

EUROPEAN DATA  
PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI  
SUPERVISOR

Mr Pier Luigi GILIBERT  
Chief Executive  
European Investment Fund (EIF)  
37B, avenue J.F. Kennedy  
L-2968 Luxembourg

Brussels, 13 May 2015  
GB/MG/sn/D(2015)0810 C 2014-0908  
Please use [edps@edps.europa.eu](mailto:edps@edps.europa.eu) for all  
correspondence

**Subject: Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Fund regarding Anti-Money Laundering and Financing of Terrorism (AML-CFT) data processing**

### **1. Proceedings**

On 29 September 2014, the European Data Protection Supervisor (EDPS) received a notification for prior checking relating to the processing of personal data in the context of Anti-Money Laundering and Financing of Terrorism (AML-CFT) verifications from the Data Protection Officer (DPO) of the European Investment Fund (EIF).

As indicated by EIF “The notification is to be seen in conjunction with the notification on the transactional due diligence process<sup>1</sup>, of which it forms an integral part”<sup>2</sup>. Therefore, the EDPS has taken into account the relevant information provided in both notifications for the assessment of this case.

Since the notification refers to data processing already in place at the moment of the notification to the EDPS, it is considered as ex-post. Hence, the two-month deadline under

---

<sup>1</sup> Notification for prior checking on “transactional integrity due diligence” by EIF, received by the EDPS on 14 July 2014, filed under the EDPS case number 2014-0725.

<sup>2</sup> As specified by EIF DPO in his comments to the factual part of the draft Opinion on Case 2014-0725, sent to the EDPS on 18 December 2014, AML-CFT verifications may be performed if the co-investor is a natural person or if the final beneficiaries of the co-investor are natural persons. This specific AML-CFT control does not occur systematically, but only if such integrity due diligence is needed to complement the transactional due diligence process.

Article 27(4) of Regulation (EC) No 45/2001 (**the Regulation**) does not apply to this case, which has been dealt by the EDPS on a best-effort basis.

The following documents were attached to the notification of the data processing by EIF for AML-CFT purpose as supporting documentation:

- EIF Compliance and Operational Risk, Operational compliance procedure (Annex 1);
- Factiva screenshot (Annex 2);
- Framework Agreement between the European Investment Bank and the European Investment Fund; and its Annex, Protocol of Understanding (Annex 3).

## **2. Facts**

EIF, together with the European Investment Bank (**EIB**), is part of the European Investment Bank Group (**EIB Group**) and operates on the basis of EIB Group compliance framework, which includes EIB Group "Compliance procedure on counterparty acceptance and monitoring, covering integrity, money-laundering and financing of terrorism risks"<sup>3</sup>.

EIF assesses -also in cooperation with EIB (pursuant to the Framework Agreement between EIB and EIF)- the risks referred to above in the context of its business activities, as funded either through its own funds or through funds provided to EIF by other institutions.

### **2.1 Description of the processing and of its purpose**

Because both EIF and EIB belong to the EIB Group, EIF conducts data processing for the purpose of countering money-laundering and financing of terrorism risks (**AML-CFT**) in a way which is generally analogous to the data processing performed by EIB<sup>4</sup>.

Processing in this regard starts when EIF considers entering into a business relationship with a new counterparty. The results of this process may lead to (i) the acceptance of counterparties, (ii) their rejection or (iii) the imposition of additional compliance requirements in the contract(s) to be signed.<sup>5</sup>

In order to apply its scrutiny regarding AML-CFT, EIF conducts customer/counterparty due diligence (**CDD**) with regard to its prospective business partners.

The organizational part of EIF entrusted with the processing of personal data is the Compliance and Operational Risk Division (**EIF COR**).

Data are collected by the operational services and by the compliance officers through electronic means from internet websites and specialised databases tools available on the market and generally used by the banking industry (databases, websites and public sanctions lists).

