**Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank (EIB) concerning procedures related to "360° Leadership feedback report"**

Brussels, 20 July 2010 (Case 2009-0215)

## 1. Proceedings

On 30 March 2009, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data in the context of the deployment of a "360° Leadership feedback report" from the Data Protection Officer (**DPO**) of the European Investment Bank **(EIB)**.

The EIB decided to deploy its tool in two different steps. In a first phase, called pilot phase, the tool was deployed only among a few EIB directorates, namely the Directorate OpsA, the Directorate Strategy and Corporate Center (SCC) and Human Resources. Then, as a second step, the full deployment of the tool within the EIB is foreseen starting from mid July.

Following his established approach as regards pilot projects, the EDPS analysed the procedure implemented in the context of the pilot project and provided specific recommendations relating to the pilot project on 14 September 2009, before its launch. The EDPS also provided recommendations that should be taken into account for the full launch of the tool, in order to avoid any contradictions between the two phases (pilot phase and full launch of the system) that could have an impact on the protection of personal data. The pilot project was conducted by the EIB and results and conclusions of this exercise were provided in writing to the EDPS on 21 May 2010.

As already announced in the comments of 14 September 2009, this prior checking opinion closes the analysis of the prior-checking, following the receipt by the EDPS of the conclusions from EIB on the pilot project.

The draft opinion was sent to the DPO for comments on 14 July 2010. The EDPS received the reply of the EIB on 16 July 2010.

## 2. The facts

The 360° Leadership tool is a self-development tool for managers and experts at C-level and above. The **purpose** of this tool is to allow them to identify their strengths and areas for development. The tool is provided on a voluntary basis, both to those who qualify for enrolment in the program ("reviewees") and to those who will provide feedback on their skills ("reviewers"). Individuals who volunteer in the program will obtain feedback regarding their

behaviour at work from peers, managers and/or those reporting directly to the reviewee. This will help formalise the needs of training and the programs for professional development. It is an online tool specially designed and customized to the EIB to compile feedback about the observed leadership behaviours from various groups of reviewers and compare the results with the reviewee's own perception.

According to the EIB, the deployment of the 360° Leadership feedback tool is based on Article 13(3) of the EIB Statute and Article 21 of the EIB Rules of procedure. The 360° Leadership Feedback tool forms part of the new human resources strategy within the Corporate Operational Plan (COP) 2009-2011, approved by the Board of Directors on 16 December 2008, which reinforces self-awareness and individual development plans that include focused training.

The **primary responsible person** for the data processing within EIB is HR Head of Division People and Organisational Development. The EIB has outsourced to a **processor**, Cubiks, the implementation of the assessment tool by means of a contract for the provision of services dated 9 October 2007. The 360° Leadership feedback tool is provided to EIB by means of a Licence Agreement, which contains a data protection clause in line with the requirements set forth in Article 23 of the Regulation (EC) N° 45/2001.

As regards **data subject**s concerned, in the pilot phase, the 360° Leadership feedback tool was rolled out as a pilot among the management of the Directorate OpsA, the Directorate Strategy and Corporate Center (SCC) and Human Resources. In the pilot phase, it was foreseen that approximately 30 individuals would be subjects to assessment through the tool. In the end, a total of 47 volunteers eventually participated.

In the full implementation of the tool, the primary target group is made of the EIB Managers and Experts, both SC and C level. It is not foreseen to offer it to senior management since the model is designed based on competencies that include management, coaching and development, and delegation as observable behaviours.

As to the **data/categories of data processed**, the name, first name, position, direction or division; strengths and areas for development (in relation to the leadership competency model) and recommendation on Training and on-the-job development activities matching development needs are processed.

Moreover, the names and the email addresses of the participants will be provided by the EIB to Cubiks who will directly invite the participants and send them the link to the 360° Leadership feedback questionnaire. Reviewees will be asked to respond to a questionnaire within a period of two weeks, and to propose at least 3 peers from the same or from a different department that will be validated by the manager to be invited as reviewers. Feedback on a particular individual's management and leadership skills will be provided by reviewers on an anonymous basis.

