Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding the recording of switchboard and security room phone conversations

1. Proceedings

On 15 March 2013, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data relating to the "recording of switchboard and security room phone conversations" from the Data Protection Officer (**DPO**) of the European Investment Bank (**EIB**), together with supporting documentation.

Questions were raised on 21 March 2013 and 5 April, to which the EIB replied on 17 April 2013, also submitting additional documentation. The draft Opinion was sent to the DPO for comments on 7 June 2013; on 19 June 2013 the DPO confirmed that there were no comments.

2. The facts

When the EIB decides that its threat level is "yellow"[1] or higher the EIB may decide to record calls made to and from the switchboard and security rooms. This decision is made by its Crisis Committee[2] upon recommendation of the EIB's Head of Security. This decision is then re-assessed on a weekly basis. The recording is deactivated as soon as possible by formal decision of the Crisis Committee.

If the procedure is initiated, calls will be recorded as follows:

- incoming calls to the switchboard during office hours will be recorded until they are forwarded to their final recipient;
- outside office hours, incoming calls to the switchboard will be forwarded to the security rooms and recorded until forwarded to their final recipient;
- outgoing calls dialled directly from the switchboard and the security rooms (for the latter only outside office hours) will be recorded in their entirety.

Additionally, the time, date and length of the call as well as phone numbers (where available) will be stored. There is no warning for incoming callers that their call might be recorded.

Audio recordings of calls and associated data will be stored for 30 days, after which they will be automatically deleted, unless there is an ongoing investigation that justifies longer storage.

[1] The possible levels are the following:
a) white - normal level, no special threats identified;
b) yellow - response to tensions or a sense of threat, preparation for abnormal situations;
c) orange - threat has been announced or observed;
d) red - specific information on high probability of imminent terrorist threat received.
During 2011 and 2012, the threat level was constantly "white".

[2] Chaired by the Director-General Information and Corporate Centre; the Secretary-General and Directors-General concerned are members.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax: 02-283 19 50

For such investigations, there is a function in the phone system that allows exporting recordings.

According to the EIB, the recordings will only be used to analyse terrorist threats that may arise, notably threats made via telephone. Only the Head of Security (or his/her deputy) can obtain the access codes (valid once) from the IT department, which manages the EIB's telephone system. Obtained data may then be transferred to the Crisis Committee and upon its agreement and information of the DPO to the Luxembourg Police Authorities.

Data subjects will be informed via an information notice to be published both on the EIB's intranet and on the EIB's website. The information notice informs data subjects that "for reasons of special security threats" calls might be recorded without the use of a warning tone and contains the phone numbers of the FM Service Desk and the Head of Security, who may be contacted for further information.

If data subjects request access to their personal data, they may receive access upon authorisation of the Head of Security, who should consult the DPO before taking a decision. Data subjects will have the right to block the recordings (for proof) and to have them erased if they are unlawful. Restrictions as set out in Article 20 of Regulation 45/2001 (the Regulation) may apply.

The controller is the EIB, while the unit entrusted with the processing is the "Security & Services" unit in the "Building and Logistics" department of the "Information and Corporate Centre" directorate.

3. Legal analysis

3.1. Prior checking

The processing of data constitutes a processing of personal data and is performed by a Union body in the exercise of activities which fall within the scope of Union law. The processing of the data is done through automatic means. Therefore, Regulation No 45/2001 is applicable.

Article 27(1) of Regulation (EC) 45/2001 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". Article 27 (2) of the Regulation contains a non-exhaustive list of processing operations that are likely to present such risks.

Processing personal data related to electronic communication raises specific concerns; the entire chapter IV of the Regulation is devoted to the protection of personal data in this context. Article 37 establishes the general principle of confidentiality of communications.

The purpose of the processing is to record the content of calls, which thus qualifies as a processing operation likely to present specific risks to the rights and freedoms of data subjects.[3]

[3] See e.g. the following EDPS prior check Opinions: "Enregistrement de la ligne réservée aux appels relatifs aux urgences et à la sécurité à Bruxelles (n° 88888)", issued 22 May 2006; "recording of emergency phone calls at the JRC Ispra site", issued 13 October 2008; "Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)", issued 19 November 2008.

The notification also mentions the processing of data related to "security measures", which are one of the special categories of data triggering prior checking (Article 27(2)(a)). Specifically, it presents the fact that the data to be collected are to be used in assessing terrorist threats as a reason for submitting the processing operation to prior checking. It is worth mentioning that the "security measures" as defined by Article 10(5) of the Regulation are measures such as preventive detention or the freezing of assets and similar measures; not every collection of data for security purposes falls under Article 10(5). It goes without saying that for the vast majority of callers, there will be no link to such further measures.

Even though Article 27(2)(a) does not apply here, the processing operation is subject to prior checking under Article 27(1), as described above.

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, the EDPS was informed about a more intrusive predecessor to the notified processing operation. The EDPS strongly urged the EIB to notify the processing operation without delay, by the latest on 15 March 2013. The notification submitted presents significant changes from the preceding processing operation.

The notification of the DPO was received on 15 March 2013. According to Article 27(4) the present Opinion must be delivered within a period of two months. When the EDPS requests further information from the controller, this period is suspended until he receives replies. This case was suspended from 21 March 2013 to 17 April 2013 and from 7 June 2013 to 19 June 2013; in total, the case was suspended for 39 days. The EDPS shall therefore render his Opinion by 24 June 2013.

3.2. Lawfulness of the processing

Personal data may only be processed if grounds can be found in Article 5 of the Regulation. Article 5 (a) mentions processing that is "necessary for 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". Recital 27 of the Regulation clarifies that "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".

In certain situations of a high threat level and crisis, it might be necessary to take extra precautions to ensure proper functioning of the EIB. The main lines of the processing are established in an internal document which has been approved by the Management Committee of the EIB. This document sets out the purposes of the processing and the criteria for activating the recording. It does not contain information on the conservation periods or on possible recipients outside the EIB.

Given that the recording of calls is an invasive action, the rules should be clearly set in a legal basis. Notably the scope, the responsibilities of different actors, the conservation periods and recipients (all as modified in line with the recommendation in this Opinion) should be clearly established. The document submitted as legal basis does not address all of these aspects and should be amended.

Recommendation: Adopt a clear and complete legal basis for the recording of these calls.

3.3. Data Quality

Article 4(1)(c) of the Regulation establishes the principle that data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed.

The purpose of the processing is to analyse terrorist threats that may arise, notably threats received via phone, which were explicitly mentioned in the notification.

Given that the vast majority of calls received and made will not be relevant for this purpose, a blanket recording of all calls would clearly be disproportionate. The approach chosen, i.e. to only record calls when the threat level is "yellow" or higher and the Crisis Committee has formally decided to do so, allows restricting the intrusiveness of the processing operation and the unnecessary processing of personal data. This is an important step from the prior practice of always recording these calls.

The notification specifically referred to terrorist threats received via phone, which can reasonably be assumed to be more likely on incoming than on outgoing calls.[4] For this reason, distinguishing between incoming and outgoing calls could serve to further avoid the unnecessary collection and storage of personal data.

Recommendation: Evaluate whether the aim of the processing can also be achieved if only incoming calls are recorded.

3.4. Conservation of data

Records of calls incoming and outgoing calls are kept for 30 days if the system is activated. The stated purpose for this period is to analyse possible terrorist threats.

Article 4 of the Regulation contains the principle that personal data shall not be stored longer than is necessary for the purpose for which they have been collected or further processed.

To assess whether this conservation period is appropriate, a comparison to the periods for other security measures can be useful. For CCTV surveillance on the premises of European Union institutions and bodies, the EDPS recommends a maximum conservation period of 7 days (unless an investigation is started).[5] In the present case, this period seems to allow sufficient time for assessing whether recorded threats should be forwarded to the Luxembourg police authorities.

Recommendation: Reduce conservation period to 7 days or justify why a longer period is necessary.

[4] Additionally, for outgoing calls, the number dialled would be known in any case.

[5] The Guidelines are available on the website of the EDPS.

3.5. Transfers of data

Recordings of calls may be transferred to the Crisis Committee and, with its approval and after information of the DPO, to the Luxembourg police authorities.

Transfers are regulated by Articles 7, 8 and 9 of the Regulation, depending on whether the recipient is a European Union institution or body (Article 7), subject to national legislation implementing Directive 95/46/EC (Article 8), or not subject to national legislation implementing said Directive (Article 9).

For transfers to the Crisis Committee, Article 7 is applicable. The standard for transfer under this Article is that the data must be "necessary for the legitimate performance of tasks covered by the competence of the recipient" (Article 7(1)). The recipient shall only use the data for the purposes for which they were transferred. The Crisis Committee is in charge of ensuring EIB business continuity in crisis situations; information about threats is important for making these decisions, such transfers comply with Article 7.

For transfers to the Luxembourg police authorities, Article 8 is applicable. Even though Directive 95/46/EC itself does not apply to police activities, its implementing rules in Luxembourg also apply to this sector. Article 3 of the Luxembourg Data Protection Act ("loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel", as amended, emphasis added) says:

"*Article 3. Champ d'application*

(1) La présente loi s'applique:

[...]