---

<sup>3</sup> The data processing in the context of this EIB Group compliance policy has been notified to the EDPS on 3 April 2012 (notification for prior checking 2012-0326). See EDPS Opinion of 7 February 2013, available on the EDPS website.

<sup>4</sup> This Opinion takes into account some specific modalities for data processing by EIF which are not envisaged by the EIB policy on AML-CFT controls, while being consistent with the EDPS Opinion of 7 February 2013 on the notification for prior checking of data processing operations performed by the EIB for AML-CFT (case 2012-0326).

<sup>5</sup> As specified in the EIF Operational Procedures Manual, TRM/Equity, accompanying the notification for prior checking for Case 2014-0725, Section 4.2.2, Integrity checks, "Integrity checks on the fund manager and on the key members of the team should be ran *at the earliest possible stage* in the due diligence process. Integrity checks consist of a Factiva search and of a general internet search of key individuals."

When both checks have been completed, EIF staff members record in the e-Front database the management company and names of the management team members. EIF uses an internal database (DLM) as internal case management system for the handling of cases (i.e. the financial projects to be funded).

Relevant findings are then presented in a 'compliance opinion' which is included in the transaction proposals sent to the EIF 'governing bodies' in view of the final financing decision.

## 2.2 Data subjects

The data subjects are the persons who -directly or indirectly<sup>6</sup>- own legal entities with which the EIF maintains or plans to enter into business relationships in the context of financing projects; persons entrusted with managing roles in these legal entities ("**counterparty key persons**").

More specifically, these persons are:

- persons with key positions and responsibility in the governing bodies of the counterparty;
- key persons and shareholders (as described in EIF notification on transactional due diligence, case 2014-0725)<sup>7</sup>.

If a person in any of the above categories also happens to be a "Politically Exposed Person" (PEP)<sup>8</sup>, this is considered by EIF as a sign for increased risk. Therefore, a more intense due diligence applies to PEPs pursuant to the provisions of Directive 2005/60/EC.

## 2.3 Categories of data

The following data categories are collected:

- identification data;
- data related to offences, investigation and prosecution and public criminal records;
- data related to business relationships.

These data are partly collected directly from the data subjects and partly from other sources such as: newspapers, specialised databases operated by the private sector (Dow Jones Risk and Compliance; Factiva); websites (Google search); public sanctions lists (OFAC; EU lists).

---

<sup>6</sup> See, in this regard, the definition of "beneficial owner" in Article 3(6) of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15-36.

<sup>7</sup> "*Key persons of management teams for private equity fund structures in which EIF invests its own financial resources or financial resources under third party mandates. The identification of such key persons is part of the commercial due diligence process performed by the due diligence team of Equity Investments (EI). Sponsoring business angels, who manage EIF funding in a co-investment scheme (European Angels Fund EAF). The European Angels Fund is structured as Luxembourg-based fund with regionally focused sub-funds, presently for Germany, Austria and Spain. Under the scheme business angels are entrusted with drawing funding from the respective regional sub-fund of the EAF with a view to co-investing with their own funds into private equity investments. Although the investments of the business angels are usually reflected in corporate structures, the individual person of the business angel is key for the success of the scheme. This has as a consequence that the business angel undergoes essentially the same due diligence process as the key persons of standard private equity management teams. (...) Exceptionally EIF Co-investors to the extent (they are) natural persons.*"

<sup>8</sup> PEPs are defined in Directive 2005/60/EC Article 3(8) as "persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons". This is further spelled out in Commission Directive 2006/70/EC, Article 2. According to this Article "prominent public function" refers to current and former (no time limit) heads of states, heads of governments, ministers and deputy or assistant ministers, members of parliaments, members of supreme/constitutional courts and other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances, members of courts of auditors or of the boards of central banks, ambassadors, *chargés d'affaires*, high-ranking officers in the armed forces and members of the administrative, management or supervisory bodies of State-owned enterprises. "Family members" are defined as parents, spouse (or equivalent), children and their partners. "Close associates" are defined as persons having joint beneficial ownership of legal entities or legal arrangements together with a PEP or owners of legal entities or legal arrangements set up for the *de facto* benefit of a PEP. These provisions are also meant to cover equivalent situations on the EU or international level.

