

(To be filled out in the EDPS' office)
REGISTER NUMBER: 1371

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 19/04/2016

CASE NUMBER: 2016-0381

INSTITUTION: EIB

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001⁽¹⁾

1/ NAME AND ADDRESS OF THE CONTROLLER

EUROPEAN INVESTMENT BANK (EIB)
98-100, Boulevard Konrad Adenauer
L – 2950 Luxembourg

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

Depending on the nature of the alleged infringement:

- a) **IG/IN** or the **Audit Committee** in cases of alleged fraud, corruption, collusion, coercion, money laundering or financing of terrorism;
- b) The **Secretary General** or the **European Anti-Fraud Office (OLAF)** directly for cases of alleged fraud, corruption, coercion, collusion or any other activity that is detrimental to the interests of the Community, if there is a conflict of interest or a risk of reprisals; or if the intended recipient of the report is personally implicated in the incidents to be reported.
- c) the **Director of Personnel** receives cases of bullying, harassment and those concerning dignity at work cases reporting of a serious failure or infringement of ethics or integrity; the **Chief Compliance Officer** receives information on event of serious misconduct or a serious infringement of the Staff Code of Conduct or the Integrity Policy and Compliance Charter;
- d) the **President or the Management Committee** receives cases where the above competences are not appropriate due to conflict of interests;
- e) the **European Ombudsman** receives cases in the event of maladministration by the Bank in the management of the above procedures (please see point III.1 and 2 of the Whistleblowing Policy - WP).

¹ OJ L 8, 12.01.2001.

3/ NAME OF THE PROCESSING

EIB Whistleblowing Policy (“WB”)

4/ PURPOSE OR PURPOSES OF THE PROCESSING

To Protect persons (Whistleblowers) reporting any illegal behavior, serious misconduct or infringement of the Banks’s rules, policies and guidelines, or action harmful for the Bank’s reputation or mission, To protect Whistleblowers against retaliation (through confidentiality of identity, entitlement to file a complaint if subject to any retaliation, disciplinary action).To protect persons allegedly suspected of any of those acts.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

EIB staff, borrowers, promoters, contractors, suppliers, beneficiaries, any other person participating or seeking to participate in the EIB activities, having reported or being suspected of any illegal behavior, serious misconduct or infringement of Banks’s rules, policies and guidelines, or of any action harmful for the Bank’s reputation or mission.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA (*including, if applicable, special categories of data (Article 10) and/or origin of data*).

Identification private and professional data
Individual behavioural data – individual reports
Individual testimonies, written or verbal
Recorded images or conversations
Electronic data, mails, traffic calls
Correspondence of theWhistle blower and or of the alleged infractor

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

The Whistleblowing policy is published on the intranet.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

The persons allegedly implicated are notified in good time and have the opportunity of a fair hearing. They have the right to access, to rectify, to block and to erase. The President decides after hearing the person or persons allegedly implicated.

On WB cases where IG/IN procedure applies respective procedural rules concerning the rights of data subject shall apply.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Automated and or manual operations

10/ STORAGE MEDIA OF DATA

Nothing foreseen on the WB policy. Depending on the alleged infringement IG/IN, Personnel and OCCO shall apply the respective rules on Anti-Fraud procedure, Disciplinary Procedure, Anti-Money Laundry - FT or Code of Conduct procedure.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Decision of the MC approving the Whistleblowing policy of 21 January 2009.

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

Depending on the nature of the alleged infringement:

a) **IG/IN** or the **Audit Committee** in cases of alleged fraud, corruption, money laundering or financing of terrorism;

b) the **Secretary General** or the **European Anti-Fraud Office (OLAF)** in cases of alleged fraud, corruption, coercion, collusion or any other activity that is detrimental to the interests of the Community, if there is a conflict of interest or a risk of reprisals; or if the intended recipient of the report is personally implicated in the incidents to be reported.

c) the **Director of Personnel** receives cases of bullying, harassment and those concerning dignity at work cases reporting of a serious failure or infringement of ethics or integrity;

d) the **Chief Compliance Officer** receives information on event of serious misconduct or a serious infringement of the Staff Code of Conduct or the Integrity Policy and Compliance Charter;

e) the **President or the Management Committee** receives cases where the above competences are not appropriate due to conflict of interests;

f) **European Ombudsman** receives cases in the event of maladministration by the Bank in the management of the above procedures (please see point III.1 and 2 of the Wistleblowing Policy - WP).

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

NOTHING IS FORESEEN ON THE WB POLICY. Depending on the alleged infringement IG/IN, Personnel and OCCO shall apply respective rules on Anti-Fraud procedure, Disciplinary Procedure, Anti - Money Laundry - FT or Code of Conduct procedure.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

NOTHING IS FORESEEN ON THE WB POLICY. Depending on the alleged infringement IG/IN, Personnel and OCCO shall apply respective rules on Anti-Fraud procedure, Disciplinary Procedure, Anti - Money Laundry - FT or Code of Conduct procedure.

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES
NOT APPLICABLE

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS
NOT APPLICABLE

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING:

AS FORESEEN IN:

↑ Article 27.2.(a)

Processing of data relating to(...) and to suspected offences(...),

↑ Article 27.2.(b)

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

↑ Other (general concept in Article 27.1)

17/ COMMENTS

IG has his own investigating procedures which were approved by the Management Committee (and cleared by the EDPS).

OCCO and Personnel still don't have a specific procedure to deal with respective reporting WB cases; a general administrative inquire procedure is under preparation; meanwhile, OCCO requests the cooperation of IG to investigate his own cases on WB. The adoption of "protective measures" by OCCO should follow IG investigating procedure or, for the time being, the administrative enquire proceeding.

Taken into account the recent EDPS Guidelines I am not sure that the existing WP would be sufficient to comply with and where the existing WP needs to be further complemented with procedural rules: (1) data subjects are not informed of permitted restrictions under article 20 of Regulation 45/2001; (2) It should be clearly stated that the identity of the WB should never be revealed apart exceptional circumstances: (a) the WB authorizes; (b) it is required for any subsequent criminal law proceedings c) the WB malicious makes a false statement). (3)- Confidentiality of the WB should also be extended to the accused persons and third persons because the risk of stigmatization and victimization; (4)The investigative authorities should be aware of the risk of collecting sensitive data (article 10 of Regulation 45/2001) or irrelevant data for the investigation.

The administration of the WP is deferred to OCCO and to Personnel:

The Chief Compliance Officer and the Personnel Director could be requested to adopt "*Protective measures*" where members of staff consider that they have been the victim of retaliation for reporting an irregularity or have good reason to believe or fear that they are exposed to a risk of retaliation as a result of their reporting an irregularity.

The Chief Compliance Officer shall be consulted in advance in the event of the adoption or amendment of any internal Bank provision on WB police and the Chief Compliance Officer, with the agreement of the Director of Human Resources, shall propose to the Management Committee any necessary amendments to these provisions.

The administration of the WP is deferred to OCCO and to Personnel:

PLACE AND DATE: LUXEMBOURG, 19 APRIL OF 2016

DATA PROTECTION OFFICER: ALBERTO SOUTO DE MIRANDA

INSTITUTION OR BODY: EUROPEAN INVESTMENT BANK