), the legal basis and legality of the transfer, and an indication of how long the data will be kept by the recipient.

3.7. Processing including a personnel number or other identifier of general application

ADMIN/DS/RA uses the personnel number of an official under investigation, and it is included in the final report. In this case, the use of the personnel number is reasonable, since its only purpose

is to identify the person concerned by the dossier. The EDPS considers that here this number can be processed.

3.8. Right of access and rectification

According to Article 13 of the Regulation, the data subject has the right to obtain from the controller, without constraint, communication in an intelligible form of the data undergoing the processing and any available information as to their source.

The right of access is the right of the data subject to be informed about any information relating to him or her that is processed by the data controller. As a matter of principle, this right has to be interpreted in conjunction with the concept of personal data. Indeed, the Regulation has adopted a broad concept of personal data, and the Article 29 Working Party has also followed a broad interpretation of this concept[4]. The respect of the rights of access and rectification is directly connected with the data quality principle and, in the context of investigations, it overlaps to a great extent with the right of defence.

Furthermore, the right of access is also applicable when a data subject requests access to the files of others, where those files contain information relating to him or her. This would be the case of informants or witnesses seeking access to the data relating to them in the context of an investigation of another person.

The information can be obtained directly by the data subject ("direct access") or, under certain circumstances, by a public authority ("indirect access", normally exercised by a data protection authority, in the present context by the EDPS).

As noted in paragraph 2.6, the general rule applied by ADMIN/DS/RA is to refuse access to the personal data relating to the data subject contained in the investigation file. According to the data controller, such a right of access would be harmful to the investigation by the competent bodies (IDOC/OLAF/national authorities, etc).

The EDPS finds that the principle of refusing access to the data is manifestly contrary to Article 13 of the Regulation. The data controller cannot apply the exception as a general rule. It must be remembered that restrictions to a fundamental right cannot be applied systematically. Such restrictions must be "necessary". The "necessity test" has to be conducted on a case-by-case basis and (just as with the right to information) the rights of access and rectification have to be provided *"as long as this would not be harmful to the investigation"* (see paragraph 3.9 below). The nature of certain cases, will not always justify the denial of access and rectification during an internal investigation by the ADMIN/DS/RA section. Therefore, the EDPS recommends the inclusion of a general rule of access to data, given its importance for the purposes of data protection.

However, Article 20 of the Regulation provides for certain restrictions to this right notably where 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"*. Moreover, in certain cases it may be necessary not to give direct access to the data subject so as not to harm the proper functioning of the inquiry even though it is not a criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001, but a "pre-disciplinary" or "pre-criminal" investigation. The interests of the authority which is going to follow up the investigation (OLAF, IDOC, national authorities) may also be taken into account in this respect.

---

[4] See Opinion 4/2007of 20 June 2007 on the concept of personal data, adopted by the Article 29 Data Protection Working Party http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf).

In any event, Article 20(3) has to be taken into account and respected by ADMIN/DS/RA: *"If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Supervisor."* Concerning the right to information, this provision must be read jointly with Articles 11, 12 and 20 of the Regulation (see paragraph 3.9 below).

Moreover, account should also be taken of Article 20(4): *"If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made."* The indirect right of access will then have to be guaranteed. Indeed, this provision will play a role, for instance, in those cases where the data subject has been informed about the existence of the processing operation, but where the right of access is still being restricted in the light of Article 20.

Article 20(5) provides that *"provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."* It may be necessary for ADMIN/DS/RA to defer the provision of such information in accordance with this provision, in order to safeguard the investigation. This necessity of such a deferral must be decided on a case-by-case basis.

As already mentioned, the right of access involves the right of the data subject to be informed about the data referring to him or her. However, as noted above, this right can be restricted to safeguard *"the protection of the (...) rights and freedoms of others"*. This has to be taken into account here as regards access by the data subject to the identity of whistleblowers. The Article 29 Working Party has made the following statement: *"under no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblowers from the scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed."* The same approach should be applied concerning informants[5].

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the sensitivity of most of the investigations conducted by ADMIN/DS/RA, this right is of crucial importance in order to guarantee the quality of the data used, which in this case is connected to the right of defence. Any restriction under Article 20 of the Regulation must be applied in the light of the above paragraphs regarding the right of access.

Finally, rules must be established so that once an investigation is closed, the official under investigation can rectify any data relating to him or her by requesting the inclusion in the investigation file of documentation related to any subsequent developments during the follow-up phase of the case (a contrary decision by the Court, for instance).

