

REGISTER NUMBER: 289
NOTIFICATION FOR PRIOR CHECKING
<p>Date of submission: 05/09/2007 and modified 17/03/2008</p> <p>Case number: 2007-543</p> <p>Institution: European Investment Bank</p> <p>Legal basis: article 27-5 of the regulation CE 45/2001 (1)</p> <p style="text-align: right;">(1) OJ L 8, 12.01.2001</p>

INFORMATION TO BE GIVEN⁽²⁾
<i>(2) Please attach all necessary backup documents</i>
<p>1/ Name and address of the controller European Investment Bank (E.I.B) 100 Bld Konrad Adenauer L- 2950 Luxembourg</p>
<p>2/ Organisational parts of the institution or body entrusted with the processing of personal data Office of the Chief Compliance Officer (OCCO)</p>
<p>3/ Name of the processing Recording and storage of documents (notes and emails) including opinions on EIB operations and associated documents both internal and external, and results of integrity checks, i.e. verification of the reputation of individuals (essentially through internet searches) and control of whether such individuals are listed on any sanction list (and especially on the EU sanction lists). Compilation of lists with "politically exposed persons" (PEP) associated with EIB operations so as to carry out the monitoring of such persons pursuant to Article 8 d. and especially Article 13.4.d of Directive 2005/60/EC requiring financial institutions to "conduct enhanced ongoing monitoring of the business relationship" with politically exposed persons and taking into account the definition of PEPs given in Directive 2006/70/EC</p>
<p>4/ Purpose or purposes of the processing The purpose is to create a record of precedents with a view to ensuring consistency of the opinions issued by OCCO and to "conduct enhanced ongoing monitoring of the business relationship" with the PEP, pursuant to article 13.4.d of Directive 2005/60/EC.</p>
<p>5/ Description of the category or categories of data subjects Individuals and bodies corporate likely to be either direct recipients or final beneficiaries of EIB's lending operations or direct participants in a lending, borrowing, treasury or investment operation carried out by EIB.</p>
<p>6/ Description of the data or categories of data (including, if applicable, special categories of data (article 10) and/or origin of data) Data will routinely include: Nationality Listing on UN, EU or other sanction lists Criminal convictions Professional and/or economic activities Reference to press allegations of corruption, money laundering, terrorism financing or any other illegal activity. Mention of official activities justifying the classification of the person as PEP The list of PEPs associated with EIB operations will include: Name of the person Project name and reference number (in project database) of the project which this person is associated with. NB. Most data stored are collected from the public domain.</p>

7/ Information to be given to data subjects

In accordance with the principle contained in Chapter III Section 2 "Prohibition of disclosure", Article 28 (1) of Directive 2005/60/EC, the EIB may not disclose to the individuals or companies whose reputation or record is verified through the integrity checks carried out by the EIB that information has been transmitted in accordance with Articles 22 and 23 of the abovementioned Directive, or that an investigation "is being or may be carried out". The purpose of the exercise is to protect EIB from any direct or indirect involvement with money launderers, terrorism financing individuals or organisations, and more generally convicted criminals or persons whose association with the bank could expose EIB to reputational risk. In deciding whether to grant information to data subjects, the EIB therefore has to take into account the provisions of Directive 2005/60/EC and Regulation 45/2001/EC. In particular, information to the data subject may be restricted in some cases pursuant to Article 20 (1), (2) and in particular (5) of Regulation 45/2001/EC, read in conjunction with Article 28 (1) of Directive 2005/60/EC.

8/ Procedures to grant rights of data subjects (*rights of access, to rectify, to block, to erase, to object*)

The right of access may be granted to data subjects subject to the exceptions outlined in Article 20 of Regulation 45/2001/EC and in particular para 1, 2 and 5. As mentioned under point 7, the provisions of Article 28 (1) Directive 2005/60/EC also need to be respected. It should be recalled that pursuant to Article 39 of the Directive, Member States should adequately sanction natural and legal persons revealing suspicions to a suspected party.

9/ Automated / Manual processing operation

Data are either directly supplied by the participants in EIB lending, borrowing or treasury operation, or obtained through internet searches, on free or paysites. These are summarised and evaluated in IT standard format documents or in emails. With the exception of emails, all other documents generated by OCCO are filed in paper form chronologically so that the file contains the subject matter of the document, the name of the author and the name of the addressee. Copies may also be held in thematic files (e.g. one file per country of operation). An electronic copy of the relevant document is stored in EIB's electronic document management system, enabling EIB Staff to carry out word searches on the content of such documents, in accordance with applicable IT data management and storage rules in force at EIB (see below). OCCO also created an excel spreadsheet listing the name of the Politically Exposed Persons (PEP) associated with the operation in question. Other than the name of the individual concerned, the list contains no other information.

10/ Storage media of data

Data are stored:
1/ in accessible document management systems supported by IT applications located at EIB's premises and
2/ in paper form chronologically

11/ Legal basis and lawfulness of the processing operation

The aforementioned activities described are necessary for EIB to conform to the requirements of Directive 2005/60/EC, Directive 2006/70/EC and the 40+9 recommendations of the Financial Action Task Force (FATF), an inter-governmental body hosted by the OECD whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

12/ The recipients or categories of recipient to whom the data might be disclosed

On an exceptional basis and with the specific prior consent of EIB's Chief Compliance Officer, data could be disclosed to compliance officers or Money Laundering Reporting Officers of co-financiers especially in the presence of clear evidence or serious suspicions of fraud, money laundering or other criminal activities, to judicial authorities and/or to OLAF, as the case may be, such disclosure would be done in compliance with articles 7/8/9 of Regulation EC 45/2001.

13/ retention policy of (categories of) personal data

Electronic and paper copies will be kept for as long as the banking relationship between EIB and the counterpart in question lasts (and in any case no longer than 15 years after the end of the relationship) and, in cases where such relationship was not established, for a period of no more than five years. OCCO must be in a position to refer back to past opinions for the following reasons:
- as background information for monitoring
- for the avoidance of unnecessary duplication of research
- in order to ensure consistency of the opinions delivered
- for audit and other control purposes in line with prevailing rules of EIB.

13 a/ time limits for blocking and erasure of the different categories of data
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

Not applicable as explained under point 7 and 8.

14/ Historical, statistical or scientific purposes

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

Not applicable

15/ Proposed transfers of data to third countries or international organisations

Transfer of data to international organisations and/or companies (banks mainly) operating in third countries would be limited to confidential sharing of information between co-financiers in the event of serious suspicions of fraud, money laundering, involvement with terrorist organisations or other criminal activities (see point 12).

16/ The processing operation presents specific risk which justifies prior checking (*please describe*):

Yes

AS FORESEEN IN:

Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Integrity checks, by their nature, look for evidence of suspected serious offences and criminal convictions, including but not limited to "sanction" lists containing the name of an organisation or individual as a result of such serious offences or criminal convictions.

Article 27.2.(b)

Processing operations intended to evaluate personal aspects relating to the data subject,

The identification of Politically Exposed Persons within the meaning of Directives 2005/60/EC and 2006/70/EC covers also family connections.

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

Not foreseen.

Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

OCCO's advice to the various services of EIB including the integrity checks it carries out, aim at preventing EIB from exposing itself to the risks of money laundering, terrorism financing and from reputation risks

Other (general concept in Article 27.1)

Not foreseen.

17/ Comments

Details of the integrity controls carried out by EIB should remain confidential to safeguard, in the terms of Regulation 45/2001 " the prevention, investigation, detection and prosecution of criminal offences". As indicated earlier, Directive 2005/60/EC Section 2 prohibits the communication of such information in most cases, as such communication would result in the impossibility for the enforcement authorities to freeze the assets of suspected money launderers and those financing terrorism.

18/ Measures to ensure security of processing (3)

Please check all points of Article 22 of Regulation (EC) 45/2001.

(3) Not to be published in the EDPS' Register (article 27.5 of Regulation (EC) 45/2001)

The data will be stored in email and documents in various electronic formats (e.g. diagrams of ownership structures in order to identify the final beneficiary). Such documents are drafted in protected sections of disc drives where only one individual has access apart from the IT system administrators who have unlimited and unrecorded access but who sign a specific Code of Conduct. Once finalised, the electronic copy of the document is either stored as an email, in the personal mail box of individuals who control the access to their mail boxes, apart from access by IT system administrators or kept in the Bank's electronic document management system where the access is fully controlled and fully subject to audit trails except in rare instances of system maintenance where the audit trail can be disconnected by IT administrators for a limited period of time.

PLACE AND DATE: Luxembourg, 31 August 2007

DATA PROTECTION OFFICER: J.-Ph. Minnaert

INSTITUTION OR BODY: European Investment Bank