Opinion on the notification for prior checking from the Data Protection Officer of the European Commission on recording the line reserved for emergency and security calls in Brussels (88888)

Brussels, 22 May 2006 (Case 2006-2)

1. Procedure

1.1. On 3 January 2006, the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001, hereinafter referred to as the "Regulation", from the Data Protection Officer of the European Commission (DPO). The notification concerns the recording of calls made on the line reserved for emergency and security in Brussels (88888).

1.2. The notification is accompanied by a document titled "Draft communication on the establishment of offices – DG Admin" and by Commission Decision (94) 2129 concerning the tasks of the Security Office.

1.3. A request for further information was submitted on 18 January 2006. A response was given to the request on 6 April 2006.

2. Examination of the case

2.1. The facts

In an emergency, Commission staff can call the emergency number displayed in all Brussels Commission buildings, namely 88888.

It is also possible that persons not on the Commission staff might use the emergency number provided, if they find themselves in such a situation inside the Commission.

In the context of the security duty office, the Personnel and Administration Directorate-General's Security Directorate (DS) records calls received on the 88888 line (emergency calls) in Brussels. The system records the content of the phone conversation, the time of the call, its length and the number the call came through to. Callers do not have to identify themselves during the conversation. The system used does not automatically provide information on the person who called the lines concerned, nor the place from which the call is made, unless this information is given during the conversation.

Recording is carried out for the purposes of subsequent checking on the content of the messages that reach the lines concerned, subsequent checking of operational events and, in the context of files on possible threats to the institution, provision of evidence.

Calls are automatically recorded in electronic form. These recordings are kept for three months, unless they are needed in the context of an official enquiry procedure.

The data are intended for internal use by the authorised permanent staff of the Security Directorate. In the context of alert checking and for certain SD investigation reports, recordings are listened to and/or used by the three people authorised to do so, all three being officials and heads of department with clearance to "secret" level and knowledge of the necessary codes and passwords. This procedure is subject to formal prior instructions from the head of the ADMIN.DS.1 unit. The system records all applications to listen to calls, including the date time and channels listened to. The system keeps recordings that have been listened to.

The recordings may be forwarded to national courts in accordance with legal procedures in force. In this case a record of the fact is kept in the service archives.

Surveillance staff are informed about recordings of calls and the use made of them during their training on starting their jobs. The fact that the lines are recorded is also stated in the instructions in the duty office.

According to the information received by the DPO, under cover of the exemption under Article 20(1)(a) of Regulation No 45/2001, no advance information is provided about the recording system, and as the recording of the call is not mentioned to the caller. However, in order to inform data subjects within the Commission, a confidentiality declaration has been prepared for inclusion on the Security Directorate website. The declaration includes the identity of the person responsible for the processing, the purpose of the data collection, the persons to whom the data may be communicated, the right of access to the data of the data subjects, the length of time for which the data are kept and the contact points for queries or complaints.

As for persons from outside, a statement that the lines are recorded is to be added to the electronic directory available from outside the Commission.

The recordings are not indexed by name of data subject. However, anyone wishing to may request access to the recording, subject to a check on the justification for the request, on the basis of the date and time of the call.

Security measures have been taken […]

2.2. Legal aspects

2.2.1. Prior checking

Regulation No 45/2001 applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. It applies to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

The situation under consideration is one of processing by the Commission carried out in the context of Community activities. It is also one of processing of personal data, since the communications recorded are between two persons at least one of whom is identified or at least "identifiable". To clarify, an "identifiable person", within the meaning of Article 2(a) of the Regulation, "is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity." Since the recording cites the number which the call reached, it is possible in most cases to identify the person on duty on that day. In some cases the caller identifies himself too.

Regulation 45/2001 is therefore applicable.

The recording constitutes automated processing within the terms of the Regulation.

Article 27(1) of Regulation (EC) No 45/2001 requires prior checking by the EDPS of all "processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". Article 27(2) of the Regulation contains a list of processing operations likely to present such risks.