According to the notification, this information will be consolidated and an **automatic** individual report will be generated that identifies the reviewee's strengths and areas for development (in relation to the leadership competency model), and which provides recommendation on training and on-the-job development activities matching development needs. The individual report containing the 360° Leadership feedback will be accessible only to the data subject. Group reports will also be generated and provided to HR responsible persons and Directors General, who will have access only to aggregated information about the

compiled group results (such as most voted and less voted competencies, number of participants), without any possibility to track or identify individual answers.

As far as the **conservation of the data** is concerned, the EIB described that both for the pilot project and for the general tool, the feedback data collected through the tool will be deleted after 6 months. The individual 360° Leadership Feedback Report will be stored on the server of the external provider (Cubiks). The owner of the individual report is the person concerned (manager, expert) and HR will not store a copy of it. Once the data subject has obtained the individual 360° report, the 360° report will be deleted automatically by the external provider Cubiks after 6 months. As concerns the group reports, the EIB states that those are kept by Human Resources for two years before they are deleted.

As regards **data transfers**, the individual report containing the 360° Leadership feedback will be accessible only to the reviewee, who may choose to disclose his/her individual report to recipients within EIB on a voluntary basis. It is specified that all managers who participate in the 360° are recommended to share their results with their direct manager, although this will not be mandatory, as input for his development plan. The reviewee may also wish to share his/her results with HR experts for further advice and support. As regards group reports, they will be provided to persons responsible within HR (Director, People & Organisation Head of Division, person responsible for Learning and Development) and Directors General, who will have access only to aggregated information about the compiled group results.

Regarding the **right of access and rectification**, the data subject has access to her/his individual 360° Leadership Feedback report through an individual access code provided by the external supplier. The participants are previously informed about the procedure and questionnaire they will receive and how to answer the questionnaire with possibility to rectify before sending it out. Access to the results is to be restricted to the data subject, who can erase the report from the server once it has been received. Hierarchy and authorized HR people within People Organisation & Staff management will receive Group reports containing statistical data of results anonymously without reference to the names. Both the data subject and those participating as reviewers are informed about this procedure.

As to **information**, the EDPS noted that in the pilot project, the EIB did not have its own privacy policy concerning this processing operation. However, reviewees were provided with Cubiks' data protection policy online before accessing the 360° tool. Similarly, reviewers were provided with Cubiks' data protection notice online before participating in the assessment.

After the evaluation of the pilot project, the EIB provided the EDPS with the data protection notice which is provided to participants in a message at the beginning of the process. A message is also provided when the reviewees have already provided the email addresses of their nominated reviewers. The EIB also provided the message which is displayed when a data subject accepts to participate and receives the invitation mail. Finally, the EIB also provided a snapshot of the first page of the website when the data subject enters the questionnaire and the message displayed before starting the questionnaire

As regards **security measures**, (...). A contract covers the legal relationship between the EIB and the processor, which contains the elements of Article 22. The website address of the processor, where data subjects fills in the assessment follows the https:// format.

## 3. Legal analysis

### 3.1. Prior checking

**Applicability of Regulation No 45/2001 ("the Regulation"):** The notification received on 30 March 2009 concerns the evaluation that will be carried out using the 360° Leadership feedback tool. This processing constitutes processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2(a) of the Regulation). The feedback received by the participant will not reveal the way in which the colleagues completed the answers ("who said what"). Nevertheless, these data can not be considered "anonymous" because the contractor has the possibility to link the answers with the colleagues who have produced them (see Recital 26 of Directive 95/46/EC: *"(...); whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person; (...)"*).

The EIB is the data controller of this processing activity because it determines the purposes (as specified under point 2 above) and the means (the use of the web-based tool) - Article 2(d) of the Regulation. The contractor is therefore not authorised to make any further processing activity beyond what is determined by the EIB and specified in the contract.

The data processing is performed by a data processor (Cubiks) on behalf of an Institution, in this case, the European Investment Bank, in the exercise of activities which fall within the scope of EU law (Article 3(1) of the Regulation). The processing of the data is done electronically. Therefore, the Regulation (EC) No 45/2001 is applicable.

**Grounds for prior checking*:*** Pursuant 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 purpose shall be subject to prior checking by the European Data Protection Supervisor*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks. This list includes Article 27(2)(b): "*processing operations intended to evaluate personal aspects relating to the data subject, including his ability, efficiency and conduct"*. The purpose of the notified processing operation is the evaluation of the data subjects' leadership skills. Therefore the use of 360° Leadership feedback tool is subject to prior checking by the EDPS.

**Deadlines*:*** The notification on the pilot phase was received from the DPO on 30 March 2009. The information relating to the final system submitted for true prior-check was received on 21 May 2010. According to Article 27(4) of the Regulation, the EDPS opinion must be delivered within a period of two months.

The procedure was suspended for a total of xxx days to require additional information and to allow for comments from the data controller. Consequently, the present opinion must be delivered no later than on 22 July 2010.

### 3.2. Lawfulness of the processing

Article 5 of the Regulation provides criteria for making processing of personal data lawful. One of the criteria provided in Article 5(a) is that the *"processing 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 or in the legitimate exercise of official authority vested in the Community institution or body"*. The 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"* (recital 27).

The legal basis of the processing is described as part of the Staff Regulations and Staff Rules. Moreover, the EIB also adopted a Corporate Operation Plan for 2009 to 2011 that includes the new HR strategy, stating that HR will focus its efforts on training and individual development plans.

Even if the assessment conducted in the context of the **360° Leadership feedback report** tool might be useful, it is not "necessary" for the performance of the task described in the mentioned rule. This is demonstrated by the fact that the participation in this activity is made on a voluntary basis.

Therefore, the processing activity under analysis has to be based on Article 5(d) of the Regulation, which states that personal data may be processed only if *"the data subject has unambiguously given his or her consent"*. The *"data subject's consent"* is defined in Article 2(h) of the Regulation as follows: *"any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*.

In the present case, the data subject is specifically informed about the processing activity in the light of Article 11 of the Regulation and the fact that he or she is free to participate or not in the exercise.

With regard to the consent of the candidates, the EDPS wants to draw the attention of the EIB to the position of the Article 29 Working Party on this matter[1]. The Article 29 takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting; the consent is not valid in terms of satisfying either Article 7 or Article 8 (of Directive 95/46) as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice

As a consequence the EDPS repeats that no negative consequences can affect the data subject if he or she decides not to participate or not to provide his assessment to his superior.

### 3.3. Data Quality

**Adequacy, relevance and proportionality:** According to Article 4(1)(c) of the Regulation, personal data must be *"adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed"*. The information presented to the EDPS on the data processed appears, *prima facie*, to meet those requirements.

As regards the pilot project, the EDPS warned that the use of open fields for comments by reviewers could lead to the disclosure and processing of data that are excessive in relation to the data processing, such as sensitive data (Article 10 of the Regulation). The data controller had to avoid processing data that are not necessary and ensure that no sensitive data in the sense of Article 10 of the Regulation were processed.

Following the EDPS' analysis, the data controller included the following sentence in the message to participants in the context of the pilot project: "the 360° questionnaire finishes

[1] Opinion 8/2001 on the processing of personal data in the employment context, Article 29 Working Party.

with an optional free text option that will be *copy/paste* to the answers in the report with the unique purpose of precising in maximum three lines a constructive and honest message aiming at the reviewee's awareness and development."

The EDPS also notes that the EIB implemented the request made in the analysis of the pilot project that in order to preserve the anonymity of participants, in case the number of participants is too reduced, no group report be generated.

Finally, as regards group report, the EDPS understands that they will be provided to persons responsible within HR and Directors General, who will have access only to aggregated information about the compiled group results. These reports, as stated by the EIB should therefore not allow any possibility to track or identify individual answers.

With these rules implemented, the requests from the EDPS can be considered as fulfilled.

**Accuracy:** Article 4(1)(d) of the Regulation provides that personal data must be *"accurate and, where necessary, kept up to date"* and that *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete are erased or rectified"*.

The EDPS noted in his analysis of the pilot project that "the data subject will have direct access to his/her individual 360° Leadership feedback report which will allow him/her to understand the data processed about him/her. It may however be difficult in such case to ensure the accuracy of feedback data provided by persons other than the data subject, which are by essence of a subjective nature."

The EDPS further noted that, "in accordance with the conditions set forth in Article 20 of the Regulation, the right of the data subject to access and rectify personal data relating to him/her may be limited in order to protect the rights and freedoms of others - in this case it is crucial that appropriate measures are implemented to prevent a reviewee from obtaining information revealing the identity of the persons who reviewed his/her skills so that he cannot exercise any retaliation against them, in particular for those reviewers that are in a subordinate position."

In the light of the EDPS analysis, the data controller stated that all measures have been taken to prevent reviewees from obtaining information revealing the identity of the persons who reviewed their competencies, as stated in the invitation to participate in the 360° leadership feedback. Information will be consolidated and will not allow the identification of individuals from inside EIB. The only information obtained by the reviewee is the consolidated answers from direct manager, peers and/or those reporting directly to the reviewee without any further information (such as nationality, age, seniority, answered or not answered).

**Fairness and lawfulness:** Article 4(1)(a) of the Regulation also provides that personal data must be *"processed fairly and lawfully"*. Lawfulness has already been discussed (cf. point 3.2) and fairness will be dealt with in relation to information provided to data subjects (cf. point 3.7)

The EDPS is satisfied with the measures implemented by the data controller on these aspects.

### 3.4. Data retention

Article 4(1)(e) of the Regulation states that personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"*.

As explained above, the EIB foresees that the feedback data collected through the tool will be deleted after 6 months. As concerns the group reports, those are kept by HR for two years.

As stated in the evaluation of the pilot project, the EDPS is satisfied with the conditions of retention established with respect to individual reports. Moreover, in the light of the data retention presented by the data controller, the EDPS considers that the retention of group reports for a period of two years complies with Article 4(1)(e) of the Regulation insofar as the group reports are kept in anonymous form.

### 3.5. Transfer of data

According to Article 7 of the Regulation, Personal data shall only be transferred within Community institutions or bodies if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient. As explained above, the individual report will be accessible only to the reviewee. As regards group reports, they will be provided to persons responsible within HR and Directors General, who will have access only to aggregated information about the compiled group results. In all these cases, the transfers appear necessary for the legitimate performance of the tasks covered by the given recipients.

In the analysis of the pilot project, the EDPS stressed that, in line with Article 7(3) of the Regulation, the recipients of the data should be reminded that they can only process the data for the purposes for which they were transmitted and not for any other purposes (such as the annual appraisal of the reviewee's performance at work).

The data controller implemented this recommendation. Indeed, all reviewers and reviewees are reminded in the invitation that the data will only be processed for the purposes for which they were transmitted: the reviewee's individual development.

Moreover, in line with Article 8 of the Regulation, personal data shall be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC *"(...) (b) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"*.

The necessity of having the data transferred is proven by the fact that if the personal data is not communicated to the provider of the web-test, Cubiks is not able to perform the tasks requested by the controller with the consent of the data subject. As to the legitimate interests of the data subject, compliance with the data quality principle, as well as with the obligations of the controller and the rights of the data subject, as described in the present Opinion, ensure that there is no reason to assume, in principle, that they might be prejudiced. Furthermore, data subjects have given their consent to the processing. As a consequence, there is no reason to believe that the transfer would affect the data subject's legitimate interests.

### 3.6. Right of access and rectification

Article 13 of the Regulation grants the data subject the right of access to personal data being processed. Article 14 of the Regulation provides a right to rectification without delay of inaccurate or incomplete data.

As explained above (point 3.3 on accuracy), the data subject has direct access to his/her individual 360° Leadership feedback report which will allow him/her to understand the data processed about him/her. Moreover, in accordance with the conditions set forth in Article 20 of the Regulation, the right of the data subject to access and rectify personal data relating to him/her may be limited in order to protect the rights and freedoms of others - in this case it is crucial that appropriate measures are implemented to prevent a reviewee from obtaining information revealing the identity of the persons who reviewed his/her skills so that he cannot exercise any retaliation against them, in particular for those reviewers that are in a subordinate position.

Moreover, the contractor has nevertheless to inform EIB that it has provided access and proceeded to rectify the data, if appropriate.

Furthermore, as regards the right of rectification, the EDPS points out that given the subjectivity involved in the feedback reports and the purpose that these reports are intended to serve, the room for rectification is relatively limited. For example, the person concerned providing feedback may later realize that he or she made a mistake in providing feedback. Therefore, a case-by-case analysis is recommended should there be a request for rectification.

### 3.7. Information to the data subject

Pursuant to Articles 11 and 12 of the Regulation, those who collect personal data are required to inform individuals that their data are being collected and processed unless the data subject already has this information. Individuals are further entitled to be informed of, inter alia, the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

In the pilot project's analysis, the EDPS recommended that all data subjects (i.e. reviewees and reviewers) were provided by the data controller with their own data protection notices containing all the specific pieces of information as required in Articles 11 and 12 of the Regulation.

He also stated that the EIB should establish a data protection notice specific to the pilot phase and provide it to all the relevant participants, which should moreover indicate that the processing is done in a pilot phase and the duration of the pilot phase. The EDPS also recommended that the voluntary nature of the participation in the pilot phase was clearly indicated to the participants, and in particular that there would be no consequences for the managers or experts and/or reviewers who did not want to participate in the 360° assessment.

As mentioned in the facts, the EIB implemented the recommendations and provided the EDPS with the content of the different information notices to reviewers and reviewees. The EDPS finds the documents adequate, and compliant with the requirements of the Regulation.

However, the EDPS reiterates the importance of the voluntary aspect of this exercise and the need to clearly inform the reviewees that no consequences will be attached either to the refusal to participate in the 360° assessment or to the transfer of the results to the superior.

### 3.8. Processing of personal data on behalf of controller

In the present case, the processing activity is mainly conducted by a processor, Cubiks, on behalf of the EIB. Article 23 of the Regulation stipulates that: *"1. Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures.*
*2. The carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
*(a) the processor shall act only on instructions from the controller;*
*(b) the obligations set out in Articles 21 and 22 shall also be incumbent on the processor unless, by virtue of Article 16 or Article 17(3), second indent, of Directive 95/46/EC, the processor is already subject to obligations with regard to confidentiality and security laid down in the national law of one of the Member States.*
*3. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form".*

The subcontractor (Cubiks) is the same for the procedure covering the evaluation 360° leadership feedback report as the one for the recruitment's procedure (EDPS ref n° 2009-0254). The EDPS received a copy of the draft contract with Cubiks, which confirm this.

The EDPS stresses that, although the entire processing is outsourced to a processor, the controller is responsible for ensuring that the obligations provided for in the Regulation are met (on information to be given to the data subject, ensuring the rights of the person concerned, the choice of processor, security and confidentiality of data, etc.).

The EDPS analysed the compliance with Article 23 in the prior-checking opinion on recruitment at the EIB (EDPS ref n° 2009-0254) and is satisfied with the measures taken as regards the way the data are handled by the subcontractor but reminds the EIB to ensure the compliance with the Regulation by the processor.

### 3.9. Security measures

According to Article 22 of the Regulation, *"the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected*". These security measures must *"in particular prevent any unauthorised disclosure or access,* accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing".

(...)

On the basis of the information available the EDPS does not see any indication to believe that EIB has not applied the security measures required in Articles 21, 22 and 23 of the Regulation.

**Conclusion:**

There is no reason to believe that there is a breach of the provisions of Regulation (EC) N° 45/2001 considering that the EIB confirmed to the EDPS that it has implemented the recommendations provided for in the analysis of the pilot project. These recommendations were the following:

- *The data controller should provide the EDPS with the conclusions adopted and with the modifications implemented in the 360° Leadership feedback tool and procedures at the end of the pilot phase and at the latest two months before the wider launch of the tool within EIB;*

- *In the present case of a data processing done on behalf of the data controller, the data controller should ensure that all the obligations provided for in the Regulation are met (information to be given to the data subject, ensuring the rights of the person concerned, security, etc.).*

- *To preserve the anonymity of participants, the data controller should ensure that, in case the number of participants is too reduced, no group report be generated. Furthermore, group reports should only be retained in anonymous form.*

- *The data controller should ensure that only data that are necessary for the processing are collected, and that no sensitive data in the sense of Article 10 of the Regulation are processed;*

- *The data controller should implement appropriate measures to prevent a reviewee from obtaining information revealing the identity of the persons who reviewed his/her skills;*

- *The data controller should remind all the recipients of the data that they can only process the data for the purposes for which they were transmitted;*

- *The data controller should provide all participants in the pilot phase with a specific data protection notice relating to the pilot project, as described above.*

The EDPS considers that the recommendations made in the analysis of the pilot project have been implemented by the EIB. Based on the foregoing, the EDPS considers that the follow-up of this opinion has been carried out and decides to close the case.

Done at Brussels, 20 July 2010

**(Signed)**

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor