Opinion on a notification for Prior Checking received from the Acting Data Protection Officer of the European Commission on the "Voice recording of Helpdesk calls"

Brussels, 23 October 2006 (Case 2006-142)

1. Proceedings

1.1. On 17 March 2006, the European Data Protection Supervisor (EDPS) received by electronic mail a notification for real prior checking in accordance with Article 27 of Regulation (EC) No 45/2001 (hereinafter the "Regulation") from the Acting Data Protection Officer (DPO) of the European Commission. This notification concerned the procedure and system of "Voice recording of Helpdesk calls" in Information Society and Media DG (DG INFSO).

1.2. The notification was accompanied by a Note to Mr Peter Hustinx, European Data Protection Supervisor from the DPO; the Privacy Statement- Voice recording System of DG INFSO IT HELPDESK calls; a broadcast note via e-mail to all DG's staff; an attachment to question 15 of the Notification DPO-886.1: the text of the short informational voice message that is to be played at the beginning of each call at the DG's IT Helpdesk.

1.3. On 30 March 2006, the EDPS made a request for further information to which he received the responses on 5 July 2006. On 4 August 2006, the EDPS made another information request, to which the responses were received on 7 August 2006. In relation to the response received another request for information was made on 8 August 2006, to which the responses were received on the same day.

On 28 August 2006, the EDPS extended the deadline by four more weeks due to the complexity of the matter.

On 8 September 2006, the EDPS indicated to the DPO of the Commission that the system as it had been presented thus far raised a number of important legal concerns. In addition the EDPS asked several further questions, to which he received the information on 21 September 2006.

On 9 October 2006, the EDPS suspended the procedure for a period of 7 by making the last information request in order to allow the DPO to give relevant comments and provide further information if necessary. This suspension was maintained for another 7 days.

2. Examination of the matter

2.1. The facts

DG INFSO plans to install a recording system to improve the quality of the support provided by the IT Helpdesk. All the conversations between the callers of the Helpdesk and the

Helpdesk operators will be recorded and stored in a NiceCall Focus II system format (NCFS). The calls recording system will be used parallel with an incident ticketing system (*Peregrine*). The original conversations will be linked to the "trouble ticket". When a user calls, the incident is reported in this system and it is either resolved or dispatched to other support groups. The information in Peregrine (timestamp, operator) can be matched to the information provided by the Nice Call Focus system to allow the identification of the conversations between operators and customers.

The defined aims of the system are:
1) to allow streamlining of the response to the support calls by allowing the re-tracing of the original conversations and the verification of the information recorded in the "trouble ticket" without having to call back the user,
2a) to allow monitoring of the quality of conversations between users and operators with the goal of improving the operator's effectiveness in managing time and the courteous gathering of information, and
2b) to simplify, shorten and increase the quality of the training of new operators due to the availability of examples of typical conversations with users in a realistic context.

The privacy statement specifically states that "*The purpose is by no means related to the Career Development Report* [hereinafter as: CDR] *system nor to similar evaluation exercises of the personnel and the information gathered by the system will not be mentioned in that context."*

The reasons given for the need to record conversations as to the first purpose: The work of the operator consists in summarising and trying to clarify the information given by the users to facilitate the work of the specialists (in support centres) that may need to intervene later on. Often the conversations are held in a non- native language for the operator which, although operators generally have adequate skills in the two main working languages, may sometimes lead to an imprecise in the interpretation of the information given by the users. The efficiency of the operators will be improved by allowing them to request to listen back the original conversations linked with the "trouble ticket" without having to call back the user to ascertain problems and dispatch it to the right support group. The controller noted that the possibility to listen again to the conversation may help in clarifying details even when the trouble ticket has been passed to other specialist support groups, without wasting the precious time of the users.

The reasons given to the need for recording conversations as to the second purpose: Helpdesks are the front-line contact with the users/customers and they account in a very large part for the perception of the quality of the service provided. The availability of realistic conversations as examples during the training phase is invaluable, as they help in consolidating the basic principles of courtesy, effectiveness and completeness in the dialogues with the customers.

The contents of the conversation will be the only element used for the monitoring the effectiveness and courtesy of the operators. The improvement of courtesy will be obtained by means of an analysis of the conversations performed by the recipients of the processing and by spotting the best and most effective practices as well as those that can be improved upon (e.g. "common mistakes"). These conversations will be played during the introductory coaching, given to the new operators, performed by the Helpdesk team leader.

To the question of the EDPS on the grounds that justify the necessity of voice recording by the Nice Call Focus II system for the proper functioning of the IT Helpdesk, the controller noted that: "In itself a recording system is not indispensable to the functioning of a Helpdesk,

but it allows enhancing the quality of the service provided while protecting, with proper management, the privacy and dignity of the workers and users concerned".