In specific situations, where EIF COR identifies a potential risk, recourse to external consultants can also be made by EIF<sup>9</sup>.

The data processing is performed manually with the support of the electronic databases DLM<sup>10</sup> and e-Front<sup>11</sup>.

## 2.4 Categories of recipients to whom data might be disclosed

Personal data collected, are -in principle- not disclosed to third parties with the exception of the Inspectorate General-Investigations of EIB (**EIB IG-IN**) on the basis of a service level agreement between EIF and EIB pursuant to which EIB IG-IN may proceed to internal and external investigations on behalf of EIF.<sup>12</sup>

## 2.5 Retention periods

Personal data are retained for a period not exceeding five years following the termination of the business relationship. As the usual "life of the fund structures" (the business relationship) in which EIF invests is, in line with market practice, "ten plus two years", this means a total retention of personal data not exceeding 17 years from the starting of the business relationship (the 12 years life-cycle of the business transaction plus five years).

## 2.6 Data protection information

According to the notification, the EIF intends to post on its website a communication on the type of data potentially collected and of the rights of the data subjects in the context of the AML-CFT due diligence<sup>13</sup>. A privacy statement has been provided in this regard by EIF to the EDPS by EIF DPO on 24 February 2015. The latter specifies that data subjects can exercise their data protection rights by contacting the EIF "at any time during the business relationship with EIF".

In addition, the counterparty key persons are specifically informed in the context of the specific due diligence regarding them; in case of collection of data falling under the categories of data indicated under Article 10 of the Regulation, EIF asks for their express consent.

## 2.7 Data subjects' rights

According to the notification "data subjects may request blocking and erasure of [their] data at any time. Data controller will execute within 30 working days following receipt of the request"<sup>14</sup>. In addition, *"the data subjects are made aware of their right to access, rectify, block or erase or to object to the collection and storage of their personal data. Rights conferred by Regulation 45/2001 can (...) be exercised by sending requests to EIF COR.*

---

<sup>9</sup> The sources are specified in the Annex III to the EIF Compliance and Operational Risk, Operational compliance procedure, Table A, "Ex-ante Controls", Table B, "Monitoring", at p. 25-26.

<sup>10</sup> DLM is the (case management) database hosted by EIF and subject to all internal rules applicable to EIF databases.

<sup>11</sup> E-Front is an electronic database developed by e-Front, a company established in France (Paris) and subject to French law implementing Directive 95/46/EC and to the supervision of the French DPA (Commission Nationale Informatique et Libertés/CNIL).

<sup>12</sup> See Framework Agreement between the European Investment Bank and the European Investment Fund (Annex 3 to the prior check notification). According to this agreement data may also be forward transferred from EIB to OLAF for investigation purposes.

<sup>13</sup> The notification on "transactional integrity due diligence" process (case 2014-0725) is accompanied by a draft data protection notice (to be published on EIF website) which also makes reference to the processing of personal data by EIF for AML-CFT purpose.

<sup>14</sup> Section 13a of the notification.

*Requests will be processed in accordance with the principles and rules laid down in Regulation 45/2001*<sup>15</sup>.

## 2.8 Security measures

In the notification for the data processing operation filed under EDPS case 2014-0725, EIF specifies that the e-Front database, hosted in Paris, France, *“is physically protected and backed-up in line with French data protection rules. E-front staff access is limited to the named administrators of the system. Within EIF, a limited number of staff has access to the database to the extent required for the fulfilment of their professional duties”*. Such access is *“password-protected”*.

DLM, the case management database hosted by EIF at EIF premises *“is subject to all internal rules applicable to EIF databases”*.

## 3. Legal aspects

### 3.1. Prior checking

**Applicability of the Regulation:** The notified operations constitute a processing of personal data performed -at least in part, through automatic means- by a body of the EU in the exercise of activities which fall within the scope of the Treaties.

