



## **Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Ombudsman on verification of telephone bills**

Brussels, 14 May 2007 (Case 2007-137)

### **1. Proceedings**

On 1 March 2007 the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Ombudsman a notification for prior checking related to the verification of telephone bills. The DPO enclosed with the notification several documents including additional details on the processing. The EDPS requested further information on 20 March 2007 and the DPO answered on the same day. The procedure was suspended anew on 27 April 2007 asking for further details on the processing. The DPO answered on 2 May 2007.

### **2. Examination of the matter**

#### **2.1. The facts**

The telephone sets used by the officials and trainees (hereinafter: staff members) of the European Ombudsman (hereinafter: the Ombudsman) may only be used for professional purposes. Use for private purposes is not permitted. The European Ombudsman's office uses the European Parliament's telephone equipment. Nevertheless, the analysis of the European Parliament's traffic and billing data management is not the subject of the present opinion. The current scrutiny focuses on the processing carried out by the Ombudsman.

The European Parliament invoices to the Ombudsman all costs linked to telephone use in extension number/name/monthly breakdown indicating the number of local, national or international calls related to each line. This information is sent in an Excel file every month to the Head of the Administration Sector of the Administration and Finance Department. Invoices are sent on a quarterly basis. Should the cost related to a certain extension number (except the Ombudsman's cabinet where this limit does not apply) exceed the 50€ ceiling, an improper use is suspected. The improper use shall be detected by the Head of Administration Sector on the basis of the data received from the Parliament (Excel file). The Head of Administration and Finance Department shall be informed in this case.

To dial external numbers, staff members can either dial them directly (if the number is placed in a certain area of France, Belgium and Luxembourg) or through the Parliament's switchboard. Certain staff members including the legal officers have a personal code for external calls. When using this code, there is no need to contact the switchboard. The

possibility to make calls by declaring the identity of the staff member to the switchboard is not yet available but negotiations are underway in order to make it operational.

The Head of the Administration and Finance Department, if the exceeding amount makes it necessary, shall initiate a consultation with the official concerned who is identified via his/her extension number. Callers' identities may also be established through the personal codes used. The staff member concerned can make any comments and add any information. The consultation is successful and the verification procedure comes to an end if the staff member provides a reasonable and work-related explanation regarding the costs or he/she admits that the excessive bill is a consequence of use of the telephone system not related to work. In the latter case the official is reminded that the telephone system of the Ombudsman shall be used only for professional purposes and the costs not related to professional telephone conversations will be deducted from his/her salary.

If the origin of excessive costs cannot be clarified in the frame of this meeting, detailed verification is needed. The Head of Administration Sector shall in this case, with the prior consent of the staff member concerned, ask for the detailed data on the calls made from the telephone set used by the staff member. These data will be analysed in a meeting attended by the Head of Administration Sector and by the staff member concerned on the basis of several aspects, like the type of the number called, location, repetitive character of calls, duration of conversations etc. The staff member concerned is invited to provide explanations on the numbers dialled which do not seem to be connected to work. If, according to the assessment of the Head of Administration and Finance Department and the Head of the Administration Sector the explanations are not satisfying, the staff member will be warned that such behaviour shall be avoided in the future or disciplinary procedure may be initiated. In assessing the abuse of the telephone system, the Head of Department and Section are not instructed with special guidelines. The main rule which has to be taken into consideration is that the telephone system may not be used for private purposes.

The purpose of the processing is to verify the proper use of the telephone with special attention to instances when the 50€ limit has been surpassed by a staff member. The verification procedure implies the assessment of the staff member concerned. The data may also be used for statistical purposes but only in anonymous form. Data related to the telephone use are kept for the actual calendar year. Should the verification procedure result in a disciplinary procedure, billing data are used and retained for this purpose. Data subjects are officials and trainees of the European Ombudsman. In the framework of the processing at issue the name, monthly costs of telephone use and eventually detailed data on the calls (number dialled, country called, date and time of call, duration of call, cost of call) are processed. Staff members were informed in 2005 in an e-mail sent by the Head of the Administration and Finance Department on the policy to be followed regarding telephone use and that improper (i.e. private) use may lead to a 'call to order'. In addition, it was also indicated that data related to the use of the telephone system are kept by the Administration and Financial Department for budgetary and verification purposes. This information is also communicated to all new recruits.

