Opinion on a notification for Prior Checking received from the Data Protection Officer of the Commission on Voice Logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten

Brussels, 29 April 2009 (Case 2008-0014)

1. Proceedings

1.1. On 7 January 2008, the EDPS received the formal prior checking notification under Article 27 by e-mail from the Data Protection Officer (DPO) of the Commission on Voice Logging at Joint Research Centre Institute for Energy **(**JRC-IE) in Petten.

1.2. On 31 January 2008 the EDPS made a request for further information. The EDPS received a reply to this request on 23 June 2008. As not all questions were answered a further request was made on 25 June 2008. This was answered on 24 February 2009.

1.3. On 26 March 2008, the EDPS extended the deadline within which to adopt his opinion on the basis of Article 27.4 of Regulation (EC) No 45/2001 (hereinafter Regulation 45/2001).

1.3. On 20 April 2009, the EDPS sent the draft opinion for comments from the controller. These comments were received on 27 April 2009.

2. The Facts

The sector SES (Safety Environment Security) at the JRC-IE in Petten records incoming and outgoing calls electronically.

The system records conversations between people calling the general phone number of JRC-IE (switchboard), the emergency centre[1] and crisis room[2]. It also records the calling telephone number, the called telephone number, date, time and length of the conversation.
The calls recorded can be divided in four groups:
a) communications internally between guards,
b) communications between guards and authorities (mainly through special lines) like police, fire brigade etc.,
c) communications between persons on site and the local alarm number
d) communications to the switchboard (either internally or externally).

[1] This covers the emergency number; direct emergency lines to national forces (police/intervention teams and authorities); Emergency phone net (restricted to international and national institutions / authorities / intervention forces / ministries / vital infrastructure societies).
[2] Emergency phones and other phones in the crisis room.

The purpose of the processing is to be able to check the content of the calls to the lines concerned in the event of an operational incident (such as violation of public order and safety or criminal and terrorist incidents), emergencies (for example, if the fire brigade is called for intervention) and to be able to evaluate emergency training exercises at a later stage. These calls may also furnish evidence for investigations into potential threats to the institution.

Only the person qualified as Plant Security Manager or persons on standby duty for this function or duly recorded replacements in case of absence have access to the recorded calls. The Director of the JRC-IE and the Local Security Officer[3] may have access, but only in the presence of the above mentioned persons. The notification also provides that the data may be communicated to Commission staff of JRC dealing directly with incidents and System administrators. The data may be transferred to national competent authorities conducting an official investigation.

In order not to reduce the effectiveness of the system, the recording of the communication is not announced in the communication. The persons operating the switchboard and the alarm central are instructed and the use of recording devices is announced to them. A privacy statement is published on JRC-IE intranet in the special section "Personal Data Protection". This privacy statement contains information relating to the purposes of the recording, the technical means used, who accesses the data and to whom it is disclosed; the security measures put in place to protect and safeguard the data; how the person can verify, modify or delete administrative information; the conservation period; contact information and the possibility of having recourse to the EDPS.

If one of persons concerned by the communication identifies him/herself and that there are no doubts concerning his/her identity, access can be granted to the recorded communication. The persons concerned can check that data are being processed, have administrative data modified, corrected, deleted or blocked. Recorded data cannot be modified but according to the notification, a written comment can be added. In order to exercise his/her rights, the data subject can refer directly to the controller or address him/herself to the DPO.

[...]

The data is erased at the latest after one year on a FIFO basis (first in first out basis). In case of an incident the data will be kept for a longer period to establish or defend a right in a legal claim pending before a court.

3. Legal aspects

3.1. Prior checking

Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of personal data by Community institutions and bodies and on the free movement of such data applies to the processing of personal data by Community institutions and bodies.

Personal data is defined as any information relating to an identified or identifiable natural person. An identifiable person 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 or her physical, physiological, mental, economic, cultural or social identity. Since the recording cites

[3] or persons on standby duty for these functions or duly recorded replacements in case of absence

the number called and the calling number, it is possible, in most cases, to identify a person party to the recorded communication and therefore personal data is present[4].

The processing of the data is carried out by a Community body (JRC-IE) and is carried out in the exercise of activities which fall within the scope of Community law.

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

Regulation 45/2001 therefore applies.

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) contains a list of processing operations that are 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 confidentiality of communications which we consider below. This special consideration of such data must be seen as constituting a specific risk within the meaning of Article 27(1).

Furthermore, in some rare cases, data relating to health could possibly be included in the call, which also qualifies the operation for prior checking under Article 27(2)(a). This will be examined below (see 3.3. Processing of special categories of data).

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 EDPS was appointed after the system was set up, the check necessarily has to be performed ex-post. This does not alter the fact that the recommendations issued by the European Data Protection Supervisor need to be implemented.

Notification from the DPO was received on 7 January 2008. Under Article 27(4), this opinion must be delivered within the following two months. The deadline for delivery of the opinion was suspended for 388 days by requests for further information and 7 days to receive comments. The deadline was also extended for one month on the basis of Article 27.4 of Regulation 45/2001. The EDPS will therefore deliver his opinion by 6 May 2009.

3.2. Lawfulness of the processing

Article 5(a) of Regulation (EC) No 45/2001 stipulates that the processing must be "*necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution"*.

In order to determine whether the processing operations comply with Article 5(a) of Regulation (EC) No 45/2001 two elements must be taken into account: first, whether either the Treaty or other legal instruments foresee a public interest task on the basis of which the data processing takes place (*legal basis*), and second, whether the processing operations are

[4] At the very least it will in principle be possible to identify the member of staff at JRC-IR receiving or initiating the communication.

indeed necessary for the performance of that task, i.e. necessary to achieve the intended goals (*necessity*).

Legal basis. According to the controller, the processing operation is based on legal obligations stemming from mandatory national legislation.
The Petten site - JRC IE - has been designated by the IAEA as a nuclear facility, a nuclear reactor and nuclear laboratories, facilities are located on the premises of the JRC in Petten. Therefore the Nuclear Law (Kernenergiewet, Dutch Law from 21.02.1963) and "The Physical Protection of Nuclear Material and Nuclear Facilities" (recommendation INF-CIRC/225/rev4) of the IAEA apply. The Netherlands laid down its rules concerning the execution of security measures in the Regulation on "Private security organisations and investigation departments" (24.10.1997) and the requirements concerning the quality of the security equipment in the Regulation BORG "Private alarm centrals from the Dutch centre of crime prevention and security" of 28.06.2005.
In article 4.3.6 of this Regulation it is stated that all conversations which are held within the framework of the reporting of an emergency or threat using the emergency connections (everyone on the JRC premises), contact persons, police, firebrigade and security services are recorded so that a complete reconstruction of the conversations is possible. The case for the recording of in- and outgoing telephone calls is therefore stated.

The question of applicability of national law within Community institutions and bodies must therefore be addressed. Article 291 EC Treaty provides that "The Community shall enjoy in the territories of the Member States such privileges and immunities as are necessary for the performance of its tasks, under the conditions laid down in the Protocol of 8 April 1965 on the privileges and immunities of the European Communities [...]". The Community institutions therefore enjoy a special status in the Member States. However the Protocol on Privileges and Immunities does not provide for absolute extra territoriality, nor for a general exemption to all legal obligations stemming from national legislation. According to case law, the privileges and immunities recognised to the Community bodies national law have a functional nature and aim at avoiding that restrictions are made to the functioning and independence of the Community bodies[5]. National law will therefore apply if it is mandatory, if there is a legal vacuum in EU law applicable to the institutions and if the application of such a national law does not run counter to the smooth running of the institutions/bodies.

The Dutch law as quoted above is indeed mandatory and, to the extent that it does not hinder the smooth functioning of the agency, it must be applied within the JRC-IE without prejudice of the application of Regulation 45/2001 concerning data processing modalities.

Necessity. As outlined above, the necessity of the processing operation is directly linked to the purpose that such processing intends to achieve. For the purpose of respecting the Dutch legislation in view of reconstructing events in the case of emergency threats or incidents, the monitoring and recording of incoming calls can be considered as necessary.

In the light of the above, the EDPS is of view that voice Logging at the JRC-IE in Petten is legitimately considered as necessary and that the requirements for compliance with Article 5(a) of regulation (EC) 45/2001 are satisfied in principle.

3.3. Processing of special categories of data

[5] *Campogrande/Commission*, T-80/91, point 42.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life is prohibited unless grounds can be found in Article 10(2) and Article10(3) for data relating to health.

Information concerning a person's health may appear in the recording of emergency calls precisely because some calls concern medical emergencies. In most cases, processing can 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.

In those few other cases, in which special categories of data may be processed during the recording of a communication and in which no "vital interests" are at stake, the EDPS may agree to the processing of such data on the basis of Article 10(2)b providing the adoption of specific guarantees. These guarantees are notably provided for in the recommendations made in the present opinion.

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".

The data which are subject to the present prior check are records conversations between people calling the switchboard of the centre, the emergency centre and crisis room and the calling telephone number, the called telephone number, date, time and length of the conversation. In the event of an incident, the recording of the entirety of a call to the emergency centre and crisis room is considered as adequate and necessary as well as the recording of the calling telephone number, the called telephone number, date, time and length of the conversation. It is indeed 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 EDPS is satisfied that these data are adequate and not excessive in the light of Article 4 of the Regulation.

Data must also be "processed fairly and lawfully" (Article 4§1(a) of the Regulation). Lawfulness has already been discussed in paragraph 3.2 above. Concerning fairness, this relates to the information which is to be communicated to the data subject (see below, 3.9 Information to the data subject).

Finally, data must be "accurate and, where necessary, kept up to date; 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 " (Article 4§1(d) of the Regulation). The direct recording of the call contributes to guaranteeing that the data concerning the recorded conversation are accurate. As concerns administrative data, the right of access and rectification as examined below (see paragraph 3.8), is also relevant in guaranteeing the accuracy of the data.

3.5. Conservation of data

According to the notification, the data is erased at the latest after one year on a FIFO basis (first in first out basis). In case of an incident the data related to the incident will be kept for a longer period to establish or defend a right in a legal claim pending before a Court.

The general rule as concerns conservation of data is provided in Article 4(1)(e) of the Regulation according to which personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

Article 37 of Regulation (EC) 45/2001 provides for specific measures as concerns the conservation of traffic and billing data which are processed and stored to establish calls and other connections over the telecommunications network. Data such as the calling number, the called number, time and data of the communication are considered to be considered as traffic data. The actual recording of the communication however is not considered as traffic data (see below 3.6 Confidentiality of communications).

Article 37(1) of the Regulation provides that traffic data should be erased or made anonymous upon termination of the call or other connection. However Article 20 of the Regulation permits for certain exceptions to Article 37 enabling longer conservation periods notably when such a restriction constitutes a necessary measure to safeguard "the national security, public security or defence of the Member States". As mentioned above, the recording of the communications to the switchboard and to the emergency centre and the crisis room are based on a national law on the basis of public security. The restrictions to immediate erasure therefore justify the keeping of traffic data surrounding calls made to the switchboard, to the emergency centre and the crisis room during a certain period in certain specific cases falling within the scope of Article 20.

The principle of limited conservation according to the purpose of the collection of the data should therefore nevertheless still need to be applied. In this respect the EDPS questions the conservation of data for one year should no incident be recorded. Should an incident be recorded, the data should be kept only for the purpose of investigation and only for the period necessary for this investigation. .

Furthermore, the storing of the actual content of the communication would need to be harmonised with the conservation period of traffic data.

The EDPS therefore recommends that the JRC-IE revise the conservation periods of the data according to the above.

3.6. Confidentiality of communications

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.

The legal basis as set out above (see 3.2 Lawfulness of the processing) justifies the recording of communications on the emergency line or in a crisis centre in accordance with national mandatory law. Article 36 is therefore respected.

3.7. Transfer of data

As mentioned in the facts, the Director of the JRC and the Local security Officer may have access to the recordings, but only in the presence of the Plant Security Manager and his deputy. The notification also provides that the data may be communicated to Commission staff of JRC dealing directly with incidents and System administrators. These transfers should be scrutinised in the light of Article 7§1 of the Regulation which covers the transfer of personal data within or between Community institutions or bodies and which may only take place "if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient". The competence of the recipients stated above seems to be reasonably founded. As to the necessity of the transfer, this will need to be established on a case by case basis. Furthermore, in accordance with Article 7§3 "the recipient shall process the personal data only for the purposes for which they were transmitted". This must be reminded to the recipients of the data.

Data are also communicated to Dutch national authorities in case of incidents.

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. Directive 95/46/EC does not in principle cover judicial activity in the criminal field (Article 3.2), so Article 8 of the Regulation is not automatically applicable. That being 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. The Dutch data protection law in principle also applies to judicial authorities. If the Dutch data protection law indeed applies, Article 8 of the Regulation 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, Article 9(6)(d) is applicable, whereby the transfer is permitted on the grounds that it is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

3.8. Right of access and rectification

Article 13 of Regulation (EC) No 45/2001 establishes a right of access upon request by the data subject. Article 14 of Regulation (EC) No 45/2001 provides the data subject with a right of rectification.

The data subject can request to access his/her data. The notification does not however mention any restrictions to this right of access. One could however consider that in some cases, access is restricted for the purpose of investigation of a disciplinary or criminal incident. In such a case, Article 20 could apply if such restriction constitutes a necessary

measure to safeguard the prevention, investigation, detection and prosecution of criminal offences[6]. The EPDS underlines that such a restriction must be limited to the time necessary in the context of an investigation. Persons concerned should also be made aware of the possibility of such restrictions to their right of access based on Article 20 of the Regulation (see below 3.9 Information to the data subject).

According to the privacy statement, administrative data can be modified. Recorded data cannot be modified but a comment can be added. This is not a problem according to the EDPS as the accuracy of the recorded data implies that no rectification need, in principle, take place.

3.9. Information to the data subject

Regulation (EC) No 45/2001 provides that the data subject must be informed where his or her personal data are processed and lists a series of specific items of information that must be provided. In the present case, some of the data are collected directly from the data subject and therefore Article 11 of the Regulation applies.

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.

However, as concerns communications internally between guards, communications between guards and authorities (mainly through special lines) and communications between persons on site and the local alarm number information is already provided. Indeed, authorities are aware of the legal obligation of recording of the communications and information is provided to persons operating the switch board and alarm central. The guards on duty in the sector SES (external company) are also informed of the recording of calls and the use made of them. Furthermore a privacy statement, for inclusion on the intranet site informs data subjects internally at the JRC-IE about the recording of data, and reproduces most of the content of Article 11 of the Regulation. The EDPS would further recommend that this information be given to staff members when they take up their jobs at JRC-IE or at least that they be notified by e-mail or by other means of the existence of this policy.

As to the content of the privacy statement, the EPDS notes that this privacy statement does not mention the transmission of the data to the Commission staff of JRC dealing directly with the incident/exercise and the system administrators nor the legal basis or the possible limitations to the right of access. This information should be added to the privacy statement.

As concerns information to external callers in communications to the switchboard, in view of the breach of the principle of confidentiality of communications as explained above, the EDPS recommends that information on the recording of the call is provided at the beginning of the call and that persons concerned are redirected to further information in the privacy

[6] As mentioned above, this restriction also applies to disciplinary investigations.

statement posted on the website of the JRC-IE. In this regard the privacy statement could be posted on the pages where the emergency telephone numbers are provided.

3.10. Security measures

Under Article 22 of Regulation (EC) No 45/2001, concerning the security of processing, "the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected".

[...]

Conclusion:

There is no reason to believe that the processing of personal data in the procedure of Voice logging at JRC-IE presents a breach of the provisions of Regulation 45/2001 provided the following recommendations are taken into account:

- that the JRC-IE revise the conservation periods of the data ;
- that the privacy statement be given to staff members when they take up their jobs at JRC-IE or at least that they be notified by e-mail or by other means of the existence of this policy;
- that information on the recording calls to the switchboard (internal and external) is provided at the beginning of the call and that persons concerned are redirected to further information in the privacy statement posted on the website of the JRC-IE;
- that the privacy statement includes information on the transmission of the data to the Commission staff of JRC dealing directly with the incident/exercise and the system administrators, the legal basis and the possible limitations to the right of access;
- that information contained in the privacy statement also be provided to persons outside of the JRC-IE;
- [...]

Done at Brussels, 29 April 2009

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor