(To be filled out in the EDPS' office)
REGISTER NUMBER: 1293

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 17/12/2014

CASE NUMBER: 2014-1163

INSTITUTION: EUROPEAN INVESTMENT FUND

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

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

European Investment Fund
37B, Avenue J. F. Kennedy
L - 2960 Luxembourg

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

EIB Inspectorate General - Fraud Investigations Division - Compliance and Operational Risk Division (EIF COR).

3/ NAME OF THE PROCESSING

Fraud Investigations

4/ PURPOSE OR PURPOSES OF THE PROCESSING

Under the provisions of the EIF's Anti-Fraud Policy, EIF Staff and EIF's business partners are required to maintain the highest level of integrity and efficiency in relation to all EIF activities and operations. The Fraud Investigation Division (IG-IN) of the European Investment Bank (EIB) is the team that has the duty to investigate credible allegations of fraud, corruption, collusion and coercion, money laundering or terrorist financing ("prohibited practices conduct") in the EIF supported operations - allegations that appear initially without basis will be filtered out at an early stage. EIF as a member of EIB Group has a zero tolerance policy against prohibited practices conduct in its activities and/or operations. Investigation services are outsourced under a service level agreement

[1] OJ L 8, 12.01.2001.

[2] **Please attach all necessary backup documents**

(cf. extracts enclosed) to the Fraud Investigations Division of the EIB Inspectorate General.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

For the purpose of fraud Investigations, IG/IN has unrestricted access to people all relevant personnel, information, documents and data within the EIF. In the course of the investigations, IG-IN may process data of staff members, EIF counterparts, suppliers and consultants, who are relevant for the investigation, as subject, whistleblower and/or informant/witnesses, in accordance with applicable procedures and rules. In particular, IG/IN may access personal file/data of EIF staff members, including their electronic data, only with the prior written approval of. Concerning staff members by standard practice both the Head of HR and the Fund's Data Protection Officer. are notified by e-mail prior to accessing personal data.

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

All EIF staff members are obliged required to cooperate with IG-IN and OLAF promptly and fully, including by answering relevant questions and complying with requests for information and records. IG/IN can also have access to the personal file of an EIF staff member if relevant for the investigation as explained above under point 5.
As provided for in the applicable EIF contracts, IG-IN and OLAF can examine and copy the relevant books and records of counterparts, suppliers, service providers and other involved parties - the so-called "audit and visiting" rights.
In case of an allegation concerning staff members of the EIF only the presonal professional history (cv provided when applying to EIF) will be checked.
In any case, the personal data quality principle is applied, as provided for in IG/IN's Investigations Procedure (already notified to EDPS – Case 2009/0459).

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

A privacy statement is included in all IG/IN's relevant outgoing correspondence in order to inform data subjects of the processing of their personal data, their rights as well as the possibility to always contact directly the EDPS. This privacy statement has already been reviewed by the EDPS (notification 2009/0459).
Concerning EIF staff members, in accordance with point 46 of the EIF Anti-Fraud Policy, 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.
Furthermore, in accordance with point 47 of the EIF Anti-Fraud Policy, a staff member, who is 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 action is taken. The information will be provided to the data subject as soon as this would not negatively impact be harmful to the ongoing investigation. This restriction measure is applied when necessary, on a case-by-case basis.
The information to a data subject may be deferred if this constitutes a necessary measure to safeguard the investigation. This restriction is subject to a "necessity test" to be conducted on a case-by-case basis. If the information to a data subject has been postponed, IG/IN shall review from time to time whether the restriction still applies.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS
(Rights of access, to rectify, to block, to erase, to object)

Any request from data subjects for an access, rectification, blocking and erasure is forwarded to the data controller, i.e. the Head of IG/IN. If the information is requested orally to IG/IN, the concerned investigator shall ask the data subject to submit his/her request in writing to the Head of IG/IN. The data controller must give a reply to such request.
As part of the rights of data subjects, access is granted to any documents containing personal data processed during an investigation to the relevant data subject. In the case of an interview, this includes the written record of interview of which a copy is given to the interviewee for review and signature.

When information has been provided by a whistleblower or external informant, the data subject requesting access must be given access to his/her personal data but he/she shall not be provided with the name of the whistleblower or external informant, nor to any element of information that would allow the data subject to identify the whistleblower or external informant.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

For Fraud Investigation both electronic and manual processing of personal data is occurring.
Accesses are limited to the Fraud Investigation Team.
The physical paper files are stored separately in specific locked archives of IG-IN.
Electronic files are stored in a restricted area of GED (information management system of EIB) only accessible to IG/IN upon authorization of the head of IG/IN and whose access is protected by individual password.

10/ STORAGE MEDIA OF DATA

As referred to under point 9, the paper files are archived separately in specific locked archives for IG-IN (only accessible to Fraud Investigation staff). The paper files will be destroyed 10 years after the case has been closed.
Electronic files are stored in a restricted area of GED (information management system of EIB) only accessible to IG/IN upon authorization of the head of IG/IN and whose access is protected by individual password.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Investigations are conducted in conformity with the Procedures for the Conduct of Investigations by the Inspectorate General of EIB (already notified to EDPS – 2009-0459) under a service level agreement with EIF. The procedures are based on the principles agreed by the IFIs' Anti-Corruption Task Force and laid out in the Uniform Framework agreement, signed in Singapore in September 2006.
The legal basis to conduct investigations in EIF operations and activities stems from:
(i) Article 325 of the Treaty on the Functioning of the European Union (TFEU);
(ii) Article 2/1 of the EIF Statute;
(iii) Article 18 of the EIB Statute;
(iii) Council Regulation (EC, Euratom) No 966/2012 of 25 October 2012.

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

Reporting on cases is done with strict confidentiality and limited circulation. IG-IN provides its findings to senior management who have specific responsibility for the project and reprorts at the same time to OLAF and the Audit Board of EIF. A monthly summary of all cases is, in addition, also sent to the external auditors of the EIF every quarter.
The Chief Executive is informed by the Inspector General on the follow-up measures to be taken by the operational services, including contractual consequences.
IG-IN may refer a matter to the appropriate national authorities for further investigation and/or criminal prosecution, see more details in point 15 below. This shall be done with or with the assistance of OLAF.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Data shall be retained for at least five years and up to ten years maximum from the date of closure of the case.
As regards allegations where the Head of IG/IN decides not to open a case (Prima Facie Non Case) or a case closed because the allegations are not substantiated, data shall be retained for up to five years maximum from the decision not to open a case or the closure of the case.
This retention policy may be subject to review, in line with OLAF's retention periods.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS *(Please, specify the time limits for every category, if applicable)*

cf. point 13 above

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

IG/IN may refer suspected prohibited conduct to national authorities within and outside the EU for further investigation or criminal prosecution and provide further assistance as may be requested. IG/IN may also share its findings with other International Financial Institutions' investigation functions. Where such referrals to third countries and international organisations include the transfer of personal data, the below procedure applies:
- Where the recipient provides an adequate level of protection, the transfer can be handled like a transfer to a recipient in a Member State. The appropriate transfer clause should be used. The list of countries deemed by the Commission to provide an adequate level of protection is used for this purpose.
- Where the recipient does not ensure an adequate level of protection but has a Memorandum of Understanding (MoU) with IG/IN including appropriate data protection clauses, data transfer is permitted using the relevant transfer clause.
- Where the recipient has neither an adequate level of protection nor a MoU with IG/IN, it is

possible to rely for occasional transfers on the derogation in Article 9(6)(d) of the Regulation which states that the "transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.". Use of this derogation must be determined on a case-by-case basis for every transfer. In such situations, the relevant standard transfer clause must be included.
NB. The transfer clauses used by IG/IN have been developed on the basis of the clauses used by OLAF and have been already reviewed by the EDPS (notification 2009/0459)

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe)*

AS FORESEEN IN:

☐ Article 27.2.(a)
(Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,)

☐ Article 27.2.(b)
(Processing operations intended to evaluate personal aspects relating to the data subject,)

☐ Article 27.2.(c)
(Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,)

☒ Article 27.2.(d)
(Processing operations for the purpose of excluding individuals from a right, benefit or contract)

☒ Other (general concept in Article 27.1)

17/ COMMENTS

Not applicable

PLACE AND DATE: LUXEMBOURG, 17 DECEMBER 2014

DATA PROTECTION OFFICER: J. NEUSS

INSTITUTION OR BODY: EUROPEAN INVESTMENT FUND