

Opinion on a notification for prior checking received from the Data Protection Officer of the European Central Bank on Investigation procedures regarding the use of office telephones

Brussels, 13 February 2007 (Case 2004-271)

1. Proceedings

- 1.1. On 20 July 2004, the European Data Protection Supervisor (EDPS) sent a letter to all Data Protection Officers (DPOs) asking them to make an inventory of the cases likely to be subject to prior checking by the EDPS as provided for by article 27 of Regulation (EC) 45/2001. The EDPS requested communication of all processing operations subject to prior checking, even those that started before the appointment of the EDPS and for which the Article 27 check could never be prior, but which had to be dealt with on an "ex-post" basis.
- 1.2. On 15 September 2004, the DPO of the European Central Bank (ECB) listed the case of investigations procedures regarding the use of telephones as a case for ex-post prior checking.
- 1.3. On 1 December 2005, the EDPS received the notification of the case for prior checking. The period of two months within which the EDPS must render his prior check opinion was however not initiated as the EDPS paper on e-monitoring which is meant to provide recommendations on the application of the data protection rules to the collection and monitoring of data related to the use of the communications network within EU institutions and bodies had yet to be issued. In Spring 2006, a draft paper was discussed with DPOs.
- 1.4. On 12 June 2006, the EDPS re-launched the prior checking procedure and the two month period within which to render his opinion.
- 1.5. On 14 June 2006, the EDPS raised a number of questions to the ECB concerning the processing operation. These questions were answered to on 13 July 2006.
- 1.6. On 25 July 2006, the EDPS suspended the case, awaiting notification of the modified version of the Administrative Circular 04/2000 on the use of the ECB's telephone and fax equipment.
- 1.7. On 21 December 2006, EDPS decided to lift the suspension on the basis of information received from the DPO according to which the modification of the Administrative Circular 04/2000 on the use of the ECB's telephone and fax equipment would not be adopted before March 2007.

1.8. On 26 January 2007, the EDPS suspended the prior checking procedure for a period of 7 days to allow the DPO to comment on the draft and to provide further information if necessary.

1.9. On 2 February 2007, the EDPS received the comments of the DPO.

2. Examination of the matter

2.1. The facts

The present rules of the ECB as concerns the use of the telephone and fax equipment are provided for in an administrative circular (AC 4/2000). This circular provides for different procedures according to whether the calls are made for business purposes or for personal purposes. The AC 4/2000 and the relevant attachments are published on the ECB's intranet site. Additionally staff members are informed in specifically organised "induction seminars" about the most important provisions concerning the professional duties, including the rules for the private and official use of the phones. Data subjects are to contact the controller for additional information concerning the processing of their personal data in the frame of this procedure.

Staff may make business calls according to appropriate levels of access granted to accommodate the business requirements of the respective member of staff in accordance with his/her function and job tasks. For example, only Director Generals, Deputy Director Generals, Directors and their secretaries have world-wide access. Where business requirements make it necessary for a member of staff to have an access level higher than that which would normally be assigned to him/her, a specific request must be made.

On a monthly basis, budget centre managers will receive two lists of business calls made from extension numbers in their area of competence for their information. The first list contains the extension names, extension numbers, the number of calls made from each extension, the duration and the total charge. The second list contains the extension name, extension number and the percentage of calls made within the city, national or international.

The budget centre managers will carry out, in a manner which can be audited, a plausibility check in order to identify and track potential irregularities.

Personal calls are defined as "any telephone calls made either by the member of staff or on his/her behalf which are not related to the performance of his/her duties at the ECB". Members of staff may make personal calls during business hours as long as the number and duration of these calls are reasonable and made in accordance with the rules laid down in the Administrative Circular.

As a general rule, all members of staff are obliged to declare personal calls. They do so by a system of call charging facility (CCF), introducing a PIN code. In case a member of staff has forgotten to enter the PIN for a personal call, he/she should address himself/herself to the switchboard where a facility exists to make cash payment. When signing the receipt of the PIN code, members of staff authorise charges related to the use of this PIN code to be automatically deduced from the member of staff's monthly salary. Once a month each member of staff will receive an itemised list of personal calls he /she has made the month before. These bills mention the date of the call, the time, the extension used, the first few digits of the number dialled, the duration of the call and the cost. The details of these personal calls cannot be disclosed to third parties without the consent of the person concerned.

According to the AC 04/2000, for legal and statistical purposes, details of personal calls will be stored and retained for up to three years from the date of the first backup. The data retained as concerns personal calls is the date, time, extension used, PIN used, number dialled and the duration. After the expiry of this period, all detailed personal call data will be deleted. There are no rules provided in the AC 04/2000 as concerns conservation of data relating to business calls.

As a general rule, persons who do not have access to the call charging facility have to make personal calls from public payphones or by using a personal, pre-paid telephone account. In cases where data subjects do not have access to the call charging facility (e.g. external consultants, trainees etc.), the persons concerned may request the deletion of traffic data related to private calls prior to the communication of the itemised billing to their respective manager.

Investigations procedures on the use of office phones

There are two potential reasons for further investigation: either a member of staff disagrees with the content of an itemised personal call listing, or a line manager disagrees with the data relating to the business calls. Should this be the case, an annex to the AC 4/2000 establishes the Call Charging Facility Investigation Procedures.

Disagreement with the content of itemised private call listing

If on receipt of an itemised call listing, a member of staff cannot identify a listed call as having been made by him or her, the member of staff should start by making investigations by following a procedure set out in the annex. This notably includes checking the extension number from which the call was made, the date and time of the call, the member of staff can contact the OSS (Office Services and Security) switchboard for details of the exact number called. If after having followed these steps, the member of staff is still unable to resolve the issue, but is still certain that he/she did not make the call(s), he/she should discuss the details of the situation with his/her line manager.

If a line manager is involved in the procedure, he should assess the situation and make a decision. Different options are left open to him in the annex. Continual complaints from a member(s) of staff relating to calls originating in the same extension, or extensions in the same area, will lead to further investigations to assess whether a PIN code(s) is being misused by a third party. Such requests should be forwarded to OSS for the analysis of data compiled over a given period, for example over three/six months. OSS may decide to involve DG-IS (Information Systems) as well in order to provide technical assistance. Once the analysis is complete and if the issue remains unsolved, the Directorate Personnel should be informed. It is then up to Directorate Personnel to decide whether or not Directorate General Legal Services (DG-LS) and the Directorate Internal Auditing (DIA) need to be consulted/informed.

Disagreement with content of business calls statistics

Should a manager wish to query the content of statistical information received relating to business calls of individual members of staff, or require additional information, he should first inform the staff member involved that an investigation will be conducted. He may then contact the switchboard and request detailed information on each individual extension number for a given call reference period. In the case where he/she is dissatisfied with the content of such listings, the line manager should discuss the issue with the member of staff concerned and resolve discrepancies where possible. If the problem is still left unresolved, the line

manager should request historical information from OSS and assistance in further investigating the situation. This may show that call patterns that could prove useful in resolving discrepancies in business call listings. For example, numbers in same region or calls made at same or similar times perhaps when owner of handset is regularly away from his or her desk. If, having assessed the situation, there are grounds to suspect misconduct on the part of a member(s) of staff, the Directorate Personnel shall be informed. It will then be up to Directorate Personnel to evaluate the situation and to consult or inform DG-LS/DIA if necessary. The manager will then decide together with Directorate Personnel and DG-LS/DIA about further actions.

According to the AC 04/2000, deliberate misuse of the CCF facility shall be treated as misconduct and shall be subject to disciplinary measures.

Security measures

[...]

2.2. Legal aspects

2.2.1. 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 (hereinafter Regulation 45/2001) 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. In most cases the data processed in this procedure are data which can be linked to a specific extension number and are therefore related to an identified or identifiable person. The data are therefore qualified as personal data according to Regulation 45/2001.

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

The Regulation applies notably to the processing of personal data wholly or partly by automatic means. Clearly here we are in the presence of processing which is at least partly automated since the data are contained not only in business/private call lists, but traffic data are also contained in the ECB's telephone log-files or on devices (CDs) where relevant data are stored.

Regulation 45/2001 therefore applies.

Article 27(2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present specific risks. The list includes, *inter alia*, (i) processing of data "relating to suspected offences or offences or security measures" (Article 27(2)(a)) and (ii) processing operations "intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct" (Article 27(2)(b)). Where a mechanism is in place to monitor the communication network for purposes of Articles 27(2)(a) and/or 27(2)(b) of the Regulation, the processing operations must be submitted to the EDPS for prior checking.

Since prior checking is designed to address 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. In any case, this is not a serious problem in that any recommendations made by the EDPS may still be adopted accordingly.

The prior check focuses on the processing of personal data relating to the investigation of the use of office telephones at the ECB, and does not concern the processing of data issued by the use of mobile phones of the ECB, the latter being the object of a separate prior check (2004-0272).

The Administrative Circular 04/2000 will be modified in the near future. This opinion is based on the AC of 8 December 2000.

The investigation procedures regarding the use of the phone may possibly lead to a disciplinary procedure. Disciplinary procedures were the object of a separate prior check by the EDPS (2004-0270) and are therefore not covered by the present prior check.

The prior checking procedure based on the notification previously received was launched on 12 June 2006. According to Article 27(4) the present opinion must be delivered within a period of two months. The time limit was suspended for 28 + 150 + 7 days. The opinion must therefore be delivered no later than the 13 February 2007.

2.2.2. Lawfulness of the processing

Article 5 (a) of Regulation 45/2001 stipulates that personal data may be processed only 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". The recitals (§27) to the Regulation further specify that "processing of data for the performance of tasks carried out in the public interest of the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies". The investigations into the use of the telephone can be considered as necessary for notably controlling costs and for budget management and to this extent can be considered as necessary for the management and functioning of the ECB as established by the EC Treaty. The legal basis as provided for by the Administrative circular further support the lawfulness of the processing in accordance with Article 5 of Regulation 45/2001.

Any processing of data in the frame of an investigation on the telephones is based on the rule according to which "all equipment and facilities, whatever their nature, are provided to the Addressees by the ECB for official use only, unless private use is permitted either according to relevant internal rules or practices or on a discretionary basis" (Article 4.2 of the Code of conduct of the ECB). The rules for the official and private use of the ECB's telephone and fax equipment are provided in Administrative circular 04/2000 of 8 December 2000. The annex to this Circular establishes the Call charging facility investigation procedures. The processing of the data is based on these instruments.

2.2.3. 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) and must be accurate and where necessary kept up to date (Article 4(1) d).

The purpose of the procedure of investigation of the use of the telephone is the management of the telephone system capacity, to ensure that the appropriate level of telephone access is granted to accommodate the business requirements of the respective member of staff according to his/her function and job tasks and to make sure that the rules for the personal use of the ECB telephones are respected. The processing of data therefore only concerns traffic data that is to say the data necessary to convey the communication or for the billing thereof and does not involve any data concerning the actual content of a telephone communication. In view of the purposes of the processing, this limitation to traffic data is fully adequate. It must however be determined which traffic data are necessary for the declared purposes and which data can be communicated to the different parties involved in the procedure.

According to Administrative circular 04/2000 (1.3), budget centre managers receive two lists of business calls made from extension numbers in their area of competence for their information.

As mentioned in the facts, the first list contains the extension names, extension numbers, the number of calls made from each extension, the duration and the total charge. The second list contains the extension name, extension number and the percentage of calls made within the city, national or international. This data are considered as adequate for the purpose of verification of the use of the office telephone for business purposes.

Members of staff receive itemised call listing of private calls. As also mentioned in the facts, the lists contain the following data: date of the call, the time, the extension used, the first few digits of the number dialled, the duration of the call and the cost of the communication. This data are considered as adequate for the purpose of the processing. Furthermore, the fact that this list is sent to the member of staff concerned contributes to ensuring the adequacy of the data as it gives him/her the possibility of correcting any incorrect data.

In cases where data subjects do not have access to the call charging facility (e.g. external consultants, trainees etc.), the persons concerned may request the deletion of traffic data related to private calls delete traffic data related to private calls prior to the communication of the itemised billing to their respective manager. The EDPS welcomes this initiative which contributes to respecting the principle of data quality.

2.2.4. Conservation of data

Article 4 §1 e) provides that data may only be kept for as long as is necessary for the purpose for which the data were collected and/or further processed.

Article 37 provides for specific rules as concerns the conservation of traffic and billing data.

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 no longer necessary for the establishment of the call or connection.

Article 37§2 however provides 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, traffic and billing data relating to personal calls are stored and retained for up to three years from the date of the first backup. This conservation period of up to three years is not compliant with Article 37 of the Regulation. Traffic and billing data processed and stored in the frame of the investigation procedure the purpose of which is precisely budget and traffic management, including the verification of authorised use of the telecommunications systems, may only be kept for six months. The data may only be kept for longer than these six months if a legal claim is actually pending. The AC 4/2000 must therefore be modified so as to provide that the traffic and billing data relating to the use of the office phones may, as a rule, not be stored for more than six months.

Adequate rules must be set up as concerns the conservation of traffic and billing data relating to business calls in accordance with Article 37 of Regulation 45/2001.

Article 20 also provides that exemptions and restrictions may be brought to Article 37 §1 if 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 investigations¹.

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 but has been dealt with in the prior check opinion on disciplinary procedures (2004-0270).

The data may also be kept for longer than six months to allow analysis on a yearly basis. In this case, the data must be made anonymous and may only be processed for statistical reasons. Making the data anonymous implies not being able to link the data to any identified or identifiable person. Since an extension number can be linked to an individual, it is recommended that the reference to the extension number be removed from the files before they are processed for statistical purposes.

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

¹ See Opinion in case 2004-0198 of 21 March 2005 on the notification for prior checking relating to data processing in the context of disciplinary files by the European Parliament.

- 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.

2.2.5. Transfer of data

The only recipients of data related to the investigation procedure on the use of the telephone system are budget centre managers; all responsible managers as concerns their units; the Directorate General Human Resources Budget and Organisation and if necessary the Directorate General Legal Services and the Directorate Internal Auditing in case of a suspected misconduct. This complies with Article 7 §1 of Regulation 45/2001 according to which personal data may only be transferred within or between Community institutions or bodies notably "if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".

In the event of the opening of a disciplinary procedure, the data may be transferred to other parties. The legal implications of this transfer have been dealt with in the prior check on disciplinary procedures (2004-0270).

2.2.6. Right of access and rectification

According to Article 13 of Regulation (EC) 45/2001, "the data subject shall have the right to obtain without constraint and at any time within three months from the receipt of the request and free of charge from the controller information at least as to the purposes of the processing operation, the categories of data concerned, the recipients to whom the data are disclosed and communication in an intelligible form of the data undergoing processing and of any available information as to their source". Article 14 provides: "the data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data".

As concerns private call listing, the member of staff concerned receives an itemised call listing and therefore has access to the data relating to him/her. As concerns business calls, according to the Administrative circular 04/2000 in the course of an administrative investigation, or prior to that during the discussions with their line manager, data subjects have access to the relevant business call lists with statistic data. The notification received from the DPO of the ECB specifies that in order to access other data related to their business calls data subjects should contact the controller. This should be mentioned in the Administrative Circular.

The notification from the DPO of the ECB mentions that all other rights laid down in section 5 of the Regulation can be exercised by the data subjects by addressing themselves to the controller. However this is not stipulated as a right in the Administrative Circular. The data subject will need to be informed of the existence of these rights and notably that of rectification of the data. This will be further developed below.

2.2.7. Information to the data subject

Article 11 of Regulation (EC) 45/2001 specifies that the controller must provide information to the data subject. This information covers at least the identity of the controller, the purposes of the processing operation for which the data are intended, the recipients or categories of recipients, whether replies to questions are obligatory or not as well as the possible consequence of a failure to reply and the existence of a right of access to, and right to rectify

the data concerning him/her. Further information may also have to be provided, depending on the circumstances, such as the legal basis of the processing operation, the time-limits for storing the data and the right to have recourse at any time to the EDPS. When personal data is collected directly from the data subject, the information should be provided at the time of collection of this data.

Personal data concerning the use of the ECB's telephone and fax equipment are collected from the data subject and Article 11 therefore applies. The data subject must be informed at two levels: about call charging facility investigation procedures at a general level, but also in the event of an investigation procedure taken following the involvement of a line manager concerning the member of staff.

The EDPS takes good note that general information on the rules for the official and private use of the ECB's fax and telephone equipment and the call charging facility investigating procedure is provided for in the AC 04/2004. As mentioned in the facts, the AC and the relevant attachments are published on the ECB's intranet site. Additionally staff members are informed in specifically organised "induction seminars" about the most important provisions concerning the professional duties, including the rules for the private and official use of the phones. Data subjects are to contact the controller for additional information concerning the processing of their personal data in the frame of this procedure.

The EDPS is satisfied that information is provided on the purposes of the processing of the data, the recipients of the data, and, as concerns personal calls, the right of access and the time limits for keeping the data. He is also satisfied that before the start of an investigation into the use of the phone facilities, the person concerned is informed that such an investigation will be carried out. He would however like to underline that information must be provided about the identity of the controller and the fact that to access data related to their business calls data subjects should contact the controller. Moreover he recommends information is provided as to the time limits for storing data related to business calls and the possibility for data subjects to have recourse at any time to the EDPS.

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 AC 4/2000 must be modified so as to provide that the traffic and billing data relating to the use of the office phones both for business and personal use, may as a rule, not be stored for more than six months;
- It is recommended that the reference to the extension number be removed from the files before they are processed for statistical purposes;
- The AC should mention that in order to access other data related to their business calls, data subjects should contact the controller;

- The AC should provide information on the identity of the controller and the fact that to access data related to their business calls data subjects should contact the controller, and preferably also the time limits for storing data related to business calls and the possibility for data subjects to have recourse at any time to the EDPS.

Done at Brussels, 13 February 2007

Peter HUSTINX
European Data Protection Supervisor