Opinion on the notification for prior checking received from the Data Protection Officer of the European Investment Bank concerning the case 'Register of telephone calls (mobile telephony)'.

Brussels, 15 May 2012 (Case 2009-0704)

1. Proceedings

In a letter dated 11 October 2006, the Data Protection Officer (DPO) of the European Investment Bank (EIB) sent the European Data Protection Supervisor (EDPS) a notification for prior checking within the meaning of Article 27(3) of Regulation (EC) No 45/2001 ('the Regulation') concerning the file 'Recording of telephone calls, mobile telephony (2006-462)'. Information was requested in an e-mail sent on 27 October 2006. A reply was provided in a letter dated 28 November 2006. A further request for information was sent on 11 December 2006. The EIB then informed the EDPS that the policy for the use of mobile telephones was to be amended. The case was suspended pending the adoption of the new rules, which were sent to the EDPS by e-mail on 22 October 2009. In view of the amendments and the time elapsed since the initial notification, the EDPS decided to open a new case (2009-704) to replace notification 2006-462. The case was suspended to allow for the submission of additional information from 18 November to 9 December 2009 and then from 11 December 2009 to 20 September 2011. A meeting was also held on 16 September 2011 with the EIB's DPO to clarify certain facts. A second meeting was held on 26 April 2012 to clarify some of the new facts in the case.

2. The facts

The EIB has implemented a system for lending mobile telephones to members of staff for whom the EIB has recognised a need for these tools. The EIB, in its capacity as controller, is represented by the Human Resources Department (the organisational entity responsible for mobile telephony).

The mobile telephony system has no functionality to allow private calls to be distinguished from professional calls *a priori*. The EIB therefore set up an arrangement to allow the two types of calls to be differentiated *a posteriori* and thus for the cost of private calls to be deducted from the payslips of members of staff. In this way the EIB can also have access to relevant information regarding the monthly cost of business calls.

The distinction between private and business calls is made by 'self-reporting' by the staff members concerned. The EIB has set rules for the use of mobile telephones and has developed appropriate checks to ensure compliance with those rules, including checks on the veracity of the self-reporting (see note dated 20 January 2009 to staff members who have a mobile telephone).
The EIB has delegated the management of mobile telephony to LUXGSM S.A. Data from incoming and outgoing telephone calls made or received by all the mobile telephone handsets with LUXGSM network contracts are collected and stored by LUXGSM. These data are then transferred to the EIB. Within the EIB, the data is processed by managers using the PeopleSoft application (in which the data is processed) in the Human Resources department. The EIB's IT department is responsible for the technical maintenance of the database.

Anyone who has a LUXGSM mobile telephone or contract allocated to them on temporary loan for operational reasons by the EIB is therefore affected by the processing.

Processing is automated.

The data processed by the EIB for incoming and outgoing calls, both business and personal (Voice and Data; in other words both data from the calls and data from accessing e-mail or the internet via a mobile telephone), from the mobile telephones are required for billing purposes (identification number, first and last name of the member of staff, accounting code, monthly billing period, rate, country called, caller number, date of call, time of call, duration of call, number called and internet connection if applicable). The network operator LUXGSM maintains a list of mobile telephone users, which includes the following information: telephone number, first and last name, personnel number, address, expenditure centre, password, PUK code (code required when the PIN code has been forgotten). Data which can reveal content (websites visited, quantity of data transferred, average connection time, Wi-Fi use, SMS) are processed in an aggregated fashion. In other words, a user is only identified if it is thought that the usage infringes the rules.

LUXGSM holds all billing-related data for six months.[1] The EIB has been storing information about the personal and professional charges incurred by GSM users in PeopleSoft and in the IT department since April 2004. However, the EIB is in the process of changing data retention periods. It intends to store information about the private and business charges incurred by GSM users for only six months:

- in PeopleSoft: from the date it is entered in the application by the HR Department;
- by the telecom section of the IT department: from the date the EIB receives it.

