EUROPEAN DATA PROTECTION SUPERVISOR

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Fund regarding data processing in the context of the transactional due diligence process

Brussels, 10 July 2015 (2014-0725)

1. Proceedings

On 14 July 2014, the European Data Protection Supervisor **(EDPS)** received from the Data Protection Officer (**DPO**) of the European Investment Fund (**EIF**) a notification for prior checking concerning the processing of personal data in the context of EIF transactional due diligence process.

On 29 September 2014, the EPDS also received from the DPO of EIF 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[1]. As indicated by EIF "The notification is to be seen in conjunction with the notification on the transactional due diligence process, of which it forms an integral part"[2]. Therefore, the EDPS has taken into account the relevant information provided in both notifications for the assessment of this case.
The following documents were attached to the notification on the data processing by EIF in the context of the transactional due diligence process:
- EIF Statutes 2014;
- Minutes of the EIF Annual General Meeting held at Lisbon on 18 June 1996;
- Operational Procedures Manual "TRM/EQUITY";
- Operational Procedures Manual "Guarantees, Securitisation & Microfinance";
- EIF transactional and integrity due diligence, data protection note;
- Operational compliance procedure "Compliance and Operational Risks";
- Framework agreement between the European Investment Bank and the European Investment Fund.

Upon EDPS request, EIF provided additional information and clarifications. In particular, EIF DPO provided, by e-mail of 17 December 2014, and –in further modified version– of 24 February 2015, a comprehensive privacy statement (replacing the "data protection note" annexed to the notification), intended to be communicated externally on the EIF institutional website. On 13 May 2015 the EDPS issued his Opinion on the data processing by EIF for the purpose of AML/CFT verifications, whereby analogous assessments were made (for example, in relation to the data retention period; to security measures) in view of the shared features (for

[1] Notification for prior checking filed under the EDPS case number **2014-0908**.
[2] As specified by EIF DPO in his comments to the factual part of the draft Opinion on this 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 needed to complement the transactional due diligence process.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

example, IT tools) of the data processing operations. Hence, the evaluation of such common features in this case 2014-0725 is consistent with the evaluation made as for case 2014-0908.

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

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"[3].

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.

The mission of EIF is to provide risk finance to Small and Medium Sized Enterprises (SMEs). This risk financing is provided through:
- financial guarantees to financial intermediaries, and
- participations in private equity fund and equivalent structures, which, in turn, provide equity finance to SMEs.

2.1 Description of the processing and of its purpose

This Opinion relates to the transactional due diligence process performed as a pre-requirement to receive risk financing investment by EIF. Via the due diligence EIF assesses the eligibility of companies with whom EIF private equity transactions would occur (EIF financial counterparties). Such eligibility check mainly focusses on the moral and professional requirements for the management and possibly other natural persons of the concerned undertakings. For this reason, even though the due diligence is chiefly directed to legal persons, personal data relating to individuals also form the object of the data processing operations. The transactional due diligence process referred to in this context is described in more details by the EIF Operational Procedures Manuals annexed to the notification.

The personal data in this context are processed by the transactional services of EIF and can be accessed by staff members of the transactional services, the Compliance and Operational Risk Division, the Risk ad Portfolio Management, internal audit, the Chief Executive and the Deputy Chief Executive and members of the Board of Directors of EIF.

[3] 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.

2.2 Data subjects

The natural persons whose personal data are processed by EIF in the context of the transactional due diligence process are the following:

- **key persons of management teams for private equity fund structures** in which EIF intends to invest its own financial resources or financial resources under third party mandates[4]. The identification and assessment of these key persons is part of the due diligence process performed by EIF before investing;
- **individuals in business angel companies** that wish to enter into framework agreements with the European Angels Fund (EAF)[5];
- **EIF co-investors** if these are natural persons (exceptional situation).

2.3 Categories of data

The following data categories are collected:

- the *curriculum vitae* of the team members of the fund/business angel company, including the age and professional references;
- professional 'track record' of the team members of the fund/business angel company and other documents spontaneously provided by the company in so far as they include reference to key individuals of the team;
- results of the integrity checks on the fund/business angel's company manager and on its key individuals (via a search on Factiva[6] and a 'general' internet search);
- assessment of the key individuals, including the notes relating to the 'due diligence meeting' with key individuals and to the 'due diligence report'.