**Grounds for prior checking:** Article 27(1) of the Regulation subjects to prior checking by the EDPS all *“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 lists processing operations that are likely to present such risks.

In the present case, data on *offences* may be processed [Article 27(2)(a)]. The aim of the ‘counterparty acceptance process’ may include the *evaluation of personal aspects* relating to the data subjects [Article 27(2)(b)], in order to assess whether they present AML-CFT risks. Moreover, the processing can result in the *exclusion of individuals from a right, a benefit or a contract* [Article 27(2)(d)]. For all these reasons, the processing operation is **subject to prior checking**.

### 3.2. Lawfulness of the processing

In the notification EIF points out that *“EIF Statutes express the basic mission of EIF and decisions of its General Meeting and its Board of Directors”*.<sup>16</sup>

In this regard, Article 5(a) of the Regulation may provide the basis for lawfulness of the processing operations under scrutiny. Under Article 5(a), a two-step test needs to be carried out to assess: (1) whether either the Treaty or other legal instruments foresee a public interest task on the basis of which the data processing takes place (*legal basis*); (2) whether the processing operations are indeed necessary for the performance of that task.<sup>17</sup>

---

<sup>15</sup> Section 8 of the notification.

<sup>16</sup> EIF notification on transactional due diligence, at point 11.

<sup>17</sup> Article 5(a) of the Regulation authorises processing that 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”*.

## 1. Legal basis

The EDPS notes that the legal basis for the purpose of Article 5(a) must be found in legal provisions which are directly applicable to the EIF, such as its Statute and the provisions adopted by EIF organs on the basis thereof.

These provisions can be found in the EIF Statute, in particular its Article 2(1), according to which: “the task of the Fund shall be to contribute to the pursuit of the objectives of the European Union. The Fund shall pursue this task through activities consisting of: the provision of guarantees as well as other comparable instruments for loans and other financial obligations in whatever form is *legally permissible*”, and its Article 2(3), stating that: “The activities of the Fund shall be based on *sound banking principles or other sound commercial principles and practices where applicable*”.

This obligation, as referred to under Article 2(1) and (3) of the EIF Statute, implies for EIF the duty to ensure, among others, that its resources are not used for money laundering or terrorism financing purposes (at the same time, the deployment of funds towards counterparties implying integrity or reputation risks would run contrary the objective of rational employment of funds in the interest of the European Union). Such transactions would reflect adversely on the image of the EIF as a public institution and thus endanger the EIF reputation.

AML-CFT verifications undoubtedly form, not only a parameter for the legality of the transactions, but also part of sound banking principles and commercial practices in the European Union and in the wider international community, as recognised by the FATF<sup>18</sup>.

While the above provisions can in principle be used as legal bases, the EDPS believes that they are too general to constitute in themselves a sufficient ground for the processing at stake. In other words, the general obligations pursuant to Article 2 of the EIF Statute need to be implemented and made more specific.

The EDPS notes that the “Compliance and Operational Risk, Operational Compliance procedure”, formally approved in its last updated version by EIF DPO on 15 October 2013, and the “Policy on preventing and deterring corruption, fraud, collusion, coercion, money laundering and the financing of terrorism in European Investment Fund Activities”<sup>19</sup> specify EIF *modus operandi* having regard to the due diligence process (including the AML-CFT check)<sup>20</sup> and may thus constitute the concrete and specific implementation of the “sound banking principles” to be followed by EIF pursuant to Article 2(3) of EIF Statute.

## 2. Necessity

The notified processing operations also appear in principle *necessary* for the purpose of such task. Without performing verifications on the identity and background of the customer prior to entering into business relationship with the latter, EIF would not be able to detect and prevent cases where its funds would be used for money laundering or terrorist financing purposes or the counterparty would entail reputational risks for EIF.