Data processed in the framework of the verification procedure may be forwarded to the Head of the Administration and Finance Department, to his/her superior and to staff members in charge of carrying out disciplinary procedures. The European Ombudsman is declared to be the controller. The Administration Section of the Administration and Finance Department is in charge of carrying out the processing operations. The Head of this Section keeps the data in electronic form on a password protected PC.

## **2.2. Legal aspects**

### **2.2.1. Prior checking**

The notification reveals that there is a processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2(a) of Regulation (EC) No 45/2001 ("the Regulation"). The processing implies collection, storage, consultation, use and transfer of personal data which qualifies the operation as processing of personal data (Article 2(b) of the Regulation). The processing operation is carried out by a Community institution, in the exercise of activities which fall under the scope of Community law (Article 3(1)).

The processing of personal data is carried out by automatic means. Thus Article 3(2) applies in this case.

Article 27(1) of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*".

The processing of traffic and billing data in the context of an internal telecommunications network presents specific issues which are specifically addressed in Chapter IV of the Regulation. Article 37 provides for further specifications on the processing.

Since the assessment of a staff member's conduct regarding the use of the telecommunications system may have consequences for the data subject, Article 27(2) applies. This Article contains a list of processing operations that are likely to present risks as stipulated in Article 27(1), among others the "*processing operation intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*" (Article 27(2)(b)). Thus the processing has to be prior checked by the EDPS.

Since prior checking aims at addressing situations that are likely to present certain risks, the opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operation has already been established. This is not a serious problem since any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 1 March 2007. According to Article 27(4) of the Regulation, the present opinion must be delivered within a period of two months following the receipt of the notification. The two months period was suspended for 6 days for requesting further information and for 5 days to allow comments from the DPO, altogether for 11 days. Thus the present opinion must be delivered by 14 May 2007 (13 May 2007 being a Sunday).

### **2.2.2. Lawfulness of the processing**

Examining the lawfulness of the processing, two purposes have been identified. First, the purpose of telecommunications traffic and budget management and second, the verification of the use of the telecommunications system.

Article 5(a) of the Regulation stipulates that personal data may be processed if "*the 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 or in the legitimate exercise of official authority vested in the Community institution or body.*" The telecommunications traffic and budget management and the verification procedure fall within the scope of the legitimate exercise of official authority

vested in the institution. Thus the lawfulness of the processing is respected. Furthermore, the EDPS considers that recital 27 of the Regulation must be also taken into consideration according to which "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*".

The EDPS considers that the processing is lawful under the above provision and recital.

Further to the lawfulness of the processing the EDPS notes that the consent of the data subject deserves special attention in the context of verification. According to the current policy of the European Ombudsman, detailed data on the calls made will only be requested from the Parliament if the staff member concerned has given his/her consent. It has to be noted that in accordance with Article 37(2) of the Regulation, traffic and billing data can be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications system without the prior consent of the data subject; in other words, the legal basis of the processing can be found in Article 37(2) of the Regulation. The EDPS, however, notes that since the verification procedure may lead to further consequences, including disciplinary procedures, it would be desirable that the Ombudsman draws up specific rules on the verification procedure. These rules themselves would constitute a more concrete legal basis for the processing.

As to the consent, 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 shall be aware of the operation of the system in general and certain details of the system, including the consequences of not giving his/her consent (see point 2.2.7. 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<sup>1</sup> 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 at 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, which means that also the consequences of the lack of consent should be foreseen and staff members should be informed of them.

### **2.2.3. Data Quality**

"*Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*" (Article 4(1)(c) of the Regulation).

In the framework of the verification procedure personal data are processed in order to monitor the proper use of the telephone system and verify the bills if the 50€ limit has been surpassed by a staff member. The verification procedure implies the assessment of the concerned staff member's conduct.

During the processing at issue data related to the use of the communications system (name, monthly costs of telephone use and eventually detailed data on the calls) and the assessment

---

<sup>1</sup> 5062/01/EN/Final. WP 48. Adopted on 13 September 2001.

of the staff member's conduct are processed. The EDPS is of the opinion that the procedure as designed complies with the criteria set out in Article 4(1)(c).

The Regulation also provides that "*personal data must be accurate and, where necessary, kept up to date*" (Article 4(1)(d)). As mentioned above, the analysis of the European Parliament's traffic and billing data management is not the subject of the present opinion and focuses on the processing carried out by the Ombudsman.

As to the data produced during the assessment of the staff member's conduct, the EDPS welcomes the fact that the staff member concerned is directly involved in the verification procedure which guarantees that the data subject may make any comments and add any information of relevance. This contributes to the accuracy of data processed.

The data must also be "*processed fairly and lawfully*" (Article 4(1)(a) of the Regulation). The lawfulness of the processing has already been discussed (see point 2.2.2.). As regards fairness, this relates to information given to the data subject (see point 2.2.7.).

#### **2.2.4. Conservation of data**

The Regulation states that 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*" (Article 4(1)(e)).

Traffic data which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection (Article 37(1)). The principle is therefore of erasure of the data as soon as they are no longer necessary for the establishment of the call or connection.

Article 37(2) provides for that traffic data, as indicated in a list agreed by the EDPS, may be processed for the purpose of budget and traffic management, including the verification of authorised use of the telecommunications systems. However, they must be erased or made anonymous as soon as possible and in any case no longer than six months after collection, unless they need to be kept for a longer period to establish, exercise or defend a right in a legal claim pending before a court. This provision therefore recognises that traffic and billing data may be kept and processed for the purposes of traffic and billing management including the verification of the authorised use, for up to six months. If the period of six months lapses without the institution of proceedings, the traffic data must be erased or rendered anonymous. If proceedings have been commenced within that period, then such proceedings will interrupt the prescriptive period until the end of the proceedings and further until the end of the prescriptive period allowed for any appeal or the conclusion of the appeal proceedings as the case may be.

In the frame of the present case, no specific retention period has been set up. The EDPS recommends that a retention period will be set up which ensures that traffic and billing data are not kept for longer than a period of six months.

Article 20 of the Regulation also provides that the application of Article 37(1) may be restricted where such a restriction constitutes a necessary measure notably to safeguard the prevention, investigation, detection and prosecution of criminal offences; an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; the protection of the data subject or of the rights and freedoms of others. This provision therefore allows the conservation of traffic and billing

data for other purposes than traffic and billing management in certain limited cases. The EDPS has interpreted Article 20 in the light of the *ratio legis*, and notably also allows for exceptions to the strict conservation periods in the frame of disciplinary investigations. The data may therefore be kept for longer than these 6 months on the basis of Article 20 of the Regulation in the frame of a disciplinary investigation. This is not, however, the object of the present prior check.

The principle as concerns conservation of traffic and billing data is therefore of immediate erasure or conservation for a period of six months at the latest for billing and traffic management unless:

- there is a pending legal claim involving such data;
- a disciplinary investigation justifies the conservation of such data under Article 20;
- the data are kept in an anonymous form for statistical purposes.

Traffic and billing data are kept for statistical purposes only in anonymous form. Thus Article 4(1)(e) is respected.

### **2.2.5. Transfer of data**

Article 7(1) of the Regulation provides that "*personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient*".

Data processed in the framework of telecommunications budget and traffic management and verification of authorised use of the telecommunications system may only be forwarded to the Head of the Administration and Finance Department, to his/her superior and to staff members in charge of carrying out disciplinary procedures. The EDPS finds that these transfers are necessary for the legitimate performance of the tasks of the recipients.

The processing may also involve data transfer to the European Union Civil Service Tribunal. Such transfer of personal data is necessary for the legitimate performance of the task of the Civil Service Tribunal and covered by its competence. Article 7(1) is therefore respected.

### **2.2.6. Right of access and rectification**

Article 13 of the Regulation establishes a right of access and the arrangements for exercising it upon request by the data subject. Under Article 14 of the Regulation the data subject has the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data.

Staff members are fully involved in the verification procedure and are given full access to the data under scrutiny. Moreover, detailed data may only be requested from the Parliament if the data subject (staff member concerned) gives his/her consent to do so. However, there are no specific rules on the data subjects' right of rectification of any inaccurate or incomplete personal data, if it is justified. The EDPS would like to see guarantees to be established in order to ensure that the right of rectification can be exercised by staff members during the verification procedure.

By the same token, the EDPS calls the controller's attention to the fact that in the context of verifying data related to calls other persons than the staff member concerned may be involved

(e.g. called persons). The right of access of any person implied in the verification should also be taken into account.

Furthermore, it has to be mentioned that data subjects have the right of access and of rectification concerning data processed by the Parliament. The verification procedure is without prejudice to the rights of staff members as data subjects *vis-à-vis* the European Parliament.

### **2.2.7. Information to the data subject**

The Regulation states that data subjects must be informed of the processing of data relating to him/her and lists a range of compulsory items of information which must be provided (identity of the controller, categories of data concerned, purposes of processing, recipients, whether replies to the questions are obligatory or voluntary, origin of the data, right of access). Insofar as such information is necessary to guarantee the fair processing, additional information has to be supplied regarding the legal basis, time-limits and the right to have recourse at any time to the EDPS. In the present case, data are stemming from two sources during the verification procedure: the European Parliament provides data on the costs of the calls made and more detailed data on the calls, if necessary; data are also received from the data subject who is invited to justify the high consumption and to give further details on the calls. Since data are obtained both from the data subjects and from another origin, both Articles 11 and 12 of the Regulation apply in this instance.

Staff members are instructed not to use the telephone system for private purposes and they are aware of the fact that the abuse of the system may lead to a 'call to order'. It is also indicated that data related to the use of the telephone system are kept by the Administration and Financial Department for 'budgetary and control purposes'. The EDPS finds this information insufficient and therefore recommends that data subjects receive all particulars on the processing, possibly in a single, easily available document. This document should include, further to the details above, at least the following information: the exact categories of data concerned (being processed with or without the consent of the data subject); the recipients of the data; the fact that detailed data on the calls made will only be requested from the Parliament if the data subject consents to it and the consequences of not giving his/her consent for verification; the existence of the right of access to, and the right to rectify the data concerning the data subject; the legal basis of the processing operation; the time limits for storing the data; the right to have recourse at any time to the European Data Protection Supervisor. Furthermore, data subjects shall be informed on the consecutive steps of the verification procedure and on the possible consequences of it, including disciplinary procedures.

In addition, it must be taken into consideration that the European Parliament's relevant services process traffic and billing data related to Ombudsman's staff members. Consequently the EDPS recommends that information on the Parliament's processing concerning telecommunications budget and traffic management is kept up to date and it is made sure that this information is also available to all, including new staff members of the Ombudsman.

### **2.2.8. 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 Article 22 of Regulation (EC) 45/2001.

## **Conclusion:**

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations are fully taken into account:

- The Ombudsman should draw up specific rules on the verification procedure. These rules would constitute a more concrete legal basis for the processing;
- A data retention period shall be set up which ensures that traffic and billing data are not kept for longer than a period of six months;
- The EDPS would like to see guarantees established in order to ensure that the right of rectification can be exercised by staff members during the verification procedure if it is needed and this right shall be ensured if other persons are concerned in the verification procedure;
- Data subjects shall receive all particulars on the processing, possibly in a single, easily available document. This document should include, further to the details above, at least the following information: the exact categories of data concerned (being processed with and without the consent of the data subject); the recipients of the data; the fact that detailed data on the calls made will only be required from the Parliament if the data subject consents to it and the consequences of not giving his/her consent for verification; the existence of the right of access to, and the right to rectify, the data concerning the data subject; the legal basis of the processing operation; the time limits for storing the data; the right to have recourse at any time to the European Data Protection Supervisor. Furthermore, data subjects shall be informed on the consecutive steps of the verification procedure and on the possible consequences of it, including disciplinary procedures;
- Information on the Parliament's processing concerning telecommunications budget and traffic management shall be kept up to date and it has to be made sure that this information is also available to all, including new staff members of the Ombudsman.

Done at Brussels, 14 May 2007

Joaquín BAYO DELGADO  
Assistant European Data Protection Supervisor