Opinion on the notification for prior checking received from the Data Protection Officer of the Council of the European Union relating to recordings of communications made over the Security Centre's telephone lines, building interphones and radios used by the General Secretariat of the Council (GSC) Security, Prevention and Medical Departments

Brussels, 23 January 2006 (Case 2005-0364)

1. Procedure

1.1. On 23 November 2005, the European Data Protection Supervisor (EDPS) received a notification for prior checking in accordance with Article 27 of Regulation (EC) No 45/2001 (hereinafter called "the Regulation") from the Data Protection Officer of the Council of the European Union (DPO). This notification concerned the recordings of communications made over the Security Centre's telephone lines, the building interphones and the radio equipment used by General Secretariat of the Council (GSC) Security, Prevention and Medical Departments.

1.2. The notification follows the DPO's consultation by telephone and e-mail on the need for prior checking by the EDPS.

1.3. The notification was accompanied by Decision 198/03 of the Secretary-General concerning the tasks of the Security Office; by a staff note dated 18.11.2005 (195/05) on emergency calls to the Security Office and by the instructions governing the recording of communications made over the Security Centre's telephone lines.

1.4. On 14 December 2005, the EDPS submitted an information request to the controller. This information was supplied on the same day. Additional information was requested on 16 January 2006 and a reply was provided the same day.

2. Examination of the matter

2.1. The facts

All calls to number XXXX, to the numbers of the Central Security Dispatch Centre *[Centre de Sécurité - dispatching]* (XX, XX, XX and XX XX XX) and via interphone are recorded by the Security Centre, which operates a 24-hour service 7 days a week as part of the mission of the Security Office as laid down in Decision 198/03 of the Secretary-General /High Representative. The same applies to all communications over the dedicated radio links of the GSC departments responsible for security, prevention and assistance.

Any person who witnesses an accident or an incident which poses a threat to persons or property must report this immediately by ringing a single telephone number (XX) or, in the lifts or car parks, by using the emergency interphones.

It cannot be ruled out that persons other than GSC staff may call the numbers or use the means provided for emergency purposes (the interphone for example).

Callers must mention their name, location (building, floor, lift, room, etc.) and the reason for the call. Depending on the nature of the incident, the security officer will immediately notify the relevant emergency department (for example, medical service, ambulance service, fire brigade, police) and send a first emergency response team to the spot.

A* or B* officials on-duty in the Internal Protection Service and the Director of the Security Service may listen to the recordings if this proves necessary in order to:

- determine the exact course of events and conversations where the nature and content of a call is in dispute;
- analyse threat calls;
- verify compliance with the Security Office's internal instructions ("verify that the instructions are properly observed"). These rules/guidelines/instructions govern the activity of Security Office staff and of the guards who support them in carrying out their duties.

In the event of an extreme emergency arising from immediate danger or at the request of the police services [1], the security guard will inform the on-duty A* or B* official and pending the latter's arrival will listen to the tape; the full text of the recording in question will be transcribed forthwith. Any intervention will be entered in the Security Centre's logbook.

To that end, the magnetic tapes containing the recordings will be kept for six months.

Where immunity is withdrawn as part of a judicial inquiry or where a person has been caught in the act, the Deputy Secretary-General may authorise the data to be shared with the Belgian judicial authorities.

Any subject of such data processing (official, other servant, etc.) has a right of access to the data which concern him or her. Those rights may be exercised by submitting a written request to the Director of the Security Office.

Staff were informed of the procedure in general terms by means of the Staff Note of 18.11.2005 (195/05). Where recordings are listened to, the parties involved will be informed as soon as possible so as to safeguard their rights and freedoms.

The magnetic tapes are kept in a safe in a secure room in a secure area. The safe contains a register for logging when tapes are changed.

[1] The police may access data where the Deputy Secretary-General so authorises for the purpose of a judicial inquiry by the host country or where a person has been caught in the act.

2.2. Legal aspects

2.2.1. Prior checking

Regulation No 45/2001 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 case in point concerns the processing of data by the General Secretariat of the Council, i.e. a Community institution and a processing operation within the framework of first pillar activities and hence the Community scope of application.

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.

The case here concerns the processing of personal data, as it involves the recording of communications between two identified or identifiable persons [2]. The recording process is automatic. Where the emergency or verification procedure is implemented, part of the communication is transcribed, which amounts to manual processing since the data are entered in a file.