In view of the above, the EDPS considers that the combination of the EIF Statute provisions and the related ‘implementing provisions’ constitute in principle a sufficient legal basis for the purposes of the applicability of Article 5(a) of the Regulation.

---

<sup>18</sup> Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.

<sup>19</sup> Published on EIF website at: [http://www.eif.org/attachments/publications/about/anti-fraud\\_procedures.pdf](http://www.eif.org/attachments/publications/about/anti-fraud_procedures.pdf).

<sup>20</sup> See Section 4, Due diligence, of the Operational Procedures Manual, p. 11-13.

### 3.3. Processing of special categories of data

Article 10(1) of the Regulation prohibits the processing of personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, and of the data concerning health or sex life. The processing of these special categories of data is prohibited unless one of the exceptions under Article 10 applies.

In the notification, the controller did not identify any special categories of data among those mentioned in Article 10(1). In any event, even if the processing of special categories of data is not the primary purpose of the processing, **it cannot be excluded that processing of such data may occur**. For example, the verifications undertaken for anti-terrorism purposes may well reveal political opinions, religious or philosophical beliefs.

It is therefore worth recalling that **EIF staff in charge of the AML-files must avoid processing special categories of data unless one of the exceptions foreseen in Article 10 applies**. COR Procedure should explicitly mention this *caveat*/general rule.

Article 10(5) of the Regulation allows "*processing of data relating to offences, criminal convictions or security measures [...] only if authorised by the Treaties [...] or other legal instruments adopted on the basis thereof or if necessary, by the European Data Protection Supervisor, subject to appropriate safeguards*".

According to the notification, "data related to offences, investigation and prosecution and public criminal records" may be processed as part of the counterparty acceptance process and the subsequent counterparty monitoring. The AML-CFT 'Framework' (EIF Statute, EIF Operational Procedures Manual) does not appear to contain a specific reference to the fact that EIF would be collecting and processing data relating to offences under Article 10(5).

The EDPS therefore recommends that the **EIF adopts a specific legal basis/decision authorising EIF to process personal data under Article 10(5) of the Regulation**.

The processing of special categories of data should in any case be limited to the extent necessary for carrying out the AML-CFT procedure. Appropriate safeguards to ensure necessity, proportionality and data quality should be set out in this respect.

### 3.4. Data Quality

Article 4(1)(c) of the Regulation states that data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. Besides, as laid down under Article 4(1)(d), personal data must be kept accurate and up to date; and every reasonable step must be taken to ensure that inaccurate or incomplete data are rectified or erased.

Regarding the criteria of relevance and adequacy, the processing should be limited to those data categories which have a direct link to ensuring compliance with the applicable banking legislation. In particular, this means that references to "data related to offences, investigation and prosecution and public criminal records"<sup>21</sup> have to be read as references to such data *as far as they relate to AML-CFT controls*.

---

<sup>21</sup> As indicated in the COR Procedure, accompanying the notification, ex-ante controls and monitoring may concern "criminal or administrative investigation on the EIF Counterpart or any Key Person or Ultimate Beneficial Owner"; "criminal records, sanctions, large civil court cases on the EIF Counterpart or any Key Person or Ultimate Beneficial Owner".

More in general, the EDPS recommends that EIF evaluates -for each and every search made- whether the latter has a clear and direct link to AML-CFT purposes, as well as the degree of 'reliability' of the information collected<sup>22</sup>.

Furthermore, the provisions imposing certain verifications should be interpreted in a balanced way in accordance with the proportionality principle, taking into account the impact on the rights and freedoms of the data subject.

The EDPS further recommends that EIF implements effective measures to guarantee a high level of data quality, including the following:

- case handlers performing the CDD should receive a specific data protection training;
- identification of 'best CDD practices', ensuring that AML-CFT checks are performed with the minimum possible impact on the rights and freedoms of the data subject;
- ensuring accuracy of public sources, including a description of how EIF case handlers make a distinction between factual data, opinion data, intelligence data.

