**Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank on procedures related to fraud investigations in the EIB Group**

Brussels, 14 October 2010 (Case 2009-0459)

1. Proceedings

On 10 July 2009, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer (DPO) of the European Investment Bank (EIB) notification for prior checking regarding the data processing operations that take place in the context of procedures related to fraud investigations (the Notification) on the basis of Article 27 of Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (Regulation (EC) No 45/2001).

EDPS raised a series of questions to the DPO of the EIB:
- On 3 September 2009 (EIB answer on 8 September 2009)
- On 18 September 2009 (EIB answer on 28 September 2009 and on 7 December 2009 by phone)
- On 7 December 2009. The requested information was provided in June 2010:
    - On 4 June 2010, a meeting was held between the EDPS services and the Head of Division Fraud Investigations.
    - On 8 June 2010 further information was sent by the DPO of the EIB including a modified notification form.
    - On 14 June 2010 further information was sent by the controller to the EDPS.

On 15 June 2010, the EDPS sent a copy of the facts to the controller for validation. Comments were received on 17 June 2010.

On 6 July 2010, the EDPS sent the draft Opinion to EIB for comments. The EIB responded on 11 October 2010.

2. The facts

**Purpose and policy**. In accordance with the principles agreed by the International Financial Institutions (IFIs) Anti-Corruption Task Force and laid out in the Uniform Framework agreement, the EIB has established Procedures for the Conduct of Investigations by the Inspectorate General of the EIB Group (EIB and EIF). The procedures have been elaborated on the basis of the Bank's Staff Regulations and Code of Conduct.

Under the provisions of the Bank's Anti Fraud Policy as defined in the "Policy on preventing and deterring Corruption, Fraud, Collusion, Coercion, Money laundering and the Financing of

Terrorism in the EIB activities"[1] (hereinafter referred to as "the Policy"), EIB Group members of staff and EIB's Group business partners are required to maintain the highest level of integrity and efficiency in all EIB Group activities and operations (Article 6 of the Policy). Any prohibited practices that occur are to be reported promptly and investigated thoroughly and fairly; wrongdoers are to be sanctioned; and appropriate legal steps are to be taken to recover misapplied funds (Article 7 (i) of the Policy). The purpose of the notified processing operation is precisely to investigate credible allegations of fraudulent practices[2] in EIB-financed operations.

The Bank's Inspectorate General (IG) and more specifically the Fraud Investigation Division (IG/IN) investigates allegations of prohibited practices in accordance with the EIB "Procedures for the Conduct of Investigations by the Inspectorate General of the EIB Group" adopted on 8 April 2008 (hereinafter "Anti Fraud procedures"). All activities related to Fraud Investigations are performed under the overall responsibility of the Inspector General by the Fraud Investigation Team.

**Activities covered**. The Policy applies to all EIB activities, including EIB-financed projects implemented on behalf of other bodies within or outside the EU. It applies to a) the Board of Directors, the Management Committee, members of staff and consultants; b) all borrowers, promoters, contractors, suppliers, beneficiaries and any other person or entity involved in EIB-financed activities and c) all counterparties and others through which the EIB deals in its borrowing or treasury activities (Article 8).

**Reporting procedures**. Under the Policy and the Staff code of conduct, EIB staff members are obliged to report any suspicion or allegation of prohibited practices, money laundering or terrorist financing that involve EIB activities, operations, members of staff or business partners immediately after becoming aware of the matter (Article 26). Under the terms of EIB finance contracts, borrowers are subject to the same obligations and promoters must immediately inform the EIB of any written complaint that it receives from a tenderer during the tender application procedure and under the Covenant of Integrity, tenderers, contractors, suppliers and consultants must report to the promoter any prohibited practice that comes to the attention of any person in their organization (article 27).

A Contact Point has been set up within the EIB for the purpose of reporting such allegations: a specific mailbox, fax machine and telephone line with access strictly limited to the Head of Division has been created to this effect. The Head of Division checks on a daily basis the incoming mail. In his absence, provision is made for another member of the Division to ensure checking all incoming mail.

If the incoming information relates to an already existing case, the information is forwarded to the relevant case in the case management system of the division, where it can be accessed by the appointed investigator.

If the information is new, and

a) is not of the competence of IG/IN, its is forwarded to another competent division in the EIB if appropriate
b) is of the competence of IG/IN, the head of division registers it as new incoming information in the case management system and appoints an investigator to evaluate the information.

[1] Adopted on 8 April 2008. This policy will be reviewed in 2011

[2] A "fraudulent practice" is defined by the Policy as "any act or omission, including a misrepresentation that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation (Article 9.b).