- au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

(2) Est soumis à la présente loi:

(a) le traitement mis en œuvre par un responsable du traitement établi sur le territoire luxembourgeois; [...]"[6]

In case the recordings contain evidence of terrorist threats, transfers to Luxembourg police authorities could be covered under Article 8(a), as the transfer would be necessary for the police to carry out its tasks in the exercise of its official authority, i.e. the investigation of criminal acts, such as terrorist threats. As such transfers would likely occur on initiative of the EIB, it would need to assess whether such transfers are necessary on a case-by-case in each case of transfer. According to the notification, the Crisis Committee takes the decision on whether or not to forward the data. It should be ensured that the Crisis Committee considers each instance on a case-by-case basis. The assessment made should be documented in a register of transfers.

Recommendation: Assess whether transfers to the Luxembourg police authorities are necessary on a case-by-case in each case of transfer and document this assessment in a register of transfers.

[6] Retrieved from the website of Luxembourg's data protection authority: http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf.

3.6. Rights of access and rectification

Data subject have the right to access their data and to have inaccurate data rectified (Articles 13 and 14 of the Regulation). These rights can be restricted in line with Article 20; for example, Article 20(1)(a) allows restrictions when they are necessary to safeguard the prevention, investigation, detection and prosecution of criminal offences.

According to the notification, "*data subjects may access to respective conversation records upon authorisation from the Head of the Bank's Security, who should consult the DPO before giving such authorisation*".

As a restriction of the general rule, Article 20 should be read in a narrow way. Therefore, access should be given as a general rule, unless there are specific reasons justifying the use of an exception in a specific case. The phrase "upon authorisation from the Head of the Bank's Security" should be read in this light.

3.7. Information to the data subject

According to Articles 11 and 12 of the Regulation, a minimum catalogue of information is to be provided to data subjects, unless they already have it. Article 11 concerns situations where the data are obtained from the data subject, e.g. in application forms. Article 12 concerns situations where data are not obtained from the data subject, that is to say if there is no direct interaction between the data subject and the controller and the data subject is not necessarily aware of her/his data being collected (e.g. video-surveillance, early phases of internal investigations). The common elements of this catalogue are the identity of the controller; the purposes of the processing operation for which the data are intended; the recipients or categories of recipients of the data; the existence of the right of access to, and the right to rectify, the data concerning him or her; any further information necessary to guarantee fair processing (e.g. the legal basis of the processing operation for which the data are intended, the time-limits for storing the data, the right to have recourse at any time to the European Data Protection Supervisor). Restrictions are possible in line with Article 20 of the Regulation.

The notice included in the notification and to be published on the EIB's website only mentions the purpose of the processing operation, the broad categories of data concerned and contact details to obtain further information.

Irrespective of whether the current situation falls under Articles 11 or 12, this information is not sufficient.[7]

It should also be noted that although this information notice would in theory be available for all data subjects, this is not enough to ensure adequate information. Unless one of the exceptions under Article 20 of the Regulation maybe properly applied (e.g., prevention, investigation, detection and prosecution of criminal offences), the EIB should play an automatic message to incoming callers while they are waiting for an operator to pick up the phone. This message should contain basic information on a possible recording and its purposes.[8] It would only need to be played when the recording is active.

[7] In similar previous cases, the EDPS has considered Article 11 to be applicable if the recording is announced (see the Opinions referred to in footnotes 1 and 1).

[8] This would mirror established practices for other procedures that involve recording calls, see e.g. EDPS prior check Opinion on "Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)", issued 19 November 2008.

The information notice should be expanded to include all the information mentioned in Article 11 of the Regulation.

While for the general public, a general privacy notice published on the EIB's website and a message for incoming callers would be sufficient, staff working at the switchboard and in the security rooms should receive more targeted information, given that they are more concerned. This could be done by additionally sending the notice via e-mail to the staff concerned or otherwise ensuring that staffs are aware.

Recommendations: Unless one of the exceptions under Article 20 of the Regulation may be properly applied, incoming callers should receive a short automatic message informing them about the processing. The information notice should be expanded to include the information mandated under Article 11. Staff working at the switchboard and in the security rooms should receive more targeted information.

3.8. Security measures

[...]

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the recommendations made in this Opinion are fully taken into account.

To recall, the recommendations made are the following:

- adopt a clear and complete legal basis for the recording of these calls;
- evaluate whether the aim of the processing can also be achieved if only incoming calls are recorded;
- assess whether transfers to the Luxembourg police authorities are necessary on a case-by-case in each case of transfer and document this assessment in a register of transfers;
- the conservation period should be reduced to 7 days or the necessity of a longer period should be justified;
- the information notice should be expanded to include the information mandated under Article 11;
- staff working at the switchboard and in the security rooms should receive more targeted information;
- Unless one of the exceptions under Article 20 of the Regulation may be properly applied, incoming callers should receive a short automatic message informing them about the processing.

Done at Brussels, 20 June 2013

(**signed**)

Giovanni Buttarelli
Assistant European Data Protection Supervisor