In certain circumstances, where it is felt crucial for the commercial success of the transaction because of potential succession problems, health data can also be collected.
Besides, in specific cases, EIF may proceed to inquiries on the creditworthiness of its business partners.

2.4 Categories of recipients to whom data might be disclosed

The personal data processed in this context are not disclosed to third parties, except in the context of financing operations performed by EIF on behalf of third parties (third party mandates). In such cases data may be disclosed to 'mandators' (EIB, European Commission or the competent authorities of the EU Member States).

2.5 Retention periods

The data are retained for a period not exceeding five years following the termination of the business relationship between EIF and the financial counterparty. As the usual lifecycle of the fund structures under which EIF invests is, in line with market practices, 12 years, this entails a total conservation period of personal data of 17 years.

---

[4] The third parties referred to are the EIB, the Commission and public authorities of EU Member States.
[5] EAF is an initiative managed by EIF which helps business angels to increase their investment capacity by co-investing in innovative companies. Instead of granting co-investments on a deal-by-deal basis, the EAF enters into long-term contractual relationships through which the EAF grants a predefined amount upfront to the business angel for future investments. The EAF is a Luxemburg-based fund with regionally focused sub-funds, presently for Germany, Austria and Spain.
[6] Factiva is a business information and research tool which aggregates content from both licensed and free sources, and provides organizations with search, alerting, dissemination, and other information management capabilities.

2.6 Data protection information

As far as information to data subjects is concerned, EIF intends publishing a privacy notice on its website[7].
In addition, the counterparty key persons are specifically informed in the context of the specific due diligence regarding them.

2.7 Data subjects' rights

According to the notification "data subjects are made aware of their rights to access, rectify, block or erase or to object to the collection and storage of their personal data"[8].
The privacy notice specifies that "every person concerned may access his or her personal data and request the actualisation or erasure of such data; he/she may obtain from EIF the blocking of the processing of his/her personal data in accordance with Article 15 of the referred Regulation 45/2001". The e-mail address of EIF DPO is indicated for this purpose in the privacy notice.

2.8 Security measures

The data processing is performed both manually and through automatic means with the support in particular of the following IT tools:
- the internal database for case management "DLM", hosted by EIF at EIF premises in Luxembourg;
- the eFront database, hosted in Paris and managed by a France-based company specialising in IT solutions for the finance industry, in particular private equity and alternatives assets.

DLM is subject to all data protection measures and controls applicable to EIF databases and ICT tools. The eFront database, is physically protected and backed up by the eFront company and is subject to French national data protection law and to the supervision by the French national data protection authority (CNIL)[9].

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. Therefore, the Regulation is applicable.

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*

---

[7] Provided as annex (annex 4) to the notification. Such privacy notice has been replaced by a new one, which has been sent to the EDPS by email of EIF DPO on 17 December 2014 and –in further modified version– on 24 February 2015, which would cover the data processing by EIF in the context of transactional due diligence as well as in the context of AML/CFT verifications.
[8] Point 8 of the notification.
[9] In the notification, EIF specifies that the e-Front database, *"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".

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.

Article 27(2)(b) of the Regulation subjects to prior checking "*processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct*". The aim of the 'transactional due diligence process' may include the *evaluation of personal aspects* relating to the data subjects, in order to assess whether them or the companies they represent are eligible as financial counterparts. Moreover, the processing can result in the *exclusion of individuals from a right, a benefit or a contract* [Article 27(2)(d)] and entail the processing of "data relating to health and to suspected offences, offences, criminal convictions or security measures" [Article 27(2)(a)]. For all these reasons, the processing operation is subject to prior checking.

3.2 Lawfulness of the processing

In the notification EIF points out to "EIF Statutes express[ing] the basic mission of EIF" and to the "decisions of its General Meeting and its Board of Directors".[10]

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 **necessary** for the performance of that task.[11]

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 financing counterparties implying integrity or reputation risks. Moreover, such use would run contrary the objective of rational employment of funds in the interest of the European Union.
Due diligence 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 international business community.
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

[10] EIF notification on transactional due diligence, at point 11.
[11] 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*". In this respect see also recital 27 of the Regulation: "*processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies*".

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" and the "Policy on preventing and deterring corruption, fraud, collusion, coercion, money laundering and the financing of terrorism in European Investment Fund Activities"[12] specify as -'implementing provisions'- EIF *modus operandi* having regard to the due diligence process 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 counterparties adversely affecting the objective of rational employment of funds in the interest of the European Union.

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.

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, unless one of the exceptions under Article 10 applies.

In the notification, the controller states that "in certain circumstances, where it is felt crucial for the commercial success of the transaction because of potential succession problems, **health data** can also be collected"[13].
With reference to these statements, the EDPS draws attention to the fact that processing of health data is prohibited in principle; that it can be performed only if one of the conditions under Article 10 of the Regulation (to be strictly interpreted) applies.
In this regard EIF seems to invoke, as possible exception to the general prohibition, on the provision under Article 10(2)(a), that is the case where "the data subject has given his or her express consent to the processing of those data".
The EDPS recalls that EIF cannot collect such information unless the explicit, **freely given** and informed consent of the data subject has been provided. In this case, we consider that, since the provision of health related data may be requested by EIF as a precondition influencing the investment decision, the qualification of consent as "freely given" is *de facto* problematic.
Most importantly, as described at section 3.4 of this Opinion, the processing of such data in the context of EIF transactional due diligence does not appear in compliance with Article 4(1)(c) of the Regulation (see below Section 3.4).

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*".

[12] Published on EIF website at: http://www.eif.org/attachments/publications/about/anti-fraud_procedures.pdf.
[13] At point 6 of the notification.

From the documentation provided, it appears that data related to (suspected) offences, investigation and prosecution and public criminal records may be processed as part of the counterparty acceptance process and the subsequent counterparty monitoring by EIF.
EIF Statute, EIF Operational Procedures Manuals do 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 these categories of data **should in any case be limited to the extent necessary for carrying out the transactional due diligence procedure**. Appropriate safeguards to ensure necessity, proportionality and data quality should be set out in this respect (see also below Section 3.4).

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; 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 and financing legislation. In particular, this means that references to data related to offences, investigation and prosecution and public criminal records" have to be read as references to such data *as far as they relate to transactional due diligence controls*.

The EDPS recommends that EIF evaluates -for each and every search made- whether the latter has a clear and direct link to the purpose of the due diligence, as well as the degree of 'reliability' of the information collected[14].

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 due diligence should receive a specific data protection training;
- identification of best practices, ensuring that the due diligence are performed with the minimum possible impact on the rights and freedoms of the data subject;
- ensuring that EIF case handlers make a distinction between factual data, opinion data, intelligence data.

As specified in the notification[15] *"the personal data collected may, in exceptional cases, contain **personal data relating to the health** of the data subject"*; *"such data is relevant for the*

[14] 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)" 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 and 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.
[15] At point 16 of the notification.

due diligence and only collected if succession issues of key persons during the time of the investment can be expected. Any such health data is limited to general information on events potentially affecting the health of the data subject as voluntarily communicated by the data subject to EIF. No medical documents are collected, nor is any independent or external due diligence on the health status performed on the data subject concerned".

Under Article 4(1)(c) of the Regulation, the required data and their processing must represent a proportionate system for the purpose (in this case, avoiding financial risks). The EDPS warns that the use of health related data for the assessment of the financial counterparties -taking into account the sensitivity of such data, the invasiveness of their collection[16], even though under a 'voluntary' basis, and the lack of clear definition of the different health data collected -is not proportional and therefore not necessary. Moreover, the EDPS notes that a formal procedure for the handling of such data seems to be missing.
Hence, **the use of health related data by EIF for the purpose of the processing operations notified to the EDPS would not be compliant with the Regulation**.

The processing of data on the "**age**" of the data subjects also does not seem to be relevant for the purpose of the notified data processing. The EDPS therefore recommends EIF to discontinue the processing of this category of data.

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 line with his Opinion on the notification for prior checking on data processing by EIF in the context of AML/CFT verifications (case 2014-0908), where an analogous retention period and the justifications provided by EIF in this regard have been assessed, the EDPS notes that the data retention period applied by EIF can be considered as 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, personal data may be transferred by EIF to EIB for investigation[17], and to EIB, the European Commission and the competent authorities of EU Member States in case of financing decisions to be taken by EIF upon mandate received by the aforementioned Institutions and public authorities.
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, or to data

[16] By email of 18 December 2014 EIF DPO sent back the draft opinion specifying (as comment to the factual part) that "*health data relates mainly on specific illness or threats to the individual health of key persons, if such threats could reasonably result in the need to replace such person. As such replacement may affect a fund's business and performance. Typically health problems such us past strokes are relevant, but also obesity or similar health issues, which may lead to serious problems, may become relevant. The data is collected informally, EIF does not ask systematically for health data, but processes them as part of the due diligence, if by chance and on voluntary basis it gets knowledge of such data*".
[17] Framework Agreement between the European Investment Bank and the European Investment Fund, attached to the notification.

transfers to the European Commission or to the EIB for the performance of EIF duties stipulated in the mandate for investments, 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 transfers under Article 8 of the Regulation, i.e. to recipients not subject to the Regulation, but still subject to the Directive 95/46/EC, are also foreseen (transfers to the competent financial authorities of EU Member States).
In this case, the transfer can be considered as justified if the recipient (the competent financial authority of the EU Member States by which EIF is mandated with the management of funds) "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" [Article 8, letter (a)].
EIF should ensure on a case-by-case basis that the recipient establishes that the data to be transferred are indeed necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority.

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 notice. **The EDPS recommends EIF to expressly mention this possibility both in the notification and in the data protection notice.**

In case of application of the exception under Article 20 of the Regulation, enabling a restricted application of Articles 13-17 of the Regulation, we recall that 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: *"[i]f 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 due diligence. 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 essential to guarantee the quality of the data used and it is of special importance taking into account the sensitivity of the context (due diligence verifications, potentially leading to exclusion from the financing).

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: a) 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; b) 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. In addition, EIF stated that "data subjects concerned are also made aware in the context of the general due diligence process"[18].

In this regard, the EDPS considers that the publication of the procedure on 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 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 latest draft version submitted to the EDPS, the privacy notice, to be published on EIF website, contains the information required under Articles 11 and 12 of the Regulation. Nonetheless, we also remark that the privacy notice contains the e-mail address of EIF DPO for the purpose if the exercise of the data subjects' rights. **Reference in this regard should instead be made to the email address of the controller (EIF Equity Investment).**

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

[18] At point 7 of the notification.

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) seems -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). In this regard, we recall EIF that pursuant to Article 23 of the Regulation, the controller must choose a processor providing sufficient guarantees in respect of the technical and organizational security measures required by Article 22 and ensure compliance with those measures. Moreover, pursuant to Article 23(2), "the carrying out of a processing operation by way of a processor shall be governed by a contract (...) binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller"; and, as laid down under Article 23(3), "for the purposes of keeping proof, the parts of the contract (...) relating to data protection and the requirements relating to the measures referred to in Article 22 shall be in writing or in another equivalent form."

On the basis of the available information, and in analogous way to the assessment made in the Opinion for prior checking on data processing by EIF for the purpose of AML/CFT verifications of 13 May 2015 (Case 2014-0908), the EDPS does not see any indication to believe that the EIF has not applied the security measures required pursuant to Article 22 and 23 of 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:

- evaluate for each and every search made whether there the latter has a clear and direct link to the due diligence for the purpose of verifying the eligibility of the potential EIF counterparties; and develop and implement effective measures to guarantee a high level of data quality as outlined in section 3.4 of this Opinion;
- ensure that EIF staff in charge of the transactional due diligence 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 Manuals of 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 the performance of the due diligence controls and monitoring activities on the financial counterparts;
- not process the health related data referred to in this notification, attached documents, and related correspondence with the EDPS, for the purpose of assessing the eligibility of financial counterparties on the basis of the impact of such data on the fund's performance;
- discontinue the processing of personal data relating to the "age" of the data subjects;
- ensure on a case-by-case basis that the competent national authority of the EU establishes that the data to be transferred are indeed necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority as outlined in Section 3.6 of this Opinion;

• expressly mention both in the notification and in the data protection notice the possibility that EIF applies the exception under Article 20 of the Regulation, enabling a restricted application of Articles 13-17 of the Regulation;
• replace in the data protection notice EIF DPO's e-mail address with the controller's e-mail address for the indication of the person to address for the exercise of the data subject's rights;
• 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 (key persons within the concerned legal person) when EIF requests for information are not directly addressed to natural persons.

Done at Brussels, 10 July 2015.

Giovanni BUTTARELLI