3.9. Information to be given to the data subject

The Regulation states that the data subject must be informed if personal data relating to him/her are being collected, and lists a number of points which must be included in that information in order to ensure the fair processing of that data. In this case, the data could be collected either directly from the data subject or indirectly, for example through informants.

Article 11 of the Regulation *(Information to be supplied where the data have been obtained from the data subject)* and Article 12 *(Information to be supplied where the data have not been*

[5] On the other hand, it is not necessary to guarantee the confidentiality of the identity of witnesses.

obtained from the data subject) are thus both applicable in this case. This means that the relevant information must be given, either at the time of collection (Article 11), or when the data are first recorded or disclosed (Article 12), unless the data subject has already been provided with it.

The type of information provided to data subjects is described in detail in paragraph 2.6. However, while the content of the information given sometimes partially corresponds to that which must be communicated by virtue of Articles 11 and 12, it is evident that not all the information listed in those provisions is actually provided. Account must be taken of the fact that all the requirements of paragraph 1 of Articles 11 and 12 must be complied with, including those under (f) since, given the sensitivity of the subject-matter, the data subjects must be made aware of all the guarantees to which they are entitled. As regards the contents of the specific privacy statement, the EDPS recommends that information should be added on the legal basis of the processing operation and on the right to have recourse at any time to the European Data Protection Supervisor and not just in the context of access to the data. During the procedure the data controller has informed the EDPS that these additions will be made to the privacy statement.

As regards timing, paragraph 2.6.1 above notes that ADMIN/DS/RA provides this information to data subjects when it first has contact with them. If a case were to arise where the department did not collect a written statement and had no contact with the data subject before transmitting the data to another department (OLAF, IDOC, national authorities) then, by virtue of Article 12 of the Regulation, ADMIN/DS/RA would have to provide the information to the data subject when the data concerning him or her were recorded, or at the latest when that data was first communicated to third parties. Simply making this information available on the internet site of DG ADMIN is not sufficient in this respect. It cannot be reasonably expected that data subjects will consult that site spontaneously. Of course, this recommendation does not concern situations where it is impossible to contact the data subject because of the facts of the case (where a person has disappeared or run away).

Article 20 of the Regulation, as quoted above, does provide certain restrictions to the right to information (see paragraph 3.8 above).

Furthermore, Article 20(5) of the Regulation will have to be applied in specific circumstances: *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."* (Paragraph 3 provides that the data subject has the right to be informed of the reasons why a restriction has been imposed as well as his right to have recourse to the EDPS; paragraph 4 provides a right of indirect right of access via the EDPS and stipulates that information on its outcome must be provided to the data subject).

3.10. Security measures

After careful analysis of the security measures described in paragraph 2.8, the EDPS considers that those measures are adequate in the light of Article 22 of the Regulation.

Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this opinion are fully taken into account. In particular, the data controller must:

- evaluate the proportionality of the processing activities on a case-by-case basis;

- ensure that when access to files that are manifestly of a private nature appears to be necessary for the purposes of the investigation, such access respects the appropriate guarantees;
- adopt formal "Standard Operating Procedures" for the conduct of forensic examinations of computers, which will also help to ensure that the principle of data quality is respected.
- in compliance with Article 7(1) of the Regulation, provide a notice to recipients informing them that personal data can only be processed for the purposes for which they were transmitted;
- forward reports and/or related documents (personal data) only if they are necessary for the legitimate performance of tasks covered by the competence of the recipient. The proportionality factor should be taken into account here;
- establish the necessity of transfer to the judicial authorities in a reasoned decision, in the light of Article 8 of the Regulation;
- set up a register of occasional transfers carried out by virtue of the derogations in Articles 9(6) and 9(7) and inform the EDPS that this has been done;
- adopt a general rule of exercise of the right of access by the data subject, on the basis of Article 13 of the Regulation; such access could be restricted if it is likely to be harmful to the investigation, which must be decided on a case-by-case basis;
- establish rules so that, when the investigation is finished and taking account of Article 20, the data subject is able to rectify his/her personal data to ensure that they are updated in the light of subsequent developments;
- provide the requisite information to the data subject when data concerning him or her is recorded or, at the latest, when that data is first communicated to third parties;
- when any restriction based on Article 20 is applied, mention it in the file;
- provide information to the data subject in compliance with Articles 20(3) and 20(4) of the Regulation;
- respect the content of the information to be given to the data subject, in accordance with paragraph 1 of Articles 11 and 12 of the Regulation (including sub-paragraph f).

Done at Brussels, 2 October 2008.

(Signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor