

(16.06)



SN 2692/09
(OR. fr)

Opinion on the notification for prior checking from the Data Protection Officer of the European Commission in relation to the dossier on recording the line reserved for calls to the dispatch centre for technical services in European Commission buildings in Brussels.

Brussels, 19 November 2008 (Case 2008-491)

1. Procedure

On 25 August 2008, the Data Protection Officer of the European Commission sent a notification for prior checking under Article 27(3) of Regulation (EC) No 45/2001, in relation to the dossier on recording the line reserved for calls to the dispatch centre for technical services in European Commission buildings in Brussels. Questions were put to the controller on 2 October 2008. A meeting was arranged by the controller on 10 October 2008 in order to clarify the facts. After a number of exchanges of e-mails, the suspension was lifted definitively on 20 October 2008. The draft opinion was sent for comments to the controller on 12 November 2008. The comments were received on xx November 2008.

2. The facts

In the event of technical problems, staff in Brussels may dial the telephone number shown in all Commission buildings in Brussels: 5555. The technical problems concerned can be of different types: problems with electricity and lifts, heating, air-conditioning, leaking water, keys, windows, carpentry, noise, painting, etc. A detailed description of the types of maintenance possible via the 55555 line is available on the Commission intranet site at the following address: http://intracomm.cec.eu-admin.net/pers_admin/office_bxl/cleaning/index_fr.html.

For safety problems in relation to people or property, the 22222 line is used¹. That line is not concerned by this analysis as it has already been the subject of a prior check by the EDPS².

The 5555 technical service dispatch centre number is also accessible from the Commission, using the same format as for all Commission numbers, i.e. by dialling 02/295 55 55.

Telephone calls to 55555 (incoming calls) are recorded for a period of six months in order to ensure that the service is working efficiently. Operators of the technical service dispatch centre (the 55555 line) thereby have the possibility of checking/listening again to the data communicated through the 55555 number to ensure that the messages were properly understood. The recording also enables operational events to be checked *a posteriori*. The objective of such *a posteriori* checks is not to evaluate the work of the operators. They are also a means of justifying the action taken (or not taken) by the service in response to a 55555 call. In the context of dossiers relating to health and safety problems, the Security Directorate or the Occupational Health and Safety Unit may also request access to certain recordings. For example, the Occupational Health and Safety Unit may ask the service responsible for managing the 55555 line for information on the number of requests relating to air conditioning during a specific period for a specific part of a building in order to determine the means by which an illness was spread. Such requests are relatively rare and fall within the framework of inter-departmental cooperation.

¹ Previously 88888.

² See the opinion published by the EDPS on 22 May 2006 (Case 2006-002) on recording the line reserved for emergency and security calls in Brussels (88888).

The date, time and duration of calls are also recorded. However, the system used does not allow the number used (internal extension, external number or mobile telephone number) or details of the caller to the 55555 line to be known automatically. The person concerned may obviously call from a location other than that for which the technical maintenance is required. Information relating to the location, the nature of the maintenance required and the contact details of the caller are generally requested by the operator.

The possibility of the 55555 line being used by non-Commission personnel present on Commission premises or even calling from outside (e.g. staff of contracting companies) cannot be ruled out.

The data subjects in respect of calls to the 55555 line are informed through different channels. The Intracomm page mentioned above states that recordings of calls will be kept for 6 months. The Intracomm site also contains a notice on the protection of personal data relating to the processing operation. The notice specifies the controller of the processing operation, its purposes, legal basis and the data retention period, the recipients of the data, and the rights of access to and rectification of the data, and the right to have recourse at any time to the European Data Protection Supervisor. The electronic telephone directory mentions in relation to the 55555 line that calls are recorded, and a link to a specific confidentiality declaration is available.

In addition, the following paragraph appears on the general Intracomm page:

"Appels enregistrés: Certaines extensions sont enregistrées pour des raisons de service: (...) 55555 Dispatching technique + Lien vers la déclaration spécifique de confidentialité (de OIB.RE.2) http://intracomm.cec.eu-dmin.net/pers_admin/office_bxl/documents/data-protection-technical-helpdesk_fr.pdf".

Lastly, the recording system now allows the caller to be informed directly that the telephone conversation is being recorded. If the data subject has further questions after listening to the automatic message, he/she can put questions to the call operator, who has received specific training in this field. If that information is insufficient, the operators have instructions to refer the data subject to the assistant controller.

The operators have received specific training and have available to them the notice on the protection of personal data.

The processing is partly automated: the telephone conversation between the caller and the 55555 operator is recorded on a magnetic band mini-cassette attached to a PC.

To check the requests submitted by the callers (in the event of audibility problems and/or to reconfirm the essential elements of a request, in the case of a fire alert for example) and for certain investigation reports from the Security Directorate, the Occupational Health and Safety Unit or Unit OIB.RE.2 (Technical Service), the recordings are listened to and/or used by operators and the officials responsible for supervising the 55555 line. In certain cases, the processing is therefore manual.

