

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 mobile telephones

Brussels, 26 February 2007 (Case 2004-272)

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 investigation procedures regarding the use of mobile telephones as a case for ex-post prior checking.
- 1.3. On 10 October 2006, the EDPS received the notification of the case for prior checking.
- 1.4. On 11 October 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.
- 1.5. On 21 December 2006, EDPS decided to lift the suspension on the basis of information received from the DPO according to which the modified version of the Administrative Circular 04/2000 on the use of the ECB's telephone and fax equipment would not be adopted before March 2007.
- 1.6. On 30 January 2007, the EDPS made a request for information to the controller and DPO. This was answered on 31 January 2007.
- 1.7. On 8 February 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.
- 1.8. On 15 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 that mobile phones are issued permanently for business purposes upon request (1.4). In addition, business areas may issue mobile phones on a temporary basis from a decentralised pool of mobile phones available to them.

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" (point 2 of AC 4/2000). Members of staff may need to make personal calls on their ECB mobile phone. This is accepted as long as such use is restricted to short and urgent calls (point 2.4 of AC 4/2000).

Monthly invoices on the use of mobile phones are downloaded from the provider's website and stored by the Service and Delivery Section (SDS) within the IT Operation and Support Division (OPS IT Service Delivery Section). Itemised bills are downloaded on a monthly basis (requested by Internal Audit) and stored in a folder with restricted access to limited staff of the Operation and Support Division's Voice team.

The data provided to the ECB by the service provider are a) the monthly mobile phone invoice that specifies the SIM card number and the total costs per card and b) the itemised phone bill per SIM card specifying the individual telephone numbers dialled.

On a monthly basis, ECB area heads receive a report from the OPS IT Service Delivery Section informing them about the total net costs of their staff's mobile phone usage. This list is produced via automated processing. Such information only contains the total expense per SIM-card, there are no individual connection costs nor any of the telephone numbers dialled.

Should a manager wish to query the monthly statistical information on the costs for calls made by an individual staff member via the ECB phone, or require additional information he should follow, by analogy, the procedure laid down in Article 3 of the annex to the administrative circular of 4 December 2000.

If area heads request more detailed information, the OPS IT Service Delivery Section produces the itemised calling list for the particular SIM-card, but only sends it to the holder of the respective phone.

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, having assessed the situation, there are grounds to suspect misconduct on the part of a member(s) of staff, the Directorate General Human Resources shall be informed. It will then be up to Directorate Personnel to evaluate the situation and to consult or inform DG-Legal Service/Directorate Internal Audit (DG-LS/DIA) if necessary. The manager will then decide together with Directorate Personnel and DG-LS/DIA about further actions.

The holders of the phone may also receive upon their own request the data related to their SIM-card from OPS IT Service Delivery Section.

The circular 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 phones. Data subjects are to contact the controller for additional information concerning the processing of their personal data in the frame of this procedure.

According to the Administrative Circular 04/2000, for legal and statistical purposes, monthly reports and if applicable itemised bills will be stored and retained for up to three years from the date of the first backup. After the expiry of this period, all detailed personal call data will be deleted. This procedure will be modified in a new administrative circular currently under adoption to the effect that data will only be retained for 6 months. The respective managers will be reminded to destroy the monthly reports they receive for verification purposes on a regular basis.

Access to monthly reports and, if applicable, to itemised bills, is restricted to a limited number of staff members, who have been authorised by the controller on a need-to-know basis. The database hosting the basic call data (monthly summary) is currently maintained by the Voice Team in IT Operation and Support Division. A limited number of staff in the Voice team may access the database for the assignment of users to mobile phones and their telephone numbers. Access to the phone data is restricted to DG-IS/OPS line management and two subordinates working in the OPS IT Service Delivery Section who are in charge of checking and paying the monthly mobile phone bill [...].

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 mobile phone 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 list of aggregate call data sent to the business unit for verification purposes on a monthly basis is produced via automated processing.

Regulation 45/2001 therefore applies.

Article 27§2 of the Regulation contains a list of processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, notably processing operations intended to evaluate personal aspects relating to the data subject, including his/her ability, efficiency and conduct. The procedure described above is used to identify abuse of the use of the telephone system. This must be considered as a processing operation intended to evaluate the conduct of a person. The case therefore qualifies for prior checking under Article 27§2 b.

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 mobile telephones at the ECB, and does not concern the processing of data issued by the use of office phones of the ECB, the latter being the object of a separate prior check (2004-0271).

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 notification of the DPO was received on 10 October 2006. According to Article 27(4) the present opinion must be delivered within a period of two months. The time limit was suspended for 72 + 1 + 7 days. The opinion must therefore be delivered no later than the 28 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 ECB mobile phones can be considered as necessary notably for 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 mobile phones are

provided in Administrative circular 04/2000 of 8 December 2000. The annex to this Circular establishes the Call charging facility investigation procedures in the event of suspicions on the lawful use of the ECB's mobile phones. 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 ECB mobile phones is to ensure that the rules for the personal use of the ECB mobile phones are respected and to monitor the costs linked to the use of these mobile phones. 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 is necessary for the declared purposes and which data can be communicated to the different parties involved in the procedure.

As mentioned in the facts above, according to administrative circular 04/2000 the business unit to which the respective mobile phone is assigned will receive a list of aggregate call data for verification purposes on a monthly basis. This list is produced via automated processing. Per business unit, this list contains data on the name of the person using the phone, the mobile phone number and the total cost of communications made with that phone number. The details of the calls will not be revealed.

The data are considered as adequate for the purpose of verification of the use of the mobile phone.

Should a manager wish to query the monthly statistical information on the costs for calls made by an individual staff member via the ECB phone he may then contact the Voice team and request detailed information on each individual mobile phone number for a given reference period. The EDPS also considers that this is adequate and in line with the purpose of the processing.

The fact that the staff member also has access to the itemised bill in the event of an investigation serves to ensure the accuracy of the data.

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 in the context of internal communication networks. According to the scope of Chapter IV as defined in Article 34, this provision applies to "the processing of personal data in connection with the use of telecommunications networks or terminal equipment operated under the control of a Community institution or body". Article 37 therefore applies to the processing of traffic and billing data by a Community body in connection with the use of mobile phones

which it has made available to its staff, as is the case here. This is especially relevant for the processing of itemised data allowing a detailed insight in the communication behaviour of users.

According to Article 37§1, 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. 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.

According to the notification form for prior checking received from the ECB, itemised bills are downloaded on a monthly basis (requested by Internal Audit) and stored in a folder with restricted access to limited staff of the Operation and Support Division's Voice team. Monthly reports and, if applicable, itemised bills per mobile phone number will be stored and retained for up to three years from the date of the first back up.

The conservation of itemised bills has notably been justified by the controller for internal audit reasons. The EDPS believes that detailed traffic data received from external service providers need not be kept for the purposes of internal audit purposes for longer than six months unless in the frame of a pending legal issue. In this respect the EDPS welcomes the fact that the new administrative circular will provide that the data will only be kept for a period of 6 months and would like to see follow up on this issue.

The EDPS also welcomes the fact that the respective managers will be reminded to destroy the monthly reports they receive for verification purposes on a regular basis. A maximum period of six months must be established for the destruction of such data.

Article 20 also provides that exemptions and restrictions to Article 37§1 may be invoked 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.

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.

The data may also therefore be kept for longer on the basis of Article 20 of the Regulation in the frame of a disciplinary investigation. This is not, however, the object of this prior checking procedure, but has been dealt with in the prior checking opinion on disciplinary procedures (2004-0270).

The data may also be kept for longer than the conservation period established 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 a mobile phone number can be linked to an individual, it is recommended that the reference to the phone number be removed from the monthly reports before they are processed for statistical purposes.

Finally, the ECB has recourse to an external service provider to provide mobile phone services. This service provider must also respect the national law of the country in which it is established, adopted according to the provisions of Directive 2006/24/EC, and the retention periods as laid down by this law. Should the period for the retention of traffic data be longer according to the national law, the EDPS is of opinion that the ECB may not make use of this data after the period of conservation of six months established by the ECB unless this is for the establishment, exercise or defence of a right in a legal claim pending before a court or if necessary for one of the purposes provided for in Article 20.

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".

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 itemised bill. The holders of the phone may also receive upon their

own request the data related to their SIM-card from OPS IT Service Delivery Section. The right of access to the data is therefore guaranteed.

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 12 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 are 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 mobile phones are collected from the service provider and Article 12 therefore applies. The data subject must be informed at two levels: at a general level about call charging facility investigation procedures, but also at an individual level 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 mobile phone equipment and the call charging facility investigating procedure is provided for in the administrative circular 04/2004. As mentioned in the facts, the administrative circular 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 would however like to underline that information must be provided about the identity of the controller and the fact that the data subject can address himself to the controller to exercise his/her rights under Regulation (EC) 45/2001. Moreover he recommends that 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.

The EDPS is also satisfied that information is provided to the person concerned in the event of the opening of a specific investigation procedure.

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 consideration is fully taken into account:

- The EDPS would like to see follow up on the inclusion in the new administrative circular as concerns the fact that the data will only be kept for a period of 6 months. This maximum period of six months should also apply as concerns conservation of data by managers;
- Should the data be used for statistical purposes, it is recommended that the reference to the phone number be removed from the monthly reports before they are processed for statistical purposes;
- The administrative circular should provide information on the identity of the controller and the fact that, to access data relating to the use of mobile phones, data subjects should contact the controller, and preferably also on the time limits for storing data related to calls and the possibility for data subjects to have recourse at any time to the EDPS.

Done at Brussels, 26 February 2007.

Peter HUSTINX
European Data Protection Supervisor