The processing of data in the context of internal communications networks has specific aspects as regards data protection, which led to a chapter being drafted specifically on those aspects (Chapter IV). In particular, Article 36 lays down the basic principle of data confidentiality which we consider below. This special treatment of such data constitutes a specific risk within the meaning of Article 27(1).

Furthermore, Article 27(2)(a) specifies that processing of data relating to suspected offences, offences, criminal convictions or security measures is likely to present such risks. Since these recordings are likely to provide evidence in relation to suspected offences or offences, in the context of dossiers concerning threats to the institution, they are likely to fall within the scope of Article 27(2). Finally, data relating to health are likely to be included in the call, which also qualifies the operation for prior checking under Article 27(2)(a).

For these reasons, the operation must be subjected to prior checking.

In principle, checks by the European Data Protection Supervisor should be performed before the processing operation is implemented. In this case, as the European Data Protection Supervisor was appointed after the system was set up, the check necessarily has to be performed ex-post. This does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented.

Notification from the DPO was received on 3 January 2006. Under Article 27(4), this opinion must be delivered within the following two months. The deadline for delivery of the opinion was suspended for 77 days by a request for further information. The EDPS will therefore deliver his opinion by 20 May 2006. Since that day is a Saturday, the opinion will be delivered on the first working day thereafter, namely 22 May 2006.

2.2.2. Legal basis and lawfulness of the processing operation

The Security Directorate protects persons, information and property of the Commission (Charter of the Security Office established in document C(94)2129 of 8 September 1994). In this context, it runs the duty office of the Commission that receives emergency calls. In the context of setting up the Operational Crisis Management Team, to which the duty office belongs, the Security

Committee, chaired by the Secretary-General, authorised a system whereby in a crisis situation all calls to the Security Office and the Operational Team would be recorded (CS/87/026 and 029). This document constitutes the legal basis.

Alongside the legal basis, the lawfulness of the processing operation as defined in Article 5 of Regulation (EC) No 45/2001 must also be considered. Article 5(a) stipulates that processing of personal data can be carried out only if "necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof". The legal basis resulting from the above provisions supports the lawfulness of the processing insofar as the recording is necessary for the accomplishment of tasks assigned to the Security Directorate.

2.2.3. 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, are prohibited except where grounds are identified in Article 10(2).

Information concerning a person's health may appear in the recording of emergency calls in that some calls are precisely concerned with medical emergencies. In most cases, the data subject will have consented to the processing of his data, thereby justifying processing on the basis of Article 10(2)(a). Finally, processing can also be justified under Article 10(2)(c) where it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

2.2.4. Data Quality

According to Article 4(1)(c) of the Regulation, personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". In addition, they must be "accurate and, where necessary, kept up to date" (Article 4(1)(d)).

The data which are the subject of the present prior check concern the entire conversations held on the 88888 number, the call time and length and the number on which the call was received.

It is not desirable to select data from within the call, since in principle all the data are pertinent from the point of view of the aims involved. The other call data are also needed for processing purposes.

Live recording of the calls ensures that the data are accurate.

The EDPS therefore considers that the principle of data quality is complied with.

2.2.5. Conservation of data

The Regulation lays down that the data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. (Article 4(1)(e)).

Retention of recordings for 3 months is in compliance with Article 4(1)(e) of the Regulation.

In addition, under Article 37(1), the traffic data, that is the data necessary to establish calls, are deleted or made anonymous at the end of the call. Exceptions to this principle are stipulated by

Article 20, inter alia where an exemption is necessary for "the prevention, investigation, detection and prosecution of criminal offences", "the protection of the data subject" or "the national security, public security or defence of the Member States".

The data on telephone calls are stored for 3 months. This data retention, and the traffic data in particular, may take the exemptions set out in Article 20 as a basis.

In the event of processing of data that are necessary for a security/administrative inquiry, they would be held until the inquiry and any appeals have been concluded. This retention period is also justified in terms of the exemptions provided for in Article 20.

2.2.6. Transfer of data

Transfer of data to national judicial authorities in accordance with the legal procedures in force, for national purposes, cannot be ruled out. Article 8 of the Regulation applies to any transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC. It is true that Directive 95/46/EC does not cover judicial activity, and Article 8 of the Regulation is not automatically applicable. That said, some Member States have broadened the scope of their national laws, transposing the Directive in such a way as to include national authorities exercising their judicial roles. In such cases, Article 8 is applicable, and transfer can take place only if the recipient shows that the data are necessary for the performance of a task carried out in the public interest or subject to public authority. In other cases, either Article 9(1) is applicable, for countries that offer an adequate level of protection, or Article 9(6)(d) is applicable, whereby the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

2.2.7. Confidentiality of data

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

This duty of confidentiality applies to the content proper of communications. In principle it prohibits any interception or recording of communications. Any restriction to this principle must comply with the general principles of Community law. The latter concept refers to the notion of fundamental rights, as set out in the European Convention on Human Rights.

In practice, this implies that any restriction on data confidentiality must comply with fundamental rights as set out in the Convention. Such a restriction may be applied only if it is in accordance with the law and is necessary in a democratic society, inter alia for purposes of national security, public safety, the prevention of disorder or crime, or for the protection of the rights and freedoms of others.

Any restriction to the principle of confidentiality must therefore be examined in the light of strict criteria, and in particular proportionality in regard to precise aims.

In the present case, since the recording of the calls is carried out for purposes of public safety or the prevention of disorder or crime, the EDPS considers that there is no breach of the principle of confidentiality provided that the data are restricted to what is strictly necessary.

2.2.8. Right of access and rectification

Under Articles 13 and 14 of Regulation (EC) No 45/2001, data subjects have a right of access to, and rectification of, personal data concerning them.

Article 20 of Regulation 45/2001 provides for restrictions on the right of access, especially if such restriction constitutes a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences. This Article has been interpreted by the EDPS as also authorising limitations in the context of disciplinary investigations (see opinion 2004-0198). It seems that this limitation could be applied in certain cases in the event of an investigation on the basis of Security Directorate recordings. The EPDS wishes to stress that such a restriction must be limited to the time necessary in the context of an investigation.

The system permits access for data subjects to the recordings involving them. The possibility of rectification of the data would appear highly unlikely since, with the recordings being made live, they reflect the reality of the call.

2.2.9. Information to be given to the data subject

Under Article 11 of the Regulation, whenever personal data are processed, data subjects must be sufficiently informed of this processing. 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 20 allows for exceptions to this principle, in particular when such a measure is necessary to safeguard "the prevention, investigation, detection and prosecution of criminal offences" (Article 20(1)(a)) or to safeguard "the national security, public security or defence of the Member States" (Article 20(1)(d)).

According to the information received by the DPO, under cover of the exemption under Article 20(1)(a), no advance information is provided about the recording system, and the recording of the call is not mentioned to the caller. The duty staff of the Security Office, on the other hand, is informed about the recording of calls and the use made of them. However, a draft confidentiality statement, for inclusion on the Security Directorate's website, informs data subjects internally at the Commission about the recording of data, and reproduces the content of Article 11 of the Regulation. The EPDS supports this initiative.

It is also possible that persons not on the Commission staff might use the Commission telephones to call the emergency number. As for persons from outside, a statement that the lines are recorded is to be added to the electronic directory available from outside the Commission. However, for full compliance with Regulation 45/2001, the EDPS recommends making provision for at least one link to the other Article 11 information.

2.2.10. Security

Article 22 of the Regulation lays down that technical and organisational measures must be taken to ensure a level of security appropriate to the risks represented by the processing and by the nature of the personal data to be protected.

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

Conclusion

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

- any restriction on the right of access to data must be strictly limited to the time necessary in the context of an investigation;

- the draft confidentiality statement to be included on the Security Directorate's website must properly inform data subjects internally at the Commission about the recording of data, by reproducing the content of Article 11 of the Regulation;

- in the reference to lines being recorded which is to be added to the electronic directory available from outside the Commission, at least one link must be provided to the other Article 11 information.

Done at Brussels, 22 May 2006

J. BAYO DELGADO
Assistant European Data Protection Supervisor