The EDPS recommends that the EIF develops and implements effective measures to guarantee a high level of data quality also making reference - in this regard - to the relevant Opinion of the Article 29 Working Party<sup>23</sup>.

### 3.5. Data retention

Personal data must be "kept in a form which permits identification of data of data subjects for no longer than is necessary for the purposes for which the data are collected and/or further processed" [Article (4)(1)(e)].

In this regard, the retention periods established under Directive 2005/60/EC and the national laws implementing it may provide guidance on the appropriate retention period. Article 30 of this Directive sets out that such data shall be kept (by the financial institution) for "at least five years *after the business relationship with the customer has ended*".

In the light of the above, the EPDS considers that the data retention period applied by EIF is compliant with Article 4(1)(e) of the Regulation.

### 3.6. Transfer of data

Article 7(1) establishes that data shall only be transferred within or between Union institutions and bodies if they are "*necessary for the legitimate performance of tasks covered by the competences of the recipient*".

According to information provided by EIF in the notification, personal data may be transferred by EIF to the Inspectorate General-Investigations of EIB (EIB IG-IN) on the basis

---

<sup>22</sup> Some of the data categories can reasonably assumed to be of 'high quality', such as identification data supplied by data subjects themselves or extracts from public criminal records. For others, such as allegations of illegal or disreputable activities ("press reports, market rumours or similar indicators of a potential reputation risk to EIF in case EIF would enter into business with the EIF Counterpart" – see Table A, Annex III to COR Procedure), this is not the case. In this regard, EIF must take appropriate steps to ensure a high level of accuracy. Such steps could include abstaining from using unreliable press reports, cross-checking information obtained from press reports against reliable independent sources or giving data subjects a possibility to state their case. The EIF should put procedures in place to guarantee that data are updated as necessary and that allegations that turn out to be unfounded are removed as soon as possible. Special care should be taken to avoid confusion due to homonyms.

<sup>23</sup> Article 29 Working Party Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, pp. 15-16 of the Annex, available at: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186\\_en\\_annex.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf).



of a service level agreement between EIF and EIB pursuant to which EIB IG-IN may proceed to internal and external investigations on behalf of EIF.<sup>24</sup>

Insofar as the data transfers relate to the investigation of specific cases by EIB, acting on the basis of the agreement with EIF and for the performance of its monitoring tasks, such transfers can be deemed in accordance with Article 7(1) of the Regulation. A case by case analysis, however, has to be performed to evaluate *in concreto* whether the conditions for the transfer are actually fulfilled.

According to the notification and to the draft data protection notice, no other transfers under Article 8 of the Regulation, i.e. to recipients not subject to the Regulation, or under Article 9, i.e. to third countries, are foreseen.

### 3.7. Rights of the data subject

Articles 13 and 14 of the Regulation establish that data subjects shall be able to access and rectify data stored about them at any time. Restrictions are possible in line with Article 20.

In the notification, EIF did not mention that these rights might be limited in accordance with Article 20(1), letters (a)-(e) of the Regulation. This reference is also not included in the draft data protection note accompanying notification 2014-0725.

In case EIF introduces the exception under Article 20 of the Regulation, enabling a restricted application of Articles 13-17 of the Regulation, the following should however be taken into account:

- any restrictions on the rights of access and rectification must only be used on a case-by-case basis and only as long as necessary for this purpose;
- any use of a restriction under Article 20 must be justified and internally (i.e. within EIF) documented;
- appropriate procedures should be put in place to allow the exercise of these rights in these cases;
- besides, according to paragraph 3 of Article 20: "*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*";
- 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 data processing, or has knowledge of it, but the right of access is still being restricted in the 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 EIF 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 the right to rectify inaccurate or incomplete data. We recall that this right is of key importance in order to guarantee the

---

<sup>24</sup> Framework Agreement between the European Investment Bank and the European Investment Fund, Annex 3 to the prior check notification.

quality of the data used, and, especially considered the sensitivity of the context (AML-CFT verifications), we further note that this right is also connected to the right of defence.

Concerning the time limits for ruling on request for access, rectification, blocking, erasure, and to object, the EDPS points out to the time-limit of three months from the receipt of the request in case of exercise of the right to access (Article 13(1) of the Regulation).

Regarding requests for blocking and rectification, the EDPS recommends: to immediately block the data for a period enabling the controller to verify the accuracy, including the completeness, of the data, when the data subject contests the accuracy of his/her data; to immediately rectify data in case the controller is aware of the inaccuracy or incompleteness.

### **3.8. Information to the data subject**

The data subject must be provided with information on the data processing in accordance with Articles 11 and 12 of the Regulation.

EIF indicated in the notification that the data subjects will be informed of the processing taking place in the context of AML-CFT due diligence by means of a data protection notice to be published on the EIF website.

Concerning this means for providing the information, the EDPS considers that the publication of the procedure in the website does not in itself suffice to ensure that data subjects receive the information in an effective manner. This publication must be complemented, to the extent possible, by some form of **individual information** containing the necessary information pursuant to Articles 11 and 12 of the Regulation. The EDPS recommends in particular providing such information to the counterparty *on the first relevant occasion* (i.e. after the initial contact triggering the start of the procedure has been established), with a request to forward it to the identified or identifiable natural persons concerned (for example, the key persons or PEPs within the counterparty organisation).

Having regard to the content of the privacy statement "EIF transactional and integrity due diligence", the EDPS notes that, in the draft version submitted to the EDPS on 24 February 2015, the privacy notice, to be published on EIF website, contains the information required under Articles 11 and 12 of the Regulation.

### **3.9. Security measures**

According to Article 22 the Regulation, EU institutions and bodies shall provide adequate security measures in the light of the nature of the data and of the risks presented by the processing.

For all notified operations, electronic files will be stored in the EIF's document management system (DLM). Access to such case management system will be restricted to those staff members involved in the relevant file. EIF indicates that the aforesaid internal EIF document management system is subject to all applicable (physical and organizational) security measures in compliance with the Regulation.

The e-Front database (the database used by EIF for registration of company names and company records) is - according to the information provided in the notification - compliant with the provisions under Article 17 of Directive 95/46/EC, which are analogous to the provisions under Article 22 of the Regulation. E-front, being located in France and managed by a company established in France, is subject to the supervision of the French Data Protection Authority (CNIL).

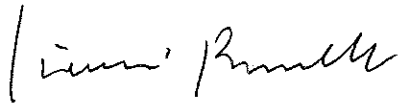
On the basis of the available information, the EDPS does not see any indication to believe that the EIF has not applied the security measures required in the Regulation.

#### 4. Conclusions

There is no reason to believe that there is a breach of the provisions of the Regulation providing the above considerations are fully taken into account. In particular, EIF should:

- ensure that EIF staff in the Compliance and Operational Risk Division in charge of the COR Procedure avoids processing of special categories of data unless one of the exceptions foreseen in Article 10 of the Regulation applies. With this aim, a general warning/provision should be included in EIF Operational compliance procedure (the COR Procedure);
- establish a specific legal basis (i.e. a decision adopted at the appropriate administrative level) authorising EIF to process data under Article 10(5) of the Regulation. The processing of special categories of data should in any case be limited to the extent necessary for complying with legal obligations regarding AML-CFT controls and monitoring activities;
- evaluate for each and every search made for the CDD whether there the latter has a clear and direct link to AML-CFT purposes; and develop and implement effective measures to guarantee a high level of data quality as outlined in Section 3.4. of this Opinion;
- in addition to the data protection notice, endeavour to provide information to data subjects via a separate privacy statement to be sent to counterparties at the beginning of the due diligence process, with a request to forward it to the identified or identifiable natural persons concerned (for example, key persons within the concerned legal person).

Giovanni BUTTARELLI



Cc: Mr Jobst NEUSS, Data Protection Officer, EIF