To the question of the EDPS whether less intrusive alternatives for achieving the goals of the Helpdesk (improving the quality of the support/ quality control) have been considered, the controller responded that: "Recording systems are becoming commonplace in all support organisations and it happens more and more frequently to receive information messages about the recordings when calling all sorts of call centres. This seems to become the standard answer to call centre to a common problem. The market is moving steadily towards recording systems because they represent the solution that provide the best quality and return on investment and it is very difficult to improve holistically the service without disposing of the actual data, rather than its interpretation or reports about it."

The persons calling DG INFSO's Helpdesk are primarily staff of the DG but nothing prevents external people from calling the Helpdesk. Helpdesk operators receiving the calls are either members of statutory staff or contractual staff hired through DIGIT's framework contract for the provision of Information Technology Support Services.

The Nice Call Focus II recording system has been selected for its technological simplicity, as it does not have speech analysis tools, for example, nor more advanced and sophisticated monitoring functions. The system does not provide for selective registration possibilities: the system is either active or not active. It does not have the possibility of manual activation or de-activation through the system administration tools. The selection of the recordings can therefore be performed only "a posteriori". It was also noticed that operators can not predict, at the beginning of the conversation, whether the information may be needed later for support reasons and a late beginning of the recordings may imply the loss of essential details.

The controller does not plan to make the recordings or the associated information anonymous, for two main reasons: 1) The system does not provide an automatic mechanism to do so. 2) The modification of the voice or the removal of some parts of the conversation may decrease the intelligibility of the content and this would be contrary to one of the goals (streamlining of the response to the support calls by allowing the re-tracing of the original conversations and the verification of the information recorded in the "trouble ticket" without having to call back the user).

The prior checking notification mentions that the data concerned are: phone number of Helpdesk operators, date/time stamp of beginning and end of each conversation, recording of each conversation. The Privacy Statement in addition specifies that the channel number is registered and[1] it is associated with the phone number of the Helpdesk operator. It states that "*Other information that might be recorded within the contents of a conversation is a.o. your first name, name, title, organisational unit, fax number, e-mail, address. However such data will never be subject to any processing and will be used only for the purpose of the quality control of the operation and improvement of the performance of DG INFSO's IT Helpdesk*". The operator would ask the user's identity only if that is not available by other means (e.g. callers IDs in the phone display). Users calling from outside the Commission and who may need to be called back for support purposes are requested to give their telephone numbers. It should be noted that it is impossible to record a "trouble ticket" and to provide support if the identity of the user is unknown.

[1] The correction in the text of the opinion follows the proposal of the controller, and the term "which" used in the privacy statement is substituted by "and". A corresponding change in the privacy statement is desirable.

The controller noted that the identity of the operator may be linked to the results of the queries, as it is associated with a specific phone number. In order to allow retracing of the calls, in line with the purposes of the system, knowing the identity of the operator is a necessary element. Most of the time, the physical link between the Nice Call Focus input channel number and phone number allows for the identification of the telephone number of the operator involved in the conversation. However, exceptionally, an operator may be using a colleague's phone (such as failure in phone device or system, rotation of staff in the Helpdesk office, etc).

During the training the recognition of the voice of the operator colleagues can not be excluded, though the operator's identity will not be explicitly communicated by the trainer to the trainee. The controller noted that "*it is not guaranteed that an operator's voice can be identified at 100% without sophisticated tools not available in standard services such as a Helpdesk".*

The Helpdesk Team Leader would send an e-mail addressed to Helpdesk operators that a given recording (identified on the basis of date/ time information, Helpdesk system call number and the phone extension number associated to the Helpdesk operators) is to be used for training.

On explicit written request from the operator to the Helpdesk Team Leader, the recording will be excluded from the use for training purposes. The written request should contain the identification details of the recording (such as precise data and time along with the Helpdesk system call number and associated helpdesk operator phone extension).

A Helpdesk operator could make a generic request for not using any of the recordings corresponding to the phone extension associated with his name by default. Though, it is observed by the controller that on certain occasions the operator could use another phone number.

System Administrator's utilities are available to search and listen back to the conversations either directly or after exporting them to computer files (WAV format). Reporting facilities are available to provide statistical information. The term "report" means the result of a query made by using the Nice Query software tool provided by the Nice Call Focus system. The term "reporting" means the action of using the query tool to obtain a list of conversations, their duration registered during a certain period of time and for the channel number(s) specified. Thus, the query tools allow for searches and processing on the phone number of the Helpdesk operators, the associated channel number (generated by the system and usually associated with the same operator number), the number of calls in specific periods, and call durations.

The phone number of the caller is not traceable from the statistics. It is not recorded by the Nice Call Focus system, hence that information is not available to perform queries.

The query tool can not use the contents of the conversation as a search criterion.

Query utilities of the system will be installed on the Personal Computers of the Helpdesk team leader, those responsible for Support, the Controller and the Delegated Controller. The categories of recipients:

- System administrators: local system administrators, helpdesk team leaders, User Support responsible,

● IDOC, ADMIN/DS (Directorate of Security), OLAF, AUDIT, OMBUDSMAN, DPO, EDPS,
● Reporting: Helpdesk team leader, User Support responsible, Controller and Delegated Controller.
● The EDPS notes that trainees are recipients of the data when a previously recorded conversation is presented to them.

There are no plans to produce transcripts of the recorded dialogues. For training purposes the audio recordings will be used directly.

Information provided to the data subjects:

● *Information page on the DG's Intranet (Privacy statement)* providing information on the system in general; the identity of the controller; a reference to Regulation (EC) 45/2001; the type of personal data being collected; the purposes of the processing operation; the legal basis; technical information about the recording (content and traffic data); access to the information in the system and to whom data can be disclosed; brief description of security measures; procedures to verify, modify and delete personal information; data storage period (6 months); contact information; and recourse to the EDPS ("*Complaints, in case of conflict, can be addressed to the European Data Protection Supervisor").*
● *Broadcast via e-mail to all DG's staff* providing information on the purpose of the system; the procedure itself; the welcome message that every person will hear at the beginning of each conversation (see the text below), a link to the privacy statement and another link to the text of the Regulation.
● Newcomers will receive information as part of the presentations on the IT facilities in the DG made by the Information Resources Manager (IRM) unit.
● A short informational voice message can be heard at the beginning of each call to the DG's IT Helpdesk: *"Welcome to DG INFSO IT Helpdesk. For quality control purposes, this conversation is being registered".*

Each person can obtain a copy of the record of his conversation with the Helpdesk staff in case he/she can be clearly and unambiguously identified through the content. A request can be made by e-mail addressed to the functional mailbox "INFSO HELPDESK." By applying the same procedure, data subjects may ask to verify which personal data is stored by the controller, and can request modification, correction or deleting their data. A specific correction request is submitted via the registration of a new conversation, identifying unambiguously the record to correct.

The storage time will not exceed a maximum of 6 months. It also applies to those recordings where the Helpdesk operator objected to their use for training purposes. Although as the controller noted, it is possible to adjust the system to enable a storage period up to a maximum of 7 years (when automatic deletion would take place), for practical reasons and with the aim to be in compliance with the Regulation the storage period is defined as above. The Helpdesk receives over 20 000 calls a year and the quantity of recordings should guarantee the continuous availability to be used for training purposes.

The time limit to block data on justified legitimate request from the data subjects is four months. According to the controller, the four months offer sufficient guarantee to the users to be able to request blocking data, should they wish to do so. Also holiday periods, sicknesses, missions, and other forms of leaves were taken into regard. This period would enable the controller to intervene before the automatic mechanisms related to the maximum storage time would erase the recordings.

Security measures:

[...]

2.2. Legal aspects

2.2.1. Prior checking

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data applies to the processing of personal data by the European Commission.

The term "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, psychological, mental, economic, cultural or social identity"*(Article 2(a) of the Regulation). Recital (8) of the Regulation stipulates that "*To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person."* The caller's' ID is shown on the phone display, or if they are persons calling outside of the Commission, their identification data (e.g. telephone number) is recorded during the conversation. In any case, the identification of the caller is a necessary element for the purposes of solving their IT problem by the Helpdesk. The voice of the Helpdesk operator makes him identifiable. It is also not excluded that trainees can recognise the voice of their colleagues in the recorded dialogue played to them during the training. In general the physical link between the NCFS input channel number and the phone number allows also for the identification of the Helpdesk operators involved in the conversation. Data contained in calls recorded and or listened to can be attributed to specific individuals (operators or callers), thus Article 2(a) of the Regulation applies.

The processing of personal data is carried out by DG INFSO at the European Commission and is carried out in the exercise of activities which fall within the scope of Community law (Article 3 (1) of the Regulation).

The present case concerns mainly automated processing (Article 3(2) of the Regulation).

Regulation 45/2001 therefore applies.

Article 27 (1) of Regulation (EC) 45/2001 subjects to prior checking by the EDPS all processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. The protection of personal data and privacy in the context of internal telecommunications networks presents a specific problem. Chapter IV of the Regulation contains a specific provision on the confidentiality of communication (Article 36). Since the Voice recording system restricts the confidentiality of communication, it clearly poses specific risk to the rights and freedoms of data subjects, thus it falls under the scope of Article 27(1) of the Regulation.

The notification of the DPO was received on 17 March 2006. According to Article 27(4) the present opinion must be delivered within a period of two months that is no later than the 18 May 2006. The procedure was suspended for 97 + 3 days. The opinion was to be delivered by

28 August 2006 (26 August 2006 being a Saturday). However the complexity of the case required an extension of the deadline. On 28 August 2006, the EDPS extended the deadline to issue the opinion for four more weeks. A new information request suspended the procedure for a period of 13 days. Thus, the opinion should be rendered on 9 October 2006 (8 October 2006 being a Sunday). The last information request to the DPO suspended the procedure for a period of 14 days, thus the opinion must be rendered not later than 23 October 2006.

2.2.2. Lawfulness of the processing

The system of "Voice recording of IT Helpdesk calls" is designed for two major purposes: 1) to ensure a good level of service provide by the Helpdesk by having the recorded conversation available for solving the IT trouble reported; and 2) quality control, which basically means the use of selected recordings on training (hereinafter: "quality control and training").

The examination of the lawfulness of the processing at question requires a joint analysis of the principle of necessity, proportionality and restriction of the confidentiality of communication, because these issues are strongly interrelated.

Personal data may only be processed if it is grounded in Article 5 of the Regulation. The notification refers to Article 5(a) of the Regulation, which lays down that processing is lawful if it "*necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body".* Recital 27 to the Regulation further specifies that "*processing of data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies".* The purpose of the system to verify information when needed for solving the problem is at the very margin of necessity. Although the practical reasons given by the controller to justify recording of each and every call for solving the trouble are understandable, the EDPS stresses that such an extensive recording is at the very limit of being necessary for carrying out the Commission's task in the public interest. Since the first purpose of the system is a borderline case, the proportionality and the issue of confidentiality of communication should be carefully examined (see part 2.2.3). Recording each and every IT Helpdesk call with the aim of having sufficient available samples to be selected for training purposes is beyond the limit that can be "necessary" for carrying out the tasks of the Commission (for remedying the situation, see below).

The requirements as to the legal basis will depend on the processing. The need for legal guarantees provided differs and has to be assessed by taking into account the risks presented by the processing operation. Recording communications and the further use of the recordings requires heightened guarantees because it presents increased risks to the rights and freedoms of individuals.

The prior checking notification states that the processing operations by the Nice Call Focus II System are necessary for the good quality of the performance and support of tasks carried out by the DG, as mandated by Article 6[2] ,7[3], 211-219[4] and 255[5] of the treaties as amended by the

[2] *Article 6. 1. "The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.*
Article 6.2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law."

Treaty of Amsterdam.[6] The Code of good administrative behaviour for staff of the European Commission and their relations with the public (published as an Annex to the Commission decision of 17 October 2000) requires a quality service in these terms: "*The public legitimately expects quality service and an administration that is open, accessible and properly run".*[7] As, said above, processing personal data for solving trouble is just within the acceptable limits of being necessary for providing the service. It is just acceptable on the legal basis of the Code of good administrative behaviour. Because of this delicate situation, further safeguards must be provided, such as a very short data conservation period (see in part 2.2.5).

The use of the recordings beyond the first purpose for quality control and training purposes, oversteps the acceptable limit of necessity (see above). Thus in order to make the processing lawful for training, while having a margin for manoeuvre, the controller should employ either of the following two solutions. A) If personal data are made anonymous no data protection concerns arise. B) Understanding the explanations of the controller that making the data concerned anonymous raises a number of technical difficulties, in order to make the use of recordings lawful for the second purpose, the processing should be grounded in an appropriate legal basis. The consent of the data subjects (callers and operators) for monitoring non-anonymous dialogues for quality control purpose and to use recordings for training could make the processing lawful under Article 5(d) of the Regulation.

Article 2(h) of the Regulation specifies that "*the data subject's consent' shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*. In order to give a real consent the data subject should be aware of the operation of the system in general and certain details of the system (see 2.2.8 part below). It should be also noted that the present case concerns "consent" in the employment context, which as the Working Party 29 highlighted in Point 10 of its 8/2001 Opinion on the processing of personal data in the employment context[8] under Directive 95/46/EC: "*where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse, it is not consent. Consent must all times be freely given. Thus a worker must be able to withdraw consent without prejudice*". The consent requirement under Regulation 45/2001 should be interpreted along the same line.

When individuals call the IT Helpdesk they listen to the welcome message explaining about the registration of the conversation for the first purpose, and when they thereafter share their personal data in the context of their need for IT help, this can be regarded as giving their consent to the processing provided that the information given in the welcome message is more explicit (see part 2.2.8 on Information to the data subjects). As to the consent of callers for the second purpose, the controller can choose between two alternatives: 1) after selecting the dialogues either to obtain the consent of the calling party to use the recording on training (similarly as consent is requested from the operators to use a particular recording on training),

---

[3] Article 7: "*The Council... may determine the existence of a serious and persistent breach by a Member State of principles mentioned in Article 6(1), after inviting the government of the Member State in question to submit its observations."*

[4] On the Commission.

[5] On the right of access to documents of the institutions and its limits.

[6] Treaty of Amsterdam Amending the Treaty on European Union, the Treaties establishing the European Communities and Related Acts. Official Journal C 340, 10 November 1997.

[7] The controller clarified that although there was some discrepancy regarding the legal basis indicated in the prior checking notification form and in the privacy statement, the relevant legal basis is the one in the notification form.

[8] 5062/01/EN/Final. WP 48. Adopted on 13 September 2001.

or 2) at the end of each call to the Helpdesk, the operators could ask the individuals calling whether they agree to the use of the recorded conversation for training purposes. If they do not agree, those records can not be used and should be deleted. Thus their consent or denial is also registered in the recordings and should be respected.

Operators have an "opt-out" possibility from the further use of recordings for training. As planned, they can make a generic request not to use any of the recordings related to their phone number, and upon their explicit written request specific recordings will be excluded from the use of training.

The EDPS recommends for reasons of fairness towards the operators, that once the selection of dialogues planned to be used on training is made within the five working days time limit (from the date of the recording) the operator should not only receive the identification data of the recording that is planned to be used, but also operators should have the opportunity to listen to the dialogue selected including their voice and personal data. Only in that case can the consent of the operator recognised as "specific" and "informed".

A freely given consent also involves the withdrawal of that consent, thus data subjects should be able to request not to use the selected recording any further.

2.2.3. Confidentiality of communications

According to Article 36 of the Regulation the "*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".*

The principle of confidentiality of communications can be read in two ways: the Community institutions must ensure the confidentiality of communications from any interference coming from the outside, but also respect the confidentiality of communications themselves. The first is linked to the security of the network (see 2.2.9 below).

From the outset above, it must be pointed out that the principle of confidentiality of communications was inspired by Article 5 of Directive 97/66[9] which notably provides that Member states must prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised in accordance with the general principles of Community law. Directive 97/66 has since been replaced by Directive (EC) 2002/58[10], but the principle remains the same: providing the parties to the communication have given their consent, there is no breach of the principle of confidentiality of communications (Article 5 of Directive (EC) 2002/58). The EDPS believes that Article 36 of Regulation 45/2001 must be interpreted along those same lines.

According to Article 36, any restriction to the principle must be in accordance with the "general principles of Community law". The concept of "general principles of Community

[9] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and telecommunications).

law" refers to the notion of fundamental human rights notably as laid down in the European Convention on Human Rights. Article 8 of the ECHR stipulates the right to respect for private and family life, and Article 8(2) provides for a test, where the right can be restricted. Thus, any restriction must be "in accordance with the law" and "necessary in a democratic society" in the interests of national security, public safety, for the prevention of disorder or crime, for the protection of morals or for the protection of rights and freedoms of others. The test of "necessary in a democratic society" includes the principle of "proportionality".

The data protection principles that the processing should be "necessary" for the purpose and "proportionate" to the aim pursued should thus be respected in the present case.

The EDPS considers that non-selective recording of Helpdesk calls for the defined purposes should be permitted only in very limited cases, where appropriate safeguards exist.

The first purpose of the system is to verify the information reported in order to solve the IT trouble. Since the operator's work consists of summarising and clarifying the problem reported and assisting the work of the specialist support group by this, the possibility to listen again to the conversation with the user/client can be helpful in clarifying details in cases when the "trouble ticket" is passed to other specialist support groups to solve the problem that was reported. This is also important in a working environment where non-native languages are used, which may lead to certain degree of imprecision. Thus, the EDPS considers that for the purpose of carrying out the task of the DG to solve the problem reported, non-selective recording can be necessary for practical reasons but only with appropriate safeguards and for a very short data conservation period (see above part 2.2.2. "Lawfulness of processing" and below in part 2.2.5 "Conservation of data").

The recording of each and every call for the purpose of having a sufficient number of calls available for selecting samples of "good practices" and "common mistakes" however is disproportionate to the aims pursued. The EDPS does not agree with the argument of the controller, that recording systems are becoming more commonplace and the response of the market to the need of the call centres would justify blanket recordings and the further use of those records. Blanket recording of Helpdesk calls with the aim of having sufficient examples available for selecting for training is an excessive data collection (see below in part 2.2.4 "Data Quality").

The EDPS recommends that the controller considers other less intrusive means to achieve the goal of having samples for training and improving efficiency of managing time and courteous gathering of information by the operators. For example, for the trainings, simulated good and less appropriate communication practices based upon the experiences of the operators could be used. Alternatively the newcomers could sit behind the Helpdesk and follow the operator's work closely.

2.2.4. Data Quality

Data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed (Article 4(1)(c) of the Regulation). This requirement echoes the principle of proportionality according to which only the necessary data for the specific purpose for which they were collected may be used. A sufficient link must exist between the purpose and the data processed. The system under examination has two main purposes: verification of information for trouble solving and quality control and training. Whether the data collected are adequate, relevant and not excessive for the two different purposes must be examined separately.

The system records the conversation between the Helpdesk operator and the caller in order to have precise information available as to the nature of the trouble reported and to facilitate the work of the specialist support group. The system further processes identification details of the recordings (precise date and time along with the Helpdesk system call number and associated helpdesk operator phone extension). After selecting the samples from the database, recorded conversations are played during training courses.

As to the problem solving purpose of the system, the EDPS concludes that the recording of the accurate and precise content of the conversation meets the data quality requirement in the Regulation. However the collection of personal data by recording each and every dialogue between Helpdesk operators and callers for the quality control and training purpose is far too excessive.

The Article 29 Data Protection Working Party outlined the meaning of the principle of proportionality in its working document "on the surveillance of electronic communications in the workplace"[11]:*"the proportionality principle...rules out blanket monitoring..."*, and *where the objective identified can be achieved in a less intrusive way the employer should consider this option (for example, he/she should avoid systems that monitor automatically and continuously)".* Also, the Article 29 Working Party stressed, that: *"Systems for the processing of electronic communications should be designed to limit the amount of personal data processed to a strict minimum".*[12] Although these principles were laid down in relation to Directive 95/46/EC and concerned blanket monitoring of individual emails and Internet use of all staff, the EDPS considers that they apply in the present context.

The blanket monitoring of Helpdesk calls by the system for the second purpose does not limit the collection of personal data to a strict minimum, because it aims to compile a vast amount of potential samples, which include personal data. Thus, it breaches the data quality requirement of the Regulation. (In order to comply with the Regulation see, below the "Conservation of data" part on anonymity).

As to the use of selected recordings for training purposes, the EDPS does not agree with the position of the controller that the removal of some parts of the conversation may decrease intelligibility of the content and this would go against the first purpose of the system. Once the IT problem reported to the Helpdesk is solved, in principle, the recordings should be deleted within a very short time limit (see in "Conservation of data" part). Within this short period, samples may be selected for training. The controller has a margin of manoeuvre to decide A) whether to make recordings anonymous, meaning that the data subjects are no longer identifiable, in which case the data protection principles do not apply, or B) whether after obtaining the consent of the data subjects, use the recordings on training courses. In this case personal data unnecessary for the training purpose should be erased from the dialogue played on the training.

Furthermore the data must be accurate and kept up to date (Article 4(1)(d) of the Regulation). The direct recording of communications ensures the accuracy of the data contained in the audio recordings. The accuracy of the data is also guaranteed by granting the right of rectification of the data subjects (see below in part 2.2.7 Right of access and rectification).

[11] 5401/01/EN/Final WP 55. Adopted on 29 May 2002.

[12] Although the content of the proportionality principle was elaborated as to the surveillance and monitoring of electronic communications in the work place under Directive 95/46/EC, the EDPS considers that the concept applies to the present case, too.

2.2.5 Conservation of data and blocking of data

"Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. The Community institution...shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes" (Article 4(1)(e) of the Regulation).

Content data are recorded by the system. The EDPS notes that in order to comply with Article 4(1)(e) of the Regulation, it is necessary to keep the dialogues only until an IT problem reported by the user is resolved. Once the requested IT help was provided, recordings should be erased as soon as possible, meaning a short conservation period, a maximum of five working days.

If the controller decides to use the recordings beyond the purpose of solving IT problem for the second purpose of quality control and training, the controller should choose whether to render personal data anonymous or whether to keep them in a non-anonymous form (with the safeguards laid down in the present opinion). Selecting the recordings and making them anonymous can be done solely in the short data conservation period defined for the first purpose of the system (in maximum five working days).

As to the first variant: Rendering the recordings anonymous both as to the callers and the operators is a fundamental requirement under Article 4(1)(e) of the Regulation. This is also a guarantee under Article 4(1)(b) of the Regulation which requires that the controller should provide appropriate safeguards, in particular ensuring that the data are not used in support of measures or decisions regarding any particular individuals. Anonymity is especially important in the context of training, where without making the voice of the operators unidentifiable on the recordings presented as samples, trainees may recognise the voice of their colleagues and form subjective judgement regarding their competences, efficiency and professional conduct.

Storing the data for a period of 6 months with the aim of having sufficient dialogues available for training as foreseen by the controller violates Article 4(1)(e) of the Regulation.

Keeping data in a non-anonymous form beyond the maximum five working days time limit (which allows selection to take place) for the purposes of using the dialogues for training, requires the consent of the data subjects (see part 2.2.2 Lawfulness of the processing).

As stated above in the section describing the facts, the use of two parallel systems makes possible the identification of the conversations between operators and customers. The Nice Call Focus system records the conversations, and parallel an incident ticketing system called Peregrine is employed. When a user calls, the incident is reported in this system and it is either resolved or dispatched to other support groups. The information kept in Peregrine is the timestamp and operator. This information can be matched to the information provided by the Nice Call Focus system to allow the identification of the conversations between operators and customers. The channel number (which is linked to the operator's phone) and the time stamp are the only available information when queries are made to obtain a list of conversations with their duration registered during a certain period of time and for the channel number(s) specified. Those identification details make it possible to identify the call itself, just as the caller and the operator.

For the first purpose of the system, it is essential to identify the call, and if necessary by tracing back and by verifying the information, to use the content of the dialogue for solving the IT problem reported. The same short data conservation period applies to the identification details of the calls themselves. Those should not be kept any further than a maximum of five working days. In this period, as stated before, the identification details can be used to select the dialogues for training purpose and obtain the consent of both the callers and operators for the secondary use of the recordings. Once it is done, those elements which could result in identification of the data subjects, should be made anonymous or erased (e.g. channel number associated to the phone of the operator).

Article 15 of the Regulation provides for the data subject the right to obtain from the controller the blocking of data in specified cases. As is it planned by the controller, the time limit to block data based on a justified legitimate request from the data subjects is defined as four months in order to have sufficient guarantee for the users to be able to request blocking data, should they wish to do so. Also holiday periods, sicknesses, missions, and other forms of leaves were taken into regard. This period would enable the controller to intervene before the automatic mechanisms related to the maximum storage time (6 months) would erase the recordings.

A request to block personal data can occur only in those cases where the data are kept in a form where the data subject is identifiable (i.e. the maximum five working days long data conservation period or if the recordings are selected and used on training in a non-anonymous form). Instead of establishing a uniform 4 months blocking period, the EDPS recommends that the blocking period should correspond to the specific reason (as given in Article 15 of the Regulation) of making the request: keeping proof, unlawful processing (e.g. when the operator did not consent to the use of recording for training and demands blocking instead of erasing the data), etc.

2.2.6 Transfer of data

Personal data shall 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 recipients. The recipients shall process the personal data only for the purposes for which they were transmitted (Article 7 (1) and (3) of the Regulation).

Personal data included and related to the recordings are transferred to local system administrators, the Helpdesk team leader, the User Support responsible, Controller and Delegated Controller, and to trainees. The system should ensure that only those people receive the personal data contained in the recording or related to them for whom it is *necessary* for the performance of their task. It should be clearly defined and a distinction should be made as to who can be a recipient of personal data for the problem solving purpose of the system, and who can receive personal data (if dialogues are not made anonymous) for the purpose of quality control and training (see also above in part 2.2.5).

The prior checking notification also mentions that data can be transferred to IDOC[13], ADMIN/DS (Directorate of Security), OLAF[14], AUDIT[15], OMBUDSMAN, DPO and EDPS.

[13] See Opinion of 20 April 2005 on the notification for prior checking relating to internal administrative inquiries and disciplinary procedures within the European Commission (Case 2004-187). Available at: www.edps.europa.eu.

[14] See Opinion of 23 June 2006 on a notification for prior checking on OLAF internal investigations (Case 2005-418)

[15] The EDPS presently prior checks the "Internal Audit Process". Case: 2006-298.

Those transfers can take place as they are "necessary for the legitimate performance of tasks covered by the competence of the recipient", who establishes the need in the context of the investigation.

2.2.7 Right of access and rectification

Article 13 of the Regulation specifies that "*the data subjects have the right to obtain without constraint, at any time within three months from the receipt of the request and free of charge from the controller: (a) a confirmation as to whether or not data related to him or her are being processed; (b) information at least as to the purposes of the processing operation, the categories of data concerned; and the recipients or categories of recipients to whom data are disclosed; communication in an intelligible form of the data undergoing processing and of any available information as to their source...".*

Data subjects should be able to exercise their rights, wherever data are identifiable.

Article 14 provides for the right to rectify personal data in these terms: "*The data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data".* To the extent that rectification can occur in a voice recording system, which precisely records the information at question, data subjects should be enabled to exercise this right. By sending an explicit e-mail to the functional mailbox of the INFSO Helpdesk data subjects can ask to delete, modify/correct their personal data. In the present system a correction request is registered through the recording of a new conversation, identifying unambiguously the record to be corrected. Although this is not a user - friendly solution, it may be an appropriate procedure, provided that there are clear rules set for the storage of the second conversation requesting the correction of the previous dialogue, i.e. it should not be kept for longer than the original record which was corrected.

The system allows each person who is unambiguously identified through the content to obtain a copy of the record of his/her conversation with the DG INFSO IT Helpdesk by sending an e-mail request to the functional mailbox. By the same procedure data subjects can verify which of their personal data are stored by the responsible controller. The EDPS finds this procedure appropriate, and also stresses that the right to access their personal data, including obtain a copy of the dialogue should also be granted to the IT Helpdesk operators. They should be informed of the procedure on how to access their personal data.

2.2.8 Information to the data subject

The Regulation provides that personal data must be processed "fairly and lawfully" (Article 4(1)(a)). Fair processing implies that it can not take place covertly. In practice, this principle is implemented by the obligation to give certain information to the data subject in accordance with Articles 11 and 12. Article 11 of the Regulation lists a set of information that the controller should provide to the data subjects where data have been obtained directly from them. Article 12 of the Regulation lays down the information that is to be supplied where the data have not been obtained from the data subject.

In the present case data are obtained from the data subjects themselves. In the various documents and information sources the controller provides the information required by Article 11 of the Regulation. The EDPS welcomes that in addition to the general requirements of Article 11, the controller provides information also on the legal basis, the time-limits to storing data and the right to have recourse to the EDPS. This is necessary for reasons of fairness towards the data subject due to the more delicate nature of the processing operations.

The EDPS however request three corrections: 1) The storage period should be corrected in the privacy statement in line with the present opinion. 2) The sentence on the right to recourse to the EDPS should be harmonised with that of Article 11 of the Regulation. It should be specifically mentioned that "at any time" the data subjects can recourse to the EDPS. 3) The Privacy Statement mentions in the identification data part that "*Other information that might be recorded within the contents of a conversation is a.o. your first name, name, title, organisational unit, fax number, e-mail, address. However such data will never be subject to any processing and will be used only for the purpose of the quality control of the operation and improvement of the performance of DG INFSO's IT Helpdesk*". The statement should be corrected by making it obvious to data subjects that the system processes their personal data for the verification of information for solving the problem, and if data are not made anonymous also for the quality control and training purpose.

If personal data are not made anonymous for the quality control and training purpose, in order to guarantee fair processing in respect of the data subjects their consent should be required to the processing. Providing more accurate and specific information in the welcome voice message played before each and every call is a pre-requisite for an informed consent. The system as planned would play this welcome message: "*"Welcome to DG INFSO IT Helpdesk. For quality control purposes, this conversation is being registered".* In order to provide more accurate information as to what is covered by the "quality control purpose", it should be explained in the welcome message that: "*Welcome to DG INFSO IT Helpdesk. This conversation is being registered to make sure that we have the accurate details of your problem reported. The information will be deleted when the problem is resolved, no later than five working days from recording."*

Had the controller decided not to make the recordings anonymous, at the end of each recording, the operators could ask: "Do you agree to this recording being used for training purposes?" (see also above in part 2.2.2). If the controller finds this solution difficult, he can ask for the consent of the person calling by other means (e.g. calling back the person for his/her consent). In any case, data subjects should be informed about the possibility of requesting their consent, and also of the details of the system to which they consent.

Helpdesk operators should receive accurate information that they have a possibility to object in a generic form to the use of recordings and also to the use of the particular recording of their dialogues. They should be also informed about the details of the procedure in which they can exercise that right.

2.2.9 Security measures

After careful analysis by the EDPS of the security measures adopted, the EDPS considers that these measures are adequate in the light of Articles 22 and 35 of Regulation (EC) 45/2001.

Conclusion:

Some elements of the processing operation breach the principle of necessity and proportionality, and violate the data quality and data storage provisions of Regulation (EC) No 45/2001. In order to comply with the Regulation the EDPS recommends the above considerations to be taken into account, in particular:

- Recorded dialogues can be used on training either by making personal data anonymous or by obtaining the consent of the callers and the operators.

- Data subjects should be aware of the operation of the system in general and certain details of the system before consenting to the processing.

- -The welcome message should provide more explicit information on the quality control purpose and the short storage period.

- The controller should consider whether less intrusive means could be employed for the training purpose.

- -Personal data unnecessary for the training purpose should be erased.

- Once the requested IT help has been provided, recordings and identification details of the recordings should be erased as soon as possible, meaning a short conservation period, a maximum period of five working days.

- Selecting the recordings for training purpose can be done only while data are kept in the system for the first purpose (maximum five working days).

- Keeping data in a non-anonymous form beyond the maximum five working days time limit for training purposes requires the consent of the data subjects.

- -The blocking period should correspond to the specific reason of making a blocking request.

- It should be clearly defined and a distinction should be made as to who can be recipient of personal data for the verifying information recorded in order to solve the problem, and who can receive personal data (if dialogues are not made anonymous) for the purpose of quality control and training.

- If rectification of information takes place by mean of a new recording, the storage period for the new recording should not exceed the storage period of the original recording that was being corrected.

- The right of accessing data should be granted to the operators.

- The information in the Privacy Statement should be corrected.

- Helpdesk operators should receive accurate information that they have a possibility to object in a generic form to the use of recordings and also to the use of the particular recording of their dialogues. They should be also informed about the details of the procedure in which they can exercise that right.

Done at Brussels, 23 October 2006.

Peter HUSTINX
European Data Protection Supervisor