In all cases an acknowledgement of receipt is sent to the source.

Information may also be received by telephone directly to the Head of the anti-fraud division or by the fax-machine only available to the Fraud investigations division and placed in the office of the Head of the division. If information is received by fax or telephone, the same procedures as above applies.

**Investigations.** IG/IN shall accept reports of suspected fraud from any source within or outside the EIB, including complaints from anonymous or confidential sources. IG/IN may also open cases on its own initiative. To the extent possible, the IG/IN should contact the complainant to acknowledge receipt of the complaint and to obtain as much other information concerning the allegation as possible such as for example a complete description of the alleged wrongdoing; the alleged connection to the EIB's financing activities; the names and locations of the persons or entities involved; the names and locations of other persons who may have information regarding the alleged misconduct and be willing to provide it to IG/IN and the basis for the complainant's knowledge. If the complainant is anonymous or insists on anonymity, IG/IN should request that he or she contact IG/IN again at an agreed date and time in the future to respond to possible further questions based on the results of the initial review.

After receipt of a complaint the IG/IN will seek to confirm that the alleged wrongdoing involves an EIB operation or a member of staff and if so whether the alleged misconduct represents either a sufficient material risk to the EIB or is of sufficient public interest to justify an investigation and the investigation is feasible based on certain defined criteria such as the specificity of the information received. The IG/IN should evaluate the reliability of the complaint. Based on this evaluation, the Head of IG/IN will decide whether to open a case. After opening a case, IG/IN shall promptly notify OLAF and provide it with necessary information. OLAF may, at the invitation of the IG/IN or on its own initiative, participate in or take the lead in any investigation including those inside the EIB[3]. A decision to that effect has been signed by the Board of Directors of the EIB.

If the Head of IG/IN decides not to open a case, he shall record the decision in the case management system. He shall make information regarding the allegation and its evaluation available upon request to appropriate parties, including the President and the Vice President responsible for investigations, the Secretary General, the Audit Committee, OLAF and the external auditors.

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 (Article 37 of the Anti Fraud Policy). In so far as provided in the applicable EIB financed contracts, IG/IN shall have the right to examine and copy the relevant books and records of the project promoters, borrowers, contractors, suppliers and other involved parties (Article 38 of the Anti Fraud Policy). Each EIB finance contract has a standard visiting and information clause, giving the Bank the right to inspect the books of the borrowers and the project financed involving EIB funds. Concerning staff members, according to the Notification, by standard practice both the HR Director and the DPO are notified by email prior to the accessing of personal data.

Sources of information for an investigation shall include, but not be limited to documents of any type, electronic data, video, audio and photographic data, the results of inspections and tests, the investigator's observations and information provided by witnesses (orally or in writing) (point 14 of the Anti Fraud procedures). With regard to electronic data, the Anti Fraud procedure also establishes that "with the approval of the Director of the Department of Human Resources, and

[3] For processing of personal data by OLAF see EDPS prior checking opinions 2005-418, 2007-050 and 2007-073

in accordance with applicable laws, rules, regulations, policies and procedures, IG/IN may access and copy potentially relevant electronic data and email created, copied or received by an EIB member of staff using the EIB IT system" (point 19).

No interception of communications and conversations is permitted.

As regards all interviews conducted by IG/IN, both within and outside EIB, including interviews of the subject of the investigation shall be reported in a written record. The IG/IN may in at its discretion, provide a copy of the record of the interview for the witnesses to review, or to review and sign; and interviews may be recorded electronically, with the knowledge and consent of the witness (point 21 of the Anti Fraud procedures). In accordance with the Policy (Articles 41 and 42), a staff member who is the subject of an investigation shall be entitled to due process rights, in particular to be notified of that fact as early as possible, unless it is determined that to do so would be harmful to the investigation. In any event, a staff member who is the subject of an investigation shall be given notice of the allegations and evidence against him or her, and the opportunity to respond before any adverse decision is taken.

According to point 24 of the Anti Fraud procedures the findings of an investigation shall be based on the most reliable factual information available and reasonable inferences and conclusions drawn from established facts. To the extent feasible, documents, electronic data, or tests and inspection results shall be authenticated as accurate by their authors, recipients, or by other persons with direct knowledge of their authenticity. Information should be corroborated to the extent possible by other reliable sources, including other witnesses, documents or data. Findings should be based on credible exculpatory as well as inculpatory information. Investigative findings may include IG/IN's comments on the perceived credibility and behavior of a witness, including the subject of the investigation.

**Outcome of an investigation**. Where the Head of IG/IN determines that a complaint or allegation has been substantiated, the findings shall be documented in a note to the file and referred to the relevant authorities within and/or outside the EIB for appropriate action. As concerns staff members, the President shall decide the appropriate and proportionate disciplinary actions, in accordance with the Staff Regulations. If a member of the Bank's governing bodies is implicated, the President, or, as appropriate, the Audit Committee, shall inform the competent decision making body of the Bank. IG/IN may refer a matter to the appropriate national authorities for further investigation or criminal prosecution. This will be done in consultation with or with the assistance of OLAF.

If, after reasonable investigation, IG/IN determines that a complaint or allegation has not been substantiated, it shall document the findings in a note to the file and close the case. IG/IN may re-open a case that has been closed if credible information is received or if it is warranted by other circumstances.

**Transmission of information**. IG/IN shall distribute the note to the file for all substantiated and unsubstantiated cases simultaneously to the President and Vice President responsible for the investigations, the Vice President responsible for the affected business area, the Secretary General, and the Audit Committee. In addition, IG/IN shall submit a status report of all cases in which at least an initial evaluation was done ten times annually for information to the Audit Committee, the External Auditors, OLAF, the President and Vice Presidents concerned. This report is also submitted at least five times annually to the Management Committee. The Status report does not identify persons subject to investigation. The Management Committee is also informed by the Inspector General what follow-up measures are to be taken by the Operational Departments, including loan cancellation and early repayment.

Respecting the EIB's rules and procedures governing the disclosure of information, IG/IN may provide assistance to and share its findings and/or relevant information with other International Financial Institutions.

**Retention periods**. According to the Anti Fraud Procedure, all documentation and information for opened and unopened, substantiated and unsubstantiated cases shall be kept in a secure and confidential manner by the IG/IN and shall be retained for at least five years. According to the notification received however, the paper and electronic files are to be destroyed / deleted 10 years after a case has been closed whether or not the enquiry reveals a fraudulent practice.

**Security.** [...]

## 3. Legal Aspects

### 3.1. Prior checking

Applicability of the Regulation. Regulation (EC) No 45/2001 applies to the "processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system" and to the processing "by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part or which fall within the scope of Community law"[4]. For the reasons described below, all elements that trigger the application of the Regulation are present here:

First, fraud investigations entail the collection and further processing of personal data as defined under Article 2(a) of Regulation (EC) No 45/2001. Second, the personal data collected undergo "automatic processing" operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001 as well as manual data processing operations. Finally, the processing is carried out by a former "Community" institution, in this case by the EIB, in the framework of former "Community law" activities (Article 3(1) of the Regulation (EC) No 45/2001).

Grounds for Prior Checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS "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 list of processing operations that are likely to present such risks. This list includes, under paragraph (b), the processing operations intended to evaluate personal aspects related to the data subject, including his or her ability, efficiency and conduct. Obviously fraud investigations intend to evaluate the conduct or reliability of persons and therefore qualify for prior checking. Furthermore, Article 27(2)(a) stipulates that processing operations relating to "suspected offences, offences, criminal convictions or security measures" shall be subject to prior checking. In the case at hand, the processing operation could be related to such type of data.

Prior Checking. 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 operations have already been established. This is not a problem provided that all recommendations made by the EDPS will be fully taken into account.

As concerns staff members of the EIB Group, the fraud investigations could lead to disciplinary actions taken on initiative of the President of the EIB. This prior check does not cover the

[4] See Article 3 of Regulation (EC) No 45/2001.

processing of personal data in the frame of any disciplinary procedure based on an investigation on fraud[5]. Neither does this opinion cover procedures linked to whistleblowing.

Notification and Due Date for the EDPS Opinion. The Notification was received on 10 July 2009. The period within which the EDPS must deliver an opinion was suspended for a total of 369 days (plus the month of August 2009) to allow for comments on the draft EDPS Opinion. The Opinion must therefore be adopted no later than 15 October 2010.

### 3.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. The grounds that justify the processing operation are based on Article 5(a), pursuant to which data may be processed if 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".

In order to determine whether the processing operations comply with Article 5(a), two elements must be taken into account: first, whether either the Treaty or another legal instrument adopted on the basis thereof foresee a public task in this context, and second, whether the processing operations carried out by the data controllers are indeed necessary for the performance of that task.

The procedures established at the EIB to combat fraud are based on principles agreed by the IFIs Anti-Corruption Task Force and laid out in the Uniform Framework agreement, signed in Singapore in September 2006[6]. On the basis of the Bank's Staff Regulations and Code of Conduct, the EIB has established Procedures for the Conduct of Investigations by the Inspectorate General of the EIB Group. These are provided for in the Bank's Anti Fraud Policy as defined in the "Policy on preventing and deterring Corruption, Fraud, Collusion, Coercion, Money laundering and the Financing of Terrorism in the EIB activities" and in the "Procedures for the Conduct of Investigations by the Inspectorate General of the EIB Group" adopted on 8 April 2008.

To comply with Article 5 of the Regulation, these instruments should be considered as "legal instruments adopted on the basis of the Treaty or other legal act adopted on the basis thereof". The EDPS therefore invites the EIB to examine to which extent the instruments mentioned above find their legal basis in the mandate of the EIB as established by the Treaties or other legal instruments adopted on the basis thereof.

The purpose of an investigation by IG/IN is to examine and determine the veracity of allegations and suspicions of prohibited practices affecting EIB activities or involving members of staff. The "necessity" of the processing has to be analysed *in concreto*. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the investigations has to be proportional to the general purpose of processing and to the particular purpose of processing in the context of the case under analysis (considering, for instance, the seriousness of the fact under investigation, the sort of data needed to clarify the facts, etc.). Thus, the proportionality has to be evaluated on a case-by-case basis, also with regard to the principle of confidentiality of communications involved and the need that any restriction to this principle must therefore be in accordance with the general principles of Community law.

[5] The processing of personal data in the frame of disciplinary investigations at the EIB has been the object of a separate prior check adopted by the EDPS on 25 July 2005 (2005-0102)

[6] http://www.eib.org/attachments/general/uniform_framework_en.pdf

### 3.3. Processing of Special Categories of Data

Article 10.1 of Regulation 45/2001 establishes that "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of data concerning health or sex life, are prohibited". The prohibition is lifted notably if grounds can be found in Articles 10(2) and 10(4) of the Regulation.

Article 10(2)(b) provides that the prohibition shall not apply if the processing is necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the Treaties establishing the European Union or other legal instruments adopted on the basis thereof. In principle the EIB should not need to process such data in the frame of fraud investigations, yet this cannot be excluded.

Concerning persons employed at the EIB this processing could be based on obligations in the field of employment law based on the instruments mentioned above (section 3.2). Indeed, according to the EIB Rules the EIB Group members of staff are required to maintain the highest level of integrity and efficiency in all EIB group activities and operations. To this end, the EIB has a legal obligation to verify the respect of this obligation. To the extent necessary, this provision could serve to justify the processing of sensitive data.

If necessary, the processing of special categories of data concerning persons not employed at the EIB can be based on article 10§4 on the basis of reasons of "substantial public interest" on the basis of a legal instrument adopted on the basis of the Treaties providing appropriate safeguards are put into place concerning the protection of personal data.

Article 10§5 stipulates that "[p]rocessing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor." In the present case, processing of the mentioned data is authorised by the legal instruments mentioned in Section 3.2 above.

### 3.4. Data Quality

Adequacy, Relevance and Proportionality. According to Article 4(1)(c) of Regulation 45/2001 "personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

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. In so far as provided in the applicable EIB financed contracts, IG/IN shall have the right to examine and copy the relevant books and records of the project promoters, borrowers, contractors, suppliers and other involved parties. 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.

The principle of data quality is also of relevance in the processing involved in forensic examinations of computers. As mentioned above in the facts, with regard to electronic data, the Anti Fraud procedures establish that "with the approval of the Director of the Department of Human Resources, and in accordance with applicable laws, rules, regulations, policies and procedures, IG/IN may access and copy potentially relevant electronic data and email created, copied or received by an EIB member of staff using the EIB IT system" (point 19). The IT Security Policy also provides that "the IT Department will act only under the instruction of, or

with the explicit approval of the HR Director or the Data Protection Officer or the Bank's Inspector General" (Article 2.3.9) . However in the answers received from further questions submitted to the EIB, it was explained that there are no specific rules as concerns computer forensics and that forensic tools are applied very widely in accordance with the case concerned.

The EDPS welcomes the existence of particular authorization mechanisms to allow the conduction of such computer forensic examinations. Precautions should also be taken regarding the access to the contents of a computer belonging to an institution or body since it may also contain files used by the data subject for private purposes (for instance in the folder "My documents", or e-mails marked as "private"), or files not relevant or excessive for the purposes of the investigation. In this regard, the EDPS recommends that whenever the access to files that are apparently of a private nature appears to be necessary for the investigation, this access be conducted respecting adequate guarantees, and considering any potential risk of inadmissibility of the evidence in a possible future court case that could arise if the fundamental rights to privacy and personal data protection are not respected in the collection of evidence (see Section 3.9 below). Furthermore, the EDPS recommends the adoption of a formal protocol for the conduction of computer forensics investigations by the EIB, which will also contribute to the safeguard of the data quality principle.

Article 4(1)(d) provides that personal data must be "accurate and, where necessary, kept up to date". Although the EDPS underlines the difficulty of speaking of "accurate" information as concerns subjective evaluation data, he welcomes the fact that a series of precautions are put into place in order to ensure the accuracy of factual information. Indeed as mentioned above, according to point 24 of the Anti Fraud procedures, the findings of an investigation shall be based on the most reliable factual information available and reasonable inferences and conclusions drawn from established facts. To the extent feasible, documents, electronic data, or tests and inspection results shall be authenticated as accurate by their authors, recipients, or by other persons with direct knowledge of their authenticity. Information should be corroborated to the extent possible by other reliable sources, including other witnesses, documents or data. Findings should be based on credible exculpatory as well as inculpatory information. Investigative findings may include IG/IN's comments on the perceived credibility and behavior of a witness, including the subject of the investigation. It is also important for the data subject to be able to exercise the right of access and rectification insofar as it enables individuals to control whether the data held about them is accurate (see Section 3.7).

Fairness and Lawfulness. Article 4(1)(a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analyzed above (see Section 3.2). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 3.8.

It has to be noted that complaints submitted by anonymous or confidential sources raise a specific problem with regard to the essential requirements that personal data should be collected fairly. The EDPS is aware that some complainants may not always be in a position or have the psychological disposition to file identified reports. Nevertheless, the EDPS considers that complaint schemes should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint.[7]

### 3.5. Conservation of Data

[7] See, in the same line, Article 29 data Protection Working Party, Opinion 1/2006 on the application of the EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auding matters, fight against bribery, banking and financial crime, WP 117, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

According to the Anti Fraud Procedure, all documentation and information for opened and unopened, substantiated and unsubstantiated cases shall be kept in a secure and confidential manner by the IG/IN and shall be retained for at least five years. According to the notification received, the paper and electronic files to be destroyed / deleted 10 years after a case has been closed whether or not the enquiry reveals a fraudulent practice.

The EDPS underlines the need to harmonize the conservation periods and to fully assess the necessity to keep data relating to fraud investigations for up to 10 years. Furthermore, the EIB should examine to what extent it is necessary to keep data for such long periods if the Head of IG/IN decides not to open a case or if after an investigation, IG/IN determines that a complaint or allegation has not been substantiated and decides to close the case.

### 3.6. Transfers of Data

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. As concerns transfers to European Union institutions or bodies, Article 7.1 establishes that data shall only be transferred if the data are necessary for the legitimate performance of the tasks covered by the competence of the recipient.

As mentioned in the facts above, if the Head of IG/IN decides not to open a case, he shall make information regarding the allegation and its evaluation available upon request to appropriate parties, including the President and the Vice President responsible for investigations, the Secretary General, the Audit Committee, OLAF and the external auditors. The EDPS underlines that should one of the persons or bodies listed request such data, the request must be examined in the light of Article 7 or 8 of Regulation (EC) No 45/2001. This notably implies the verification of the necessity of the transfer.

Also mentioned in the Notification, is the fact that IG/IN shall distribute the note to the file for all substantiated and unsubstantiated cases simultaneously to the President and Vice President responsible for the investigations, the Vice President responsible for the affected business area, the Secretary General and the Audit Committee.

In addition, IG/IN shall submit a status report of all cases in which at least an initial evaluation was done ten times annually for information to the Audit Committee, the External Auditors, OLAF, the President and Vice Presidents concerned. This report is also submitted at least five times annually to the Management Committee. The EDPS is satisfied that these status reports do not identify the persons under investigation.

Article 7(3) states that "*The recipient shall process the personal data only for the purposes for which they are transmitted*". The EDPS underlines that at all stages of the procedure, the recipients to whom the data are transferred must be reminded that they can only process the data for the purposes of fraud investigations.

As mentioned above, IG/IN may refer a matter to the appropriate national authorities for further investigation and/or criminal prosecution. Two scenarios can be observed in Member States: (a) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC covers every sector of the national legal system,

including the judicial sector; and (b) those Member States where the national data protection law adopted for the implementation of Directive 95/46/EC does not cover every sector, and particularly, not the judicial sector.