A private company provides the standby service for the 55555 line as part of the operation of the technical service dispatch centre which has been subcontracted to it by the Commission. All the operators of the 55555 line are from that private company and they are supervised by officials from Unit OIB.RE.2. All the operators of the 55555 line from the private company work in Commission buildings with equipment and facilities provided by the Commission.

The 55555 line is available 24 hours a day/7 days a week.

Outside Unit OIB.RE.2 (statutory staff and subcontractors), only staff from the Security Directorate and the Occupational Health and Safety Unit have access to the data in the event of an investigation, as mentioned above.

In future, recordings will be kept for only three months, rather than the current six months. It is not planned to erase the recordings before the expiry of the data storage period. However, in response to a specific request, data can be erased within an hour of agreement by the controller.

Recording is carried out with the assistance of a computer system installed in secure Commission premises, accessible only to authorised persons. The computer system is protected by a password known only by the operators and by two officials. On each login, the system provides information on the most recent connection made. Only the above persons can use the system. The computerised storage media (magnetic tapes) are kept in the same secure premises. The same storage media are reused within a period of at most 6 months and the data recorded are automatically deleted. The recordings are not transcribed onto paper (except, possibly, in the context of an investigation report), but rather are stored only on computer media.

3. Legal aspects

3.1. Prior checking

The prior check concerns the processing of personal data ("any information relating to an identified or identifiable natural person", Article 2(a) of the Regulation) in relation to the recording of calls to the 55555 line. It involves the recording of communications between two persons, at least one of whom is identified or at least "identifiable". In some cases the caller identifies him/herself. The processing includes the collection, consultation and storage, etc. of data. It is carried out by a European institution in the exercise of activities all or part of which fall within the scope of Community law. The processing of personal data is done largely by automatic means (Article 3(2) of the Regulation). This processing therefore falls within the scope of Regulation (EC) No 45/2001.

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*".

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 particular processing of such data constitutes a specific risk within the meaning of Article 27(1).

Article 27(2) contains a list of processing operations that are likely to present such risks. Under Article 27(2)(a) of the Regulation, processing operations relating to "*suspected offences, offences, criminal convictions or security measures*" are also subject to prior checking by the EDPS. In the case at hand, contrary to what is stipulated in the notification, the processing operation does not concern data of this kind. Such data are more likely to arise in the case of calls to the 22222 line relating to security (see above).

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be issued prior to the start of the processing operation. In this case, however, the processing operation is already under way. This should not pose any serious problems, however, since the recommendations made by the EDPS can still be adopted if necessary.

Notification from the DPO was received on 25 August 2008. Pursuant to Article 27(4), the present Opinion must be delivered within two months of receipt of the notification. The procedure was suspended for xx days (18 + xx + the month of August). The Opinion will therefore be delivered no later than xx November 2008.

3.2. Legal basis and lawfulness of the processing operation

The Commission Decision of 6 November 2002 (2003/523/EC) establishes the Office for infrastructure and logistics in Brussels (OIB). Article 3 of the Decision lists the Office's tasks: "The Office shall be responsible (...) in respect of the Brussels site, for: (d) implementing rules relating to the physical security of buildings (...); (g) adopting the necessary measures to ensure compliance with health and safety requirements in Commission buildings." The legal basis is therefore valid.

Article 5(a) of Regulation (EC) 45/2001 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 recording is necessary for the performance of the missions assigned to Unit OIB.RE.2, which is responsible for the maintenance of Commission buildings in Brussels. The establishment in this context of the 55555 emergency line enables it to better manage urgent technical action relating to the maintenance of buildings. The processing operation is therefore lawful.

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 except in the circumstances set out in Article 10(2).

In general, the processing operation should not concern special categories of data. It cannot be ruled out, however, that information relating to the health of an individual may appear in recordings of calls to the 55555 line, in cases where the data subject refers to his/her health as the reason for requesting a maintenance operation. In most cases, the data subject will have consented to the processing of his/her data, thereby justifying processing on the basis of Article 10(2)(a).

3.4. 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 entire conversations held on the 55555 line, as well as the time and length of the call.

It is not desirable to select data from the conversation, since in principle all the data are relevant from the point of view of the objectives pursued. The other traffic data are also needed for processing purposes.

Moreover, 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). As for fairness, this relates to the information which must be transmitted to the data subject (see section 3.9 below).

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

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

3.5. Data storage

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)).

Storage 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, i.e. the data necessary to establish calls, must be erased or made anonymous upon termination of the call. Exceptions to this principle are provided for under Article 20, particularly when such an exemption is necessary to "safeguard the protection of the data subject".

The data on telephone conversations are stored for 3 months. This storage of data, particularly traffic data, after the end of the call may be based on the exemption provided for in Article 20.

In the event of the processing of data necessary for a security investigation or an investigation by the Occupational Health and Safety Unit, the data are held until the investigation and any legal appeals have been concluded. This retention period is also justified in terms of the exemption provided for in Article 20.

3.6. Transfer of data

Article 7(1) of the Regulation stipulates: "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".

As already mentioned, outside Unit OIB.RE.2 (statutory staff and subcontractors), only members of the Security Directorate and the Occupational Health and Safety Unit will be, on an exceptional basis, the recipients of data. The data are necessary for the legitimate performance of tasks covered by the competence of the recipient and Article 7(1) is therefore complied with.

When data are transferred following a request from the recipient, both Unit OIB.RE.2 and the recipient bear the responsibility for the lawfulness of the transfer, in accordance with Article 7(2). Unit OIB.RE.2 is required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller must seek further information from the recipient.

In any case, pursuant to Article 7(3) of the Regulation, the recipient must be informed that personal data can be processed only for the purposes for which they were transmitted.

3.7. Confidentiality of data

Under Article 36 of the Regulation, Community institutions and bodies must 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 actual content of communications. In principle it prohibits any interception or recording of communications. Any restriction on 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 on 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 (health and safety at work), the EDPS considers that there is no breach of the principle of confidentiality provided that the data are restricted to what is strictly necessary.

3.8. 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.

The system permits access for data subjects to the recordings concerning them. The possibility of rectification of the data would appear highly unlikely since, as the recordings are made live, they reflect the reality of the call. However, rectification or deletion is possible by contacting the Head of Unit OIB.RE.2.

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 restrictions in the context of disciplinary investigations (see Opinion 2004-0198). It seems that this limitation could be applied in certain cases, extremely rare according to the controller, in the event of an investigation on the basis of recordings transferred to the Security Directorate. The EDPS wishes to stress that such a restriction must be limited to the time necessary in the context of an investigation.

3.9. 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 the operation. This information should usually be given at the latest when the data are collected from the data subject, unless the data subject has already been informed.

As already mentioned, such information is provided to the data subject through various channels. Callers to the 55555 line are automatically informed that all calls are recorded for security reasons. This information has the advantage of reaching all data subjects, whether they call from within or outside the Commission. The EDPS is pleased that Unit OIB.RE.2 has established a large number of information channels and is therefore in compliance with Article 11 of Regulation (EC) 45/2001.

3.10. Management of a processing operation on behalf of the controller

As mentioned above, a private company provides a standby service for the 55555 line as part of the operation of the technical service dispatch centre which has been subcontracted to it. The staff of that company work exclusively in Commission buildings, using installations and equipment supplied by the Commission.

Where a processing operation is carried out on its behalf, Article 23 of the Regulation stipulates that the controller must choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by the Regulation. The carrying out of a processing operation by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor must act only on instructions from the controller and that the obligations with regard to confidentiality and security are also incumbent on the processor.

In the present case, Unit OIB.RE.2 fulfilled its obligation since the terms of the call for tender stipulate the obligation of the contractor to guarantee the confidentiality of the personal data processed by the contractor for the sole purposes of executing the framework contract, in accordance with the provisions of Regulation (EC) 45/2001. This obligation is laid down in the contract (II.9 and II.10).

Under Article 23(2)(b), the obligations set out in Articles 21 and 22 are also incumbent on the processor. In the case under consideration, however, as explained in the "facts" section, only one processing operation is subcontracted (the staff responsible for the telephone standby), and the rest of the processing, including security, is the responsibility of the Commission. This is underlined by the fact that the processing is carried out in Commission buildings and using Commission facilities. The security measures put in place are analysed below.

3.11. Security

Article 22 of the Regulation stipulates 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 in-depth examination of the security measures adopted, 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 means in particular that:

- the recipients of the data should be informed that the personal data can only be processed for the purposes for which they were transmitted, in accordance with Article 7(3).

Done at Brussels, 19 November 2008

Summary:

In the event of technical problems, staff in Brussels may dial the telephone number shown in all Commission buildings in Brussels: 5555. Such technical problems can be of different types: problems with electricity, lifts, heating, air conditioning, leaking water, keys, etc. Telephone communications to 5555 line (incoming calls) are recorded for a period of three months to ensure that the service is working efficiently. Article 36 of Regulation 45/2001 establishes the fundamental principle of the confidentiality of data. This particular data processing operation constitutes a specific risk within the meaning of Article 27(1) and should be subject to prior checking by the EDPS. The EDPS is very satisfied with the measures put in place by the Commission in order to comply with the Regulation. However, the EDPS recommends that recipients of the data should be informed that the personal data can only be processed for the purposes for which they were transmitted, in accordance with Article 7(3).

(signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor