GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr. Alberto SOUTO DE MIRANDA
Data Protection Officer
European Investment Bank
100, Boulevard Konrad Adenauer
L-2950 Luxembourg
LUXEMBOURG

Brussels, 17 April 2013
GB/MV/mk /D(2013)0746 **C 2013-0279**
Please use edps@edps.europa.eu for all correspondence

Subject: Consultation under Article 46(d) on the use of data collected for a specific purpose to a different purpose.

Dear Mr Souto de Miranda,

I thank you for your consultation on the use of data collected for a specific purpose to a different purpose at the European Investment Bank ("EIB").

Your consultation was covering three points, which are all connected on this aspect. Therefore, this reply will address them together.

1. Facts

In your consultation, you ask whether it is legal or not to use personal data collected for a specific purpose for an investigative purpose, in order to instruct a disciplinary process. You specifically mention the case of data originating from an access security system or from a time management system that would be used for investigative purpose, in order to instruct a disciplinary process at the EIB.

The EDPS prior checked processing operations on disciplinary procedure at the EIB. Specifically, regarding notifications for prior checking on investigative purposes received from the Data Protection Officer (DPO) of the EIB, the EDPS adopted:

- an Opinion on a notification regarding data processing in the framework of the disciplinary procedure on 25 July 2005 (C 2005-0102);
- an Opinion on a notification on procedures related to fraud investigations in the EIB Group (2009-0459) on 14 October 2010. Fraud investigations are relevant in this context as the result of fraud investigations could lead to disciplinary actions taken on initiative of the President of the EIB.

Please note however that, as indicated in our letter of 8 January 2013, the procedure on administrative investigations at the EIB has to date not been notified to the EDPS under Article 27 of Regulation (EC) 45/2001 (the Regulation).

In the context of these prior checking cases, the EDPS considered that the legal bases for these processing operations were sufficiently lawful in the light of Article 5 of the Regulation.

Regarding the use of certain data for a specific purpose, in the notification on disciplinary procedures, the EDPS stated that "*There are no systematic rules on the type of data which may be included in a disciplinary file. The nature of the data depends to a large extent on the case in question. That being the case, rules should be drawn up on the criteria to be applied before entering evidence or data in a disciplinary file in order to ensure that only relevant data are kept*".

Furthermore, on the case of fraud investigations, the EDPS stated that: "*As mentioned in the facts, in order to conduct an investigation, the IG/IN shall have full access to all relevant personnel, information, documents and data, including electronic data within the EIB. [...] It is not easy to define a priori the exact data which will be collected and further processed in an investigation procedure. Guarantees must be established in order to ensure the respect of the data quality principle. This could take the form of general recommendation to the persons handling the files recommending them to respect the principle of data quality*".

Finally, the EIB also states in its request that the purpose assigned on the "access control" notification was to protect individuals, equipment and sites from someone who is not authorised to enter the premises of the bank and that the purpose of "time management" notification was to manage, among others, presence/absence of staff.

2. Legal analysis

Personal data must be collected for specified, explicit and legitimate purposes (Article 4(1)(b) of the Regulation). Article 4 (1)(b) further provides that personal data must not be further processed in a way "incompatible" with the purposes for which they were initially collected. These requirements are normally referred to as the "purpose limitation principle".

Furthermore, Article 6 provides that personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by internal rules of the EU institution or body.

As regards a change of purpose of data which are collected for a specific purpose, the EDPS wants to stress, as stated in a recent paper by the Article 29 Working Party[1], that the concept of purpose limitation is an essential first step in applying data protection laws since it constitutes a pre-requisite for other data quality requirements including the adequacy, relevance, proportionality and accuracy of the data collected, along with the rules surrounding data retention periods. It contributes to transparency, legal certainty and predictability and aims to protect the data subjects by setting limits on how controllers are able to use their data. At the same time, it is also designed to offer some degree of flexibility for the controller.

[1] Opinion n. 03/2013 on purpose limitation, adopted on 2 April 2013, available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf*.

The principle of purpose limitation -which includes the notion of compatible use- requires that in each situation where further use is considered, a distinction be made between additional uses that are 'compatible', and other uses, which should remain 'incompatible'. The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other.

In the case at stake, from the analysis of the rules governing disciplinary procedures and fraud investigations at the EIB, these rules can be considered as allowing the use of any relevant types of data in the context of disciplinary investigations. Furthermore, the processing of the data stemming from the access security system or time management can be considered as compatible in the framework of disciplinary proceedings. Therefore, the further use of data from the access security system or from the time management system can be allowed in the context of disciplinary process opened by the EIB.

That being said, the authorisation must be understood restrictively. First of all, when a disciplinary process has started, the EIB should ensure that the proportionality and necessity of the processing is respected. Indeed, such access would not be necessary in all cases and the decision to access these data should be clearly evaluated and justified in terms of proportionality and necessity beforehand.

Furthermore, such possibility of re-use for another purpose should only be permitted in the specific context of an open disciplinary process for a specific case. As underlined in the prior checking Opinions on disciplinary procedure and anti-Fraud procedure mentioned above, the nature of the data used depends on the case in question and only that data which are relevant and necessary to the case under investigation may be processed.

It is important to underline that any further systematic or structured use of access security data or time management data in the context of administrative enquiries or disciplinary investigations would need to be based on a specific internal rule in compliance with Article 6.1 of the Regulation.

We hope that this answers your consultation and remain available for additional consultation.

Sincerely yours,

(**signed**)

Giovanni BUTTARELLI