As to the first scenario, Article 8 of the Regulation foresees: *"Without prejudice to Articles 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, (...)."*

Even if judicial authorities do not fall within the scope of application of Directive 95/46/EC, a Member State may, when transposing Directive 95/46/EC into internal law, extend its application to these public authorities. In these cases, Article 8 of the Regulation has to be taken into account. As to the specific wording of Article 8 of the Regulation ("... if the recipient establishes..."), as data are not required by the recipient, but it is the EIB who decides unilaterally on the transfer, it flows from EIB rules on fraud investigation procedures that EIB has to establish the "necessity" of the transfer in a reasoned decision in this regard.

For those countries that have not extended their implementation of Directive 95/46/EC to judicial authorities, Article 9 of the Regulation has to be considered[8].

According to the notification, IG/IN may also provide assistance to and share its findings and/or relevant information with other Financial Institutions. Should these Financial Institutions be based in third countries, Article 9 of the Regulation will apply. According to Article 9, "*Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive (EC) 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out."*

In light of Article 9.2 of the Regulation (as well as Article 25.2 of Directive 95/46), the controller should assess all the circumstances surrounding a data transfer or set of data transfer operations. The analysis has to be conducted *in concreto*, taking into account the specific characteristics (guarantees and/or risks) of the transfer or set of transfers in question. This assessment would come to a conclusion as to the existing level of protection regarding a specific transfer or set of transfers, and would be limited to the purposes taken into account by the data controller and the recipients in the country of destination. In that case, the controller would assume the responsibility of verifying whether the conditions for adequacy are present. When the analysis is done by the data controller, the conclusion would be subject to the supervision of the data protection authority.

An assessment of the adequacy of the protection afforded to data protection should therefore be carried out. Such an assessment should entail a review of the national law that applies to the financial institution and its effective implementation. The assessment should be subject to the supervision of the EDPS.

Failing an adequate level of protection, Article 9(6)(d) provides that the Community institution or body may transfer personal data if "*the transfer is necessary or legally required on important public interest grounds*". On the basis of this provision, the EIB may only transfer personal data relating to fraud investigations to international organizations, such as Financial Institutions in a third country if this transfer is deemed necessary on important public grounds. These transfers may not be done

[8] Council of Europe Convention 108 could be considered as providing an adequate level of protection for the matter under analysis in those countries where it is applicable to judicial authorities

on a systematic basis and a case by case examination will need to be carried out before the transfer takes place in order to assess the interests at stake and the necessity of the transfer[9].

Furthermore according to Article 9.7 of the Regulation, *"[w]ithout prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses"*.

The application of this rule would result only in the authorization by the EDPS of the stream for a specific case ("transfer" or "set of transfers") on the basis of what has been adduced by the data controller. Thus, the controller has to present sufficient evidence supporting the adoption of adequate safeguards in the specific case, even if the country of destination is not adequate as such. The "adequate safeguards" are then created ad hoc.

The EDPS therefore recommends that the EIB ensure compliance with Article 9 of Regulation (EC) 45/2001.

### 3.7. Right of Access and Rectification

According to Article 13 of Regulation (EC) 45/2001, the data subject shall have the right to have confirmation as to whether data related to him/her are being processed; information at least as to the purposes of the processing operation, the categories of data concerned, and recipients or categories of recipients to whom data are disclosed; communication in an intelligible form of data undergoing a processing operation and any available information as to their source and knowledge of the logic involved in any automated decision process concerning him or her.

The right of access concerns not only the person under investigation, but any other person whose personal data is being processed in the frame of an investigation and who request access to data relating to them included in an investigation relating to another person (witness, investigator, informant...).

As concerns persons subject to an investigation, the Policy (Articles 41 and 42) provides that a staff member who is the subject of an investigation shall be entitled to due process rights, in particular to be notified of that fact as early as possible, unless it is determined that to do so would be harmful to the investigation. In any event, a staff member who is the subject of an investigation shall be given notice of the allegations and evidence against him or her, and the opportunity to respond before any adverse decision is taken.

Article 20 of the Regulation provides for certain restrictions to this right notably where such a restriction constitutes a necessary measure to safeguard *"(a) the prevention, investigation, detection and prosecution of criminal offences; (b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters; (c) the protection of the data subject or of the rights and freedoms of others"*. Moreover, in certain cases it may be necessary not to give direct access to the data subject so as not to harm the proper functioning of the inquiry even though it is not a criminal investigation within the meaning of Article 20 of Regulation (EC) No 45/2001, but a pre-disciplinary or pre-criminal investigation. The EDPS considers that Article 20 must take

[9] As to Article 26.1 of Directive (EC) 95/46 and the interpretation by analogy of Article 9.6, see: Article 29 Data Protection Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC, WP114, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

account of the *ratio legis* of the provision and must allow for restrictions on the obligation to provide direct access during a pre-disciplinary or pre-criminal investigation.

In the context of the right of access to data processed in the frame of fraud investigations, therefore it has to be borne in mind that the restrictions to a fundamental right cannot be applied systematically. Indeed, as foreseen in Article 20 of the Regulation, the measure has to be "necessary". This requires that the "necessity test" has to be conducted on a case-by-case basis, and as well as the right of information, the right of access and rectification will have to be provided "*as long as this would not be harmful to the investigation"*.

As concerns persons not under investigations, according to the Anti Fraud procedures (Article 21) the IG/IN may at its discretion, provide a copy of the record of the interviews conducted by the IG/IN, both inside and outside the EIB, for the witnesses to review, or to review and sign. The EDPS considers that access to the records of the interviews should be granted to the persons concerned as a right and that the IG/IN may only restrict this right on the basis of the grounds provided in Article 20 of Regulation (EC) 45/2001 which is to be interpreted restrictively. Access rights should be granted as concerns the interviews themselves, but also as concerns any other documents containing personal data processed in the frame of an investigation. The EDPS therefore recommends that the access be granted as a rule to interviews and any other documents containing personal data relating to these other parties, with possible restrictions on the grounds of Article 20 applied on a case by case basis.

In any case, paragraph 3 of Article 20 has to be considered and respected by the EIB: *"If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his right to have recourse to the European Data Protection Supervisor."* Concerning the right to information, this provision has to be read jointly with Articles 11, 12 and 20 of the Regulation (see below point 3.8).

Moreover, account should also be taken of paragraph 4 of Article 20: *"If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Supervisor shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether the necessary corrections have been made."* The indirect right of access will then have to be guaranteed. Indeed, this provision will play a role, for instance, in those cases where the data subject has been informed about the existence of the process, or has knowledge of it, but the right of access is still being restricted in light of Article 20.

Paragraph 5 of Article 20 establishes that *"Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect."* It may be necessary for the EIB to defer such information in accordance with this provision, in order to safeguard the investigation. The necessity of such deferral must be decided on a case-by-case basis.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the sensitivity, in most cases, of the investigations conducted, this right is of key importance, in order to guarantee the quality of the data used, which, in this specific case, is connected to the right of defense. Any restriction, as provided in Article 20 of the Regulation, has to be applied in light of what has been said regarding the right of access in the paragraphs above. Rules must also be established to the effect that at the moment an investigation is closed, the staff member under investigation can rectify any data relating to him or her by requesting the inclusion in the investigation file of documentation related to any subsequent developments during the follow-up phase of the case (a decision by the Court ruling otherwise, for instance).

The EDPS therefore requests the EIB to ensure the respect of rectification rights for the data subject.

### 3.8. Information to the Data Subject

The Regulation states that the data subject must be informed where his or her personal data are being collected and lists a number of points to be included in the information, in order to ensure the fairness of the processing of personal data. In the case at hand, the data could be collected directly from the data subject and could also be collected indirectly, for instance, through informants.

The provisions of Article 11 of the Regulation (*Information to be supplied where the data have been obtained from the data subject*) and Article 12 (*Information to be supplied where the data have not been obtained from the data subject*) are thus both applicable to the present case. This means that the relevant information must be given, either at the time of collection (Article 11), or when the data are first recorded or disclosed (Article 12), unless the data subject already has it. The latter may be the case, *inter alia*, if the same information has been given before.

Staff members at the EIB and any other persons who may be subject to an investigation on fraud should be informed of the processing of personal data in a fraud investigation procedure in general. The information should cover the items listed in Articles 11 and 12. Furthermore, should a person be specifically involved in a fraud investigation case whether as suspect or as witness or other, the principle of fair processing implies that he or she should also be informed of the opening of an investigation and of the processing of personal data which results from this procedure unless the restrictions of Article 20 apply as described above (3.7 Right of Access and Rectification).

The EDPS notes that no information has been provided to staff or to any persons potentially likely to be subject to a fraud investigation and therefore requests that the EIB provide general information in compliance with Articles 11 and 12. This information could be provided on the intranet, internet and/or in contracts signed with EIB contractors. Furthermore should an investigation be opened, specific information must be given to data subjects concerned unless restrictions apply in accordance with Article 20. This must be examined on a case by case basis. Information should also be provided on an ex-post basis to persons who have already been subject to an investigation procedure unless restrictions founded on Article 20 apply.

### 3.9. Confidentiality of communications

As mentioned in the facts, IG/IN can collect electronic data and the Anti Fraud Procedures provide that "with the approval of the Director of the Department of Human Resources, and in accordance with applicable laws, rules, regulations, policies and procedures, IG/IN may access and copy potentially relevant electronic data and email created, copied or received by an EIB member of staff using the EIB IT system" (point 19). Although according to the notification and further information received, in principle the IG/IN only collect data concerning the professional history contained in the CV provided when applying to the Bank, one cannot exclude access to further data including electronic data as foreseen by the Anti Fraud Procedures and notably the content of an electronic communication or to traffic data surrounding this communication.

Under Article 36 of Regulation 45/2001, *"Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law"*. Any restriction of the confidentiality principle must therefore be *"in accordance with the general principles of Community law"*.

The collection of evidence concerning electronic communications must be qualified as interference in the privacy of communications and may hence imply the violation of the confidentiality of communications[10].

The concept of *"general principles of Community law"* refers to the fundamental human rights enshrined in particular in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights which is binding to EU institutions and bodies according to Article 6(1) TEU. In particular, Article 8 (2) of ECHR sets four criteria to be examined before the principle of confidentiality is restricted:

- Is the restriction authorised by a legal provision or equivalent measure?

- Is it necessary? Could the same result be obtained without breaching the principle of confidentiality? It would only be in exceptional circumstances that the monitoring of a staff member's personal use of the e-mail (apart from scanning viruses) or telephone would be considered as necessary.

- Is it proportionate to the concerns it tries to ally? The principle of proportionality implies that the application of the restrictions to the confidentiality of communications will be different if we are in the case of personal communications or business communications. It also implies that if it is necessary to check the e-mail accounts of workers in their absence, this should in principle be limited to e-mails that are not marked as private or personal or that are addressed to the address of the institution.

- Have all other intrusive means of investigation been exhausted?

In practice, this means that any restriction on the principle of confidentiality of communications must be consistent with the fundamental human rights enshrined in the European Convention on Human Rights and the EU Charter of Fundamental Rights. Such restriction may take place only if it is *"in accordance with the law"* and *"is necessary in a democratic society"* in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The EDPS consequently stresses that the confidentiality of communications can be infringed only in exceptional circumstances (in the course of a fraud investigation, where no other less invasive method could be used), that infringing the confidentiality principle should be an extraordinary procedure and that it must always be restricted to those data which are strictly necessary.

As already mentioned above, the EDPS considers that a methodology should be developed in a systematic and formal fashion, and recommends the adoption of a formal procedure and policy for the performance of computer forensic investigations by the IG/IN, that will contribute to safeguard the confidentiality of communications, as well as to preserve the validity of the evidence.

[10] A breach of confidentiality of communications is defined in article 5 of Directive 2008/977/JHA as any "listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the persons concerned except when legally authorised to do so in accordance with Article 15(1)".

It has been made clear on the other hand, that the EIB does not envisage any interception or tapping of communications during the communication in the frame of fraud investigations whether this be oral (audio/video) conversations or other automated communications.

### 3.10 Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement the appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

[...]

## 4. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, the EIB must:

- Examine to which extent the instruments mentioned above find their legal basis in the mandate of the EIB as established by the Treaties or other legal instruments adopted on the basis thereof;
- establish guarantees 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;
- adopt a formal protocol for the conduction of computer forensics investigations by the EIB;
- harmonize the conservation periods and fully assess the necessity to keep data relating to fraud investigations for up to 10 years;
- examine to what extent it is necessary to keep data for 10 years if the Head of IG/IN decides not to open a case or if after an investigation, IG/IN determines that a complaint or allegation has not been substantiated and decides to close the case;
- ensure compliance with the principles set out in Article 9 of Regulation (EC) 45/2001 as explained above;
- as a rule provides access to interviews and any other documents containing personal data relating to these other parties, with possible restrictions on the grounds of Article 20 applied on a case by case basis;
- ensure respect of the right of rectification for data subjects;
- provide information to data subjects in compliance with Regulation (EC) 45/2001;
- define or confirm the business owner of the IT systems as belonging to the Fraud Investigation Division;
- [...]

Done at Brussels, 14 October 2010

(**signed**)

Giovanni BUTTARELLI