Article 27(1) of Regulation (EC) No 45/2001 subjects 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" to prior checking by the EDPS. The confidentiality of communications is so sensitive an issue that it forms the subject of a special provision in the Regulation (Article 36). In this context, it may be affirmed that a risk such as that referred to in Article 27(1) of the Regulation exists.

Moreover, Article 27(2) of the Regulation lists the processing operations likely to present such risks. Article 27(2)(b) requires the prior checking of processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct. One of the identified goals of recording conversations is to verify that the Security Office's internal rules are observed and more specifically that security staff have complied with them. The processing operation is therefore intended, albeit only partially, to evaluate the conduct of certain persons. It could also lead to the adoption of disciplinary measures. For these reasons, the processing must be subject 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. However, this does not alter the fact that it would be desirable for the recommendations issued by the European Data Protection Supervisor to be implemented.

As already mentioned, all interventions will be entered in the Security Dispatch Centre's logbook. This prior checking exercise is not aimed at analysing the processing of data in the context of this logbook but is confined to the specific processing operation under discussion.

---

[2] The caller is supposed to identify himself/herself at the beginning of the call. The person receiving the call is identified as the person on duty at the time of the call.

The DPO's notification was received on 23 November 2005. In accordance with Article 27(4), this opinion must be delivered within the two following months. The Supervisor will therefore deliver his opinion by 24 January 2005 at the latest.

2.2.2. Legal basis and lawfulness of processing

Article 23 of the Council Decision of 22 March 2004 adopting the Council's Rules of Procedure stipulates that the Council shall decide on the organisation of the General Secretariat. On that basis the Secretary-General of the Council adopted a Decision concerning the tasks of the Security Office (Decision 198/03). The preamble to the Decision states: "It is necessary to ensure the provision of efficient security for the Council and its subordinate bodies, their activities, its staff and visitors, as well as its buildings and the property and resources contained therein and the proprietary, sensitive and classified information circulating within it, in compliance with the provisions of the Staff Regulations and other applicable rules of law in force". The Decision stipulates that it is for the Security Office to ensure such protection (Article 2(1)). In cases of extreme urgency, the Security Office may, with the authorisation of the Secretary-General or of the Deputy Secretary-General have access to all documents and information to the extent necessary for the enquiry (Article 6(1)). Moreover, the Security Office is responsible for managing a central Security Dispatch Centre operating 24 hours a day and for reacting to emergencies in the event of an alert, incident or accident (Article 9(1)).

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 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". The legal basis deriving from the abovementioned provisions supports the lawfulness of processing.

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 unless grounds can be found in Article 10(2).

Information relating to a person's state of health may appear in the recording of emergency calls precisely because some calls are medical emergency calls. In that case, processing may be regarded as authorised under Article 10(2)(b), which authorises processing of sensitive data where it is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof.

Moreover, Article 10(2)(c) also authorises the processing of such data 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 or her consent. This provision serves to justify the processing of sensitive data relating to persons other than Council staff whose vital interests are at stake.

2.2.4. Data quality

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

The data which form the subject of this prior checking cover all calls which are made to number XXXX, to the numbers of the Security Dispatch Centre, by the dedicated radio links of GSC departments and via interphone and which are recorded by the Security Centre. It is unreasonable to select data from the conversations themselves because all data are, in principle, relevant to the aims pursued.

2.2.5. Data storage

Data relating to telephone conversations are held for six months.

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.

The Regulation provides that the data are "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)).

Moreover, under Article 37(1), traffic data, i.e. data necessary to establish calls, are erased or made anonymous upon termination of the call. However, Article 20 provides for exemptions from this principle, especially where such exemption constitutes a necessary measure to safeguard "the prevention, investigation, detection and prosecution of criminal offences", "the data subject " or "the national security, public security or defence of the Member States". The EDPS interprets the provision "to safeguard the prevention, investigation, detection and prosecution of criminal offences" in the light of its *ratio legis* and hence as applying also to disciplinary inquiries [3]. All are exemptions justifying storage of the data after the call for a six month period or more in the event of an inquiry.

Moreover, Article 37(2) provides for data to be kept for the purpose of telecommunications budget and traffic management, including the verification of the authorised use of the telecommunications systems for no more that six months after collection, unless they need to be kept longer in order to establish, exercise or defend a right in a legal claim pending before a court. This provision therefore permits storage of data beyond six months in the event of an appeal before a court.

2.2.6. Transfer of data

In the event of an incident, the recorded data will be communicated to the A* or B* staff on duty at the Internal Protection Service and to the Director of the Security Office.

Under Article 7 of Regulation No 45/2001, personal data may be transferred within a Community institution only if they are necessary for the legitimate performance of tasks covered by the competence of the recipient. This is the case here: the instructions regarding listening to the Security Centre's recordings (adopted on the basis of Decision 198/03) provide

[3] See EDPS opinion 2004-198 of 21 March 2004.

that it is the A* or B* official responsible who listens to the tape and who, in case of an emergency, informs the Director of the Security Office. These persons must therefore have the technical means for examining the calls.

Where immunity is withdrawn during a judicial inquiry or where a person is caught in the act, the Deputy Secretary-General may authorise the data to be shared with the Belgian judicial authorities. In that case, Article 8 (covering the transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46/EC) is applicable.

Directive 95/46/EC is not aimed at judicial activities. However, apart from certain Articles, the Belgian law of 8 December 1992 on the protection of personal data is applicable to public authorities when carrying out their judicial police duties (Article 3(5) thereof). Hence, Article 8 of the Regulation is applicable in that it provides that the transfer may take place only if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, which is the case here.

2.2.7. Data confidentiality

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 obligation of confidentiality applies to the content proper of the communication. In principle, it prohibits any interception or recording of communications. Any restriction on this principle will have to comply with the general principles of Community law. The latter concept refers to the notion of fundamental rights as laid down in the European Convention on Human Rights.

In practice, this means that any restriction on the confidentiality of data must respect fundamental rights as laid down in the Convention. No restriction may be imposed unless it is in accordance with the law and is necessary in a democratic society, in particular, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others.

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

In this case, since communications are recorded with the knowledge of the data subjects and for reasons of national security, public safety, for 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.

The use of the recordings for disciplinary proceedings cannot be ruled out. The reference in Article 36 to respect for the general principles of Community law does not exclude such use provided that the principle of proportionality is observed. Any use of the recordings to assess security staff in a more general manner (for the purpose of promotion, for example) would go beyond what is permissible.

Moreover, as we are dealing with an exemption from the principle of data confidentiality, it is

important to stress that the aim of verifying whether the Security Office's internal rules have been observed must be interpreted narrowly and may not serve to check the conduct of staff in general. Verification should be carried out against the instructions, i.e. written rules laid down by the Security Office and accessible to the staff concerned.

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 their own personal data and the right to rectify them.

The Council Decision of 13 September 2004 adopting implementing rules concerning Regulation No 45/2001 provides in section 5 for procedures for data subjects to exercise their rights. Moreover, the Security Office's internal instructions to Security Centre staff state that any data subject concerned by such data processing (official, other servant, etc.) has a right to access the data concerning him/her by submitting a written request to the Director of the Security Office.

Article 20 of Regulation No 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. The EDPS has interpreted this Article as also allowing limitations in the context of a disciplinary investigation (see opinion 2004-0198). It appears that such a limitation could be imposed during certain investigations based on Security Centre recordings. The EDPS wishes to stress that such a restriction should be limited to the purposes of the investigation and to the time necessary for conducting it.

2.2.9. Information for data subjects concerned

Pursuant to Article 11 of the Regulation, if personal data are to be processed, the data subject must be given adequate information. The information should normally be provided at the latest when the data are obtained from the data subject, except where he or she already has it.

The Staff Note of 18.11.2005 (195/05) informs the data subject of the identity of the controller; the purposes of the processing operations, the persons to whom the data are to be communicated, rights of access, the possibility of referring the matter to the European Data Protection Supervisor, and how long the data are to be kept.

It cannot be ruled out that persons other than GSC staff may call the numbers or use the means provided for emergencies such as the interphone. Where such communications are recorded, appropriate means for informing persons external to the GSC must be put in place.

2.2.10. Security

Article 22 of the Regulation provides 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 careful scrutiny of the security measures taken, the EDPS concludes that they are adequate in the light of Article 22 of Regulation (EC) No 45/2001.

Conclusion

The proposed processing does not seem to involve any breach of the provisions of Regulation (EC) No 45/2001 provided that account be taken of the above observations. This implies in particular that:

– the aim of verifying compliance with the Security Office's internal rules must be interpreted strictly and may not be used to verify the conduct of staff in general. Verification should be carried out against the instructions, i.e. written rules established by the Security Office and accessible to the staff concerned,

– any restriction on the right of access should be limited to the purpose of the investigation or inquiry and the time necessary for conducting it,

– where the communications of persons external to the GSC are recorded, appropriate means of information should be put in place.

Done at Brussels, 23 January 2006

Peter HUSTINX
European Data Protection Supervisor