Some content data are kept in aggregated form for statistical purposes (quantity of data transferred, average connection time, etc.).

In the event of an alleged infringement of the rules of use, the EIB's Data Protection Officer and Inspectorate General may receive the data. The legal department may also receive the data in the event of a dispute.

The data subject is informed of the rules for the use of telephones when he/she applies for a mobile telephone in a declaration regarding its use (the note of 20 January 2009 is annexed to the declaration). The application for a mobile telephone is accompanied by a declaration ('application for a mobile phone and declaration regarding its use') which must be signed by

[1] The EIB has signed an amendment to the contract concluded with LUXGSM to change the time limit for the retention of data. The retention time was reduced from one year to six months on 1 February 2010.

the applicant and submitted to the telecom section of the IT department; it contains a series of rules on the use of mobile telephones to which the user must adhere.

Access to the PeopleSoft database is controlled by password for EIB staff. The number of people who have access to the data is limited to PeopleSoft application managers in the HR department and to certain managers in the IT department.

Processing by LUXGSM on a sub-contracting basis is carried out under contract.

The procedure:

Several times a month, the telecom section of the IT department sends LUXGSM updated versions of the list of names of the persons concerned, together with a list of telephones on loan with user information (as Excel files) to allow LUXGSM to update its own database and draw up its monthly bills. At the beginning of the following month, LUXGSM sends the contract manager a complete file which shows the total volume of calls made by users. The contract manager checks the file which is then sent to the management section in the Human Resources department to be entered into the PeopleSoft system, which is accessible by users via My/HR to allow them to approve the total cost of their private phone usage.

Users are responsible for checking and, if necessary, challenging the bill within two months, by e-mail and directly with the operator. Both private and business communications are shown on the bill. After checking the bill, the user approves the total cost of his/her private telephone usage on the intranet via PeopleSoft. Access to this information in PeopleSoft is confidential and may only be accessed by the user using their password. If a user has failed to approve his/her calls after three months, all the costs will be deemed to be private and charged as such to the user.

The possibility of performing ad hoc ex-post checks is possible when the monthly mobile telephone bill for 'business' usage exceeds EUR 200. In this case, the system sends a message to the user and also to his or her line manager, who may decide to ask the user about the calls made. Both the staff, who are subject to these checks, and their line managers are informed immediately of the checks performed, the outcome thereof and how they may be used. A staff representative and the Data Protection Officer are also informed in confidence and without delay of any personal use of records of numbers called using the business line. Cases where use is deemed to be excessive or illicit may be subject to a technical investigation by the IT department following the approval of the HR Department and after the data subject has had the opportunity to state his/her case and his/her line management has informed the Human Resources Department. Article 1.5 of the EIB Code of Conduct is applicable if a member of staff has knowingly infringed his/her obligations, and disciplinary measures may then be applied by the EIB. This aspect of the procedure is not part of this analysis; processing data in the context of disciplinary procedures was examined already in EDPS opinion 2005-0102.

3. Legal aspects

3.1. Prior checking

The notification received on 22 October 2009 concerns the processing of personal data within the meaning of Article 2(a) of the Regulation on any information relating to an identified or identifiable person. Data regarding the users of mobile telephones on loan from

the EIB are processed by LUXGSM on behalf of the EIB, and also by the EIB itself in PeopleSoft.

Processing is carried out by a European institution and is carried out in the exercise of activities which fall within the scope of Community law (Article 3(1)). Data is processed wholly by automatic means (Article 3(2)). Therefore, the processing falls within the scope of the Regulation.

According to Article 27(1) of the Regulation, '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' are subject to prior checking by the EDPS. Processing data relating to traffic and billing in the context of internal telecommunication networks raises specific issues which are so significant that Chapter IV of the Regulation lays down a specific provision and special guarantees. In light of the foregoing, the processing operation in question is subject to prior checking by the EDPS.

In principle, the checks carried out by the EDPS should take place before the processing is carried out. In this case the prior checking takes place after the start of the processing operation. However, the recommendations of the EDPS still must be implemented.

Mobile telephony also allows internet access. The general policy for checking internet use is not examined in this opinion.

The DPO's notification was received on 22 October 2009. In accordance with Article 27(4) of the Regulation, this opinion must be delivered within two months of receipt of that notification. A request for information suspended the time-limit for submitting the opinion for 877 days. The EDPS will therefore give his opinion by 18 May 2012.

3.2. Lawfulness of the processing

In accordance with Article 5(a) of the Regulation, the lawfulness of the processing is associated with the performance of a task in the public interest on the basis of legal instruments adopted according to the Treaties establishing the European Union.

Two aspects must therefore be considered: firstly whether the Treaty or other legal instruments make provision for the task carried out in the public interest, namely the processing (the legal basis), and secondly whether the processing is indeed necessary to perform this task in the public interest (the necessity).

In the present case the EDPS notes that the EIB has adopted rules of use for mobile telephone handsets. These rules provide that the telephones are normally reserved for business use but may, within reason, be used for private purposes provided such use is declared, as their costs will be deducted from the salaries of the persons concerned. The EIB may carry out checks. The adoption of this note and the communication thereof to each mobile telephone user is a relevant aspect in determining that the legal basis is adequate pursuant to Article 5(a).

The legal basis for the processing is crucial since the data processed may be sensitive and the risks with respect to the rights and freedoms of data subjects considerable. In the present case this is based on staff notes (26 April and 15 May 2004) and Coordination memoranda (20 January 2009) on new procedures for private telephone charges and on the declaration which data subjects must sign when they wish to use a mobile telephone supplied by the EIB.

The EDPS has interpreted the concept of legislative acts in the widest sense, as documents with a legislative scope. An administrative decision by the EIB may therefore be deemed sufficient to comply with Article 5(a).

Furthermore, Article 37(2) of the Regulation states that traffic data may be processed for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems. The EIB has developed this processing for the purposes both of managing its budget effectively – through the self-reporting of private and business calls – and of ensuring compliance with the rules of use for mobile telephone handsets which it has adopted (see note to staff who have a mobile telephone, 20 January 2009).

In addition, recital 27 of the Regulation provides that '*[p]rocessing of personal 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 processing in question is, inter alia, the effective management of the institution's budget as regards mobile telephony.

The necessity of the processing must be assessed in light of the purpose of the processing. Indeed the processing must be necessary to achieve the purposes set out. Necessity and purpose are therefore directly linked.

As explained above, in the present case the purpose of the processing is for the EIB to ensure that the cost of private use of mobile telephones is charged to employees and that they are used for a reasonable amount of time.

3.3. Data quality

Data which is processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected (Article 4.1(c)), which, in this case, are the management of the telephone communications budget and ensuring compliance with the rules for the use of mobile telephones. It is necessary to establish whether the data are necessary to achieve the purposes for which they are collected. In the case analysed, the only data processed are those relating to billing and traffic, and no data concerning the content of communications are processed. The data described seem, in the present case, necessary in view of the purpose for which they have been collected. However, it is necessary to determine which traffic data are required for the stated purpose – see paragraph 4 regarding numbers dialled – and which data may be disclosed to the various parties involved in the proceedings.

Furthermore, the data must be processed fairly and lawfully (Article 4(1)(a) of the Regulation). Lawfulness has already been analysed (see paragraph 3.2). With regard to fairness, close attention must be paid to this aspect given the sensitive nature of the matter. In the case under examination this is linked to the information which must be communicated to the data subject. The information must be clear for the data subject – in other words form part of a transparent and comprehensive informative framework – and be available in a single document (see paragraph 3.8 below).

Finally, the data must be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased

or rectified' (Article 4(1)(d) of the Regulation). The system in itself seems to ensure data quality. The data subject's rights to access and rectification represent the second means of ensuring data quality (see paragraph 3.7). Furthermore, the list of calls sent to data subjects and the possibility for them to challenge the list is an additional way of ensuring data accuracy.

3.4. Data retention

The general principle of the Regulation is for personal data only to 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) of the Regulation).

Article 37 of the Regulation lays down specific rules regarding the storage of traffic and billing data in the context of internal telecommunication networks. These networks are defined in Article 34 as being 'telecommunications networks or terminal equipment operated under the control of a Community institution or body'.

Traffic data relating to users which are processed and stored to establish calls are erased or made anonymous upon termination of the call or other connection (Article 37(1)). The general principal is therefore to erase the data as soon as they are no longer required to establish the call or the connection.

Article 37(2) of the Regulation does, however, establish that traffic data stored for the purpose of telecommunications budget and traffic management, including the verification of authorised use of the telecommunications systems, must be erased or made anonymous as soon as possible and no later 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.

At present,[2] LUXGSM stores mobile telephony data relating to EIB staff for a period of six months.

The data have been stored since April 2004. The EDPS is pleased that the EIB is now endeavouring to comply with Article 37(2) of the Regulation by setting as short a storage period as possible, and of no more than six months after collecting the data, 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. All data older than six months which are not required for a legal claim must therefore be erased without delay.

In addition, some data required for approving private calls made by staff are no longer needed for verification of the budget once the approval has been given. This is the case, for example, of numbers dialled. The EDPS therefore recommends that these data, which are only necessary for the approval of private calls, be deleted as soon as approval has been given. Indeed the data have to be necessary for the purpose for which they have been collected. There is an insufficient link, once the private calls have been approved by the data subject, between the purpose – budget verification – and the data stored (e.g. the number dialled).

[2] The EIB signed an amendment to the contract concluded with LUXGSM to change the data retention period. The retention period was reduced from one year to six months on 1 February 2010.

Article 20 of the Regulation provides that exemptions and restrictions may be applied to Article 37(1) where such a restriction constitutes a necessary measure 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 Union, including monetary, budgetary and taxation matters; the protection of the data subject or of the rights and freedoms of others. This provision thus permits the retention of traffic and billing data for purposes other than the telecommunications budget and traffic management in a limited number of cases. The EDPS has interpreted Article 20 in the light of the *ratio legis*, and in particular by permitting exceptions for retention periods in the context of disciplinary investigations. In the context of disciplinary investigations, data which are appropriate, relevant and non-excessive for the purposes for which they are processed may thus be stored for more than six months in accordance with Article 20 of the Regulation (see in this regard the opinion of the EDPS regarding data processing in the framework of the disciplinary procedure at the EIB, 2005-102).

If there are plans to retain the data for longer for statistical purposes, this must be done in accordance with Article 4(1)(e), in that the data must be made anonymous.

3.5. Transfer of data

The processing operation must also be examined in light of Article 7(1) of the Regulation. Under that Article, personal data shall only be transferred within or to other Community institutions 'if [they] are necessary for the legitimate performance of tasks covered by the competence of the recipient.' Article 37(3) of the Regulation stipulates that the processing of traffic and billing data shall only be carried out by persons handling billing, traffic or budget management. The transfers described in the foregoing appear to meet the criteria of these articles adequately.

Article 7(3) of the Regulation provides that 'the recipient shall process the personal data only for the purposes for which they were transmitted'. Safeguards must be put in place to ensure that any person receiving and processing traffic and billing data at the EIB cannot use them for other purposes.

3.6. Processing including the personal number or identifier

The EIB uses personnel numbers. The use of an identifier is, in itself, no more than a means (and a legitimate one in this case) of facilitating the task of the data controller in processing personal data. However, such use may have serious consequences. Indeed, this is what prompted the European legislator to regulate the use of identifiers in Article 10(6) of the Regulation, which makes provision for the EDPS to intervene.

The aim here is not to establish the conditions under which the EIB may process personnel numbers but to draw attention to that provision of the Regulation. In the present case, use of the personnel number by the EIB is reasonable because use of this number merely is a way of facilitating the processing work, and billing in particular.

3.7. Right of access and rectification

Article 13 of the Regulation makes provision, and sets out the rules, for the right of access on the request of data subjects. Article 14 of the Regulation provides for the right to rectification of data subjects. In the present case, data subjects have access to an itemised bill which may be checked and challenged. This is in compliance with Articles 13 and 14 of the Regulation.

The EDPS, however, highlights that the EIB must ensure that the data is blocked and erased the data in accordance with Articles 15 and 16 of the Regulation.

Two separate situations should be distinguished with regard to the blocking of data:
(1) when the data subject contests the accuracy of the data, they must be blocked 'for a period enabling the controller to verify the accuracy, including the completeness of the data'. Thus, when the EIB receives a request for blocking on these grounds, it must immediately block the data for the period necessary to check the accuracy and completeness of the data;

(2) when the data subject requests the blocking of data as a result of unlawful processing or when data has to be blocked for purposes of proof, the EIB will require a certain amount of time to carry out an assessment to decide whether or not to block the data. In this case, even if they cannot be blocked immediately, the request must be processed quickly in order to ensure that the rights of the data subject are protected. The EDPS therefore takes the view that the request should be assessed as early as possible and within a maximum of 15 working days.

3.8. Information to be given to data subjects

Articles 11 and 12 of Regulation (EC) No 45/2001 cover information to be given to data subjects to ensure transparent processing of personal data. Data subjects must receive clear and proactive information. Article 11 provides that where the data have been obtained from the data subject, information must be supplied at the time they are collected. Where the data have not been obtained from the data subject, the information must be supplied at the time when the data are recorded or disclosed for the first time, except where the data subject already has it (Article 12).

In the present case, the data have not been obtained from the data subject. Therefore, Article 12 applies. It should be noted that data subjects are given a series of documents, in the form of staff notes, rules of use and a user guide when they are given a mobile telephone by the EIB. The data subjects also sign their application ('application for a mobile phone and declaration regarding its use') and receive a copy thereof. Although the information to be provided may be inferred from those documents, the EDPS wishes to emphasise that this information is somewhat lacking in clarity and may thus hinder a fair processing of the data. The type of information set out in Article 12 should be provided more clearly and preferably be made available in a separate document. Similarly, the EDPS requests that data subjects should also be informed of the data retention period and also of their right to refer the matter to the European Data Protection Supervisor at any time. Furthermore, reference to the Code of Conduct and to the potential consequences in the event of an infringement of the obligations under the Code should be included in the application signed by data subjects.

3.9. Processing personal data on behalf of the EIB in its capacity as controller

LUXGSM must be considered as the processor within the meaning of Article 2(e): LUXGSM processes personal data on behalf of the EIB.

Article 23 provides that processing carried out by a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations set out in Articles 21 and 22 shall also be incumbent on the processor. The sub-contracting of processing is indeed regulated by contract which states that LUXGSM shall only act on instructions from the EIB and that Regulation (EC) No 45/2001 shall apply to the processing of data which are sub-contracted. Article 23 therefore seems to have been complied with correctly.

3.10. Security

After careful examination by the EDPS of the security measures adopted, the EDPS considers that these measures are satisfactory in the light of Article 22 of Regulation (EC) No 45/2001.

4. Conclusion

The proposed processing does not appear to involve any infringement of the provisions of Regulation (EC) No 45/2001, provided that the aforementioned observations are taken into account. In particular this requires the EIB to:

- Comply quickly with Article 37(2) of the Regulation by making provision for a shorter retention period - of no more than six months - after the data have been collected, unless such retention is necessary to establish, exercise or defend a right arising from a legal claim pending before a court, and to erase all data older than six months which are not required for the purposes of a legal claim.

- Provide data subjects with information that is clear and preferably available in a separate document. The data subjects must also be informed of the data retention period and of their right to refer a case to the European Data Protection Supervisor at any time.

Done at Brussels, 15 May 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor