Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding AML-CFT data processing

Brussels, 07 February 2013 (2012-0326)

1. PROCEEDINGS

On 3 April 2012, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data "AML-CFT Data Processing" from the Data Protection Officer (**DPO**) of the European Investment Bank (**EIB**).

The following documents were attached to the notification as supporting documentation:

- Draft Compliance Policy on Counterparty Acceptance and Monitoring, Covering Integrity, Money Laundering and Financing of Terrorism (Integrity and AML-CFT Policy) [and connected documents];
- [...]
- Code of good administrative behaviour for the staff of the European Investment Bank in its relations with the public.

Questions were raised on 13 April 2012 to which the DPO of the EIB replied on 23 May 2012, annexing the following additional documentation:

- EIB Integrity Charter;
- Basel Committee on Banking Supervision: Compliance and the Compliance Function in Banks;
- EIB Statutes;
- Extract from the Audit Committee's report to the Board of Governors 2009;
- Extract from the Audit Committee's report to the Board of Governors 2010;
- []
- AML-CFT questionnaire;
- Compliance Procedure on Counterparty Acceptance and Monitoring, Covering Integrity, Money Laundering and Financing of Terrorism (Integrity and AML-CFT Procedure) [and connected documents];
- [...]

Additional questions were sent on 26 June 2012 and 6 August 2012 and 8 October 2012; answers were received on 30 July 2012, 1 October 2012 and 5 December 2012. The draft Opinion was sent to the DPO for comments on 6 December 2012. The EDPS received a reply on 15 January 2013, following which a meeting between EIB and EDPS was scheduled for 4 February 2013.

2. FACTS

In order to apply best banking practices in the areas of anti money laundering (AML) and combating the financing of terrorism (CFT, together: AML-CFT) and to minimise other

integrity and reputational risks, the EIB Group (consisting of the European Investment Bank and the European Investment Fund) conducts counterparty due diligence (CDD) with regard to its (prospective) business partners.

Before entering into a new business relationship, the EIB performs a "counterparty acceptance process" to assess whether doing so would raise any of the above risks. Counterparties which are considered *a priori* as not raising any particular integrity concerns are subject to a simplified CDD. This is the case for example for counterparties such as credit or financial institutions within the Best Practice Area[1], listed companies within the Best Practice Area or public authorities. By contrast, high risk operations or high risk business relationships, as determined by the Office of the Chief Compliance Officer (**OCCO**) risk assessment and the principles outlines in the EU Directives on AML-CFT[2] require an enhanced due diligence. If this is the case, additional information might be demanded. This can for example be the case if politically exposed persons (PEPs) are involved, charity institutions, high risks compliance operations, etc.

The results of this process feed into the compliance checking for new projects and may lead to the rejection of counterparties or the imposition of additional compliance requirements in the contracts to be signed. Processing starts when the EIB officer considers entering into a business relationship with a new counterparty.

After a business relationship has been established, monitoring of counterparties continues in order to evaluate whether there is a need to revise the initial assessment ("ongoing counterparty relationship monitoring").

The **controller** is the European Investment Bank, with the OCCO mentioned as a contact point.

Data subjects concerned are persons who directly or indirectly own[3] legal entities with which the EIB maintains or plans to enter into business relationships in the context of financing projects and persons entrusted with managing roles in these legal entities ("counterparty key persons"). These are persons with key positions (e.g. chairperson, chief executive officer) and persons sitting on governing bodies (board of directors, management committee, supervisory board, local authorities' council or equivalent) of the counterparty.

If a person in any of the above categories also happens to be a PEP, this is seen as a sign for increased risk. PEPs are defined in Directive 2005/60/EC Art. 3(8)[4] 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.[5] 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

[1] [...]
[2] [...]
[3] This term is to be seen as identical to 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.
[4] cited above.
[5] OJ L 214, 4.8.2006, p. 29–34.

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.

The **data categories** collected in the counterparty acceptance process are the following, according to the notification form:

- identification data;
- data related to offences, investigation and prosecution and public criminal records;
- 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 and websites. The latter two may include news reports on (alleged) illegal behaviour.

A more detailed **description of the processing operation** follows: data collected during the **counterparty acceptance process** are used by the case officer dealing with the EIB operation in question to [assess the counterparty for compliance purposes]. [Case officers shall cover items such as] the identity and background of the counterparty and the operation in question. Among others, [it shall be assessed] whether the counterparty or counterparty key persons have been exposed to allegations of illegal or harmful/disreputable activities or dubious practices[6], whether their wealth is alleged to be derived from illegal activities, or whether they demonstrate inappropriate business behaviour.

[Further assessment shall ascertain] whether they appear in any relevant sanctions list, whether they are under criminal and/or administrative investigation by any relevant authorities, whether they have criminal records, criminal convictions, sanctions or large civil court cases and whether they present other integrity concerns suitable to expose the EIB to reputational risk. This [assessment] is intended to help in evaluating the risk of money laundering, terrorist financing and other compliance risks in line with the EIB's Integrity Charter[7] and the Basel Committee on Banking Supervision's paper on compliance and the compliance function in banks.[8]

If any of these questions are answered with "yes", the OCCO has to be consulted. The OCCO then issues an opinion evaluating the risk posed by the counterparty to be included in or issued alongside of the report submitted to the Board of Directors for approving the business relationship. These reports may include recommendations, such as including integrity covenants in the contract, obliging the counterparty to dismiss sanctioned and/or convicted managers or staff or reporting obligations on the outcome of investigations and compliance with rulings of relevant authorities.

Certain counterparties[9] qualify for simplified due diligence ("SDD"), provided that no specific integrity concerns exist. In this case, documentation requirements are eased.[10]

---

[6] [...]
[7] Available at: http://www.eib.org/attachments/general/occo_charter_en.pdf.
[8] Available at: http://www.bis.org/publ/bcbs113.pdf.
[9] Credit or financial institutions in the best practice area [], listed companies whose securities are admitted to trading on a regulated market within the best practice area, public authorities or other counterparties that meet the technical criteria established in accordance with Article 40(1) (b) of Directive 2005/60/EC.
[10] This mainly refers to the documentation requirements for legal persons.

Operations classified as higher risk are subject to enhanced due diligence ("EDD"). Such a classification may for example occur if there are PEPs involved. This means that on top of the checks mentioned above, additional checks as recommended by OCCO have to be carried out. These may include obtaining identity documents of counterparty key persons, documentary evidence of the beneficial owner's and/or PEPs sources of wealth and a curriculum vitae or declaration of interests of beneficial owner and/or PEP.

If a business relationship is entered into, counterparties remain subject to **ongoing monitoring**. This process includes keeping the information collected during the counterparty acceptance process up to date by conducting regular reviews. Such reviews are to be carried out prior to the first payment, prior to payments if the last payment was made more than a year before, and thereafter as a general rule on an annual basis. Additionally, EIB officers having contact with counterparties shall look for any issues or rumours and certain red flags regarding counterparties. Aside from issues such as whether transactions fall out of the usual pattern or whether there have been recent changes in ownership, these also include whether counterparties (or persons publicly associated with them) have a questionable background or are the subject of news reports indicating possible criminal, civil, or regulatory violations. In case of such red flags, the OCCO is informed. If there are PEPs involved, there is an annual[11] review to see whether they have been entrusted with additional public functions that might raise integrity concerns and whether they have been the subject of prosecution or investigation for illegal activities. Similarly, counterparty key persons are monitored to see whether they have become PEPs, or in case they already are PEPs, whether their functions in the counterparty have changed.

Data obtained both during the counterparty acceptance process and the ongoing monitoring of counterparties may be **transferred** to Members of the EIB governing bodies, EIB internal services, EU institutions and bodies (in particular OLAF) and national financial intelligence units (FIUs). Transfers to external entities will happen either upon request of the recipient or upon the EIB's own initiative for transfers to national FIUs in case of suspicion of money laundering or terrorism financing. Transfers to third countries are not planned.

Data subjects are **informed** of the processing operation in a section in a number of ways. The Integrity and AML-CFT Procedure states that "*personal data submitted to the bank* [in this context] *will be processed in accordance with (EC) Regulation 45/2001*" and that it will be "*processed under the supervision of the EIB Group Chief Compliance Officer (GCCO) and used only for the EIB's AML-CFT purposes*". According to the procedure, data subjects are entitled to "*access, rectify and block*" these data and "*may exercise their rights by contacting the OCCO and/or the European Data Protection Supervisor at any time*". This procedure also gives a general description of the steps the EIB will take in the course of the counterparty acceptance process. According to the notification, the controller will deal with requests for erasure and blocking within 30 working days. The Integrity and AML-CFT Procedure will be available to the public on the EIB website. Also, finance contracts will include a clause on the applicability of the Regulation[12]. The EIB has also announced that it will publish an "ad hoc notice" on compliance with Regulation (EC) 45/2001.

Data are **retained** for ten years after the end of the business relationship. No further processing for scientific or statistical purposes is foreseen.

[11] Or more frequent, if recommended by the OCCO.

[12] The clause reads as follows: "*[t]he processing of personal data shall be carried out by the Bank in accordance with applicable European Union legislation on the protection of individuals with regard to the processing of personal data by the EC institutions and bodies and on the free movement of such data*".

Data are stored electronically in a restricted area of the EIB's servers, subject to general EIB **security rules** (e.g. staff code of conduct, IT standards, and password rules). Paper copies are kept locked in dedicated OCCO cupboards with access restricted to duly authorised OCCO staff.

3. LEGAL ANALYSIS

3.1. Prior checking

The notified operations constitute a processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2(a) of Regulation 45/2001 ("the Regulation")). It is performed by a body of the EU in the exercise of activities which fall within the scope of the Treaties. The processing of the data is done, at least in part, through automatic means. Therefore, the Regulation is applicable.

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 contains a non-exhaustive list of processing operations that are likely to present such risks. Letter (a) mentions among others processing data relating to suspected offences, offences and criminal convictions. Letter (b) mentions processing operations intended to evaluate personal aspects relating to the data subjects, including their conduct. Letter (c) refers to processing operations that allow linkages between data originally processed for different purposes not provided for in national or Union legislation. Finally, letter (d) subjects processing operations that have the purpose of excluding individuals from a contract to prior checking. In the notification, all of these points were mentioned as reasons for prior checking.

As described above in chapter two, data on (suspected) offences may be processed (Article 27(a)). The aim of the counterparty acceptance process is to evaluate personal aspects relating to the data subjects (Article 27(b)), namely their conduct, in order to assess whether they present AML-CFT or integrity/reputation risks. It can also not be excluded that the verifications carried out by EIB officers prior to entering into a contract would lead to link personal data originally processed for different purposes (Article 27(c)). Finally, the processing can well result in the exclusion of individuals from a right a benefit or a contract (Article 27(d)). For all these reasons, the processing operation is subject to prior checking.

The prior checking pursuant to Article 27 of the Regulation should in principle take place before the processing has initiated. In further exchanges with the EDPS, it has been clarified that the notified procedure "*reorganises, completes, modernises and aims to make more consistent and efficient EIB compliance activities, some of which were already in place beforehand*". It has been also stated that this was already indicated to the EDPS in a previous notification made in 2007. Irrespective of whether the EIB communicated or not the existence of this processing, the fact remains that the notified processing activity was in place at the EIB prior to the notification, albeit in a different, less structured form. The present prior-checking does not therefore qualify as a true prior checking, but rather as an ex post one. The EDPS regrets to note that in the present case the notification was not submitted to him in due time, i.e. prior to the start of the processing operations. Any recommendations made in the context of the present opinion should nevertheless be duly implemented by the controller.

The notification of the DPO was received on 3 April 2012. Additional questions were sent on 13 April, 26 June, 6 August and 8 October 2012; answers were received on 23 May, 30 July,

1 October and 5 December 2012. The draft Opinion was sent to the DPO for comments on 6 December 2012. The EDPS received a reply on 15 January 2012. Following these replies, a meeting was scheduled for 4 February 2013. According to Article 27(4) of the Regulation the present Opinion must be delivered within a period of two months. In total, the case has been suspended for 248 days. In consideration of all the periods of suspension, the Opinion must therefore be rendered no later than 11 February 2013.

3.2. Lawfulness of the processing

According to the notification, Article 5(a) and (b) of the Regulation provide the bases for lawfulness**.** 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.[13] For Article 5(b), it has to be established that the controller is subject to a legal obligation to collect and process data which leaves him no space for discretion.[14] The requirement of a legal obligation under Article 5(b) is notably stricter than the requirement of a legal basis under Article 5(a), as a specific obligation leaving to the controller no choice but process is normally required.

3.2.1. Article 5(a)

3.2.1.2. The legal bases submitted by the EIB

In the notification, the controller submitted a number of possible legal bases without specifying which ones were deemed to be grounds for lawfulness under Article 5(a) or 5(b). These provisions are, respectively, Articles 67(3), 75, 215 and 325 of the Treaty on the Functioning of the European Union (TFEU), Protocol N° 5 to the Treaties (EIB Statute), in particular its Articles 16 and 18(1), Directives 2005/60/EC and 2006/70/EC, as well as "*Council Decisions and Regulations adopted under the EU Common Foreign Security Policy*". Several of these provisions do not constitute appropriate legal bases for the notified processing operation, as will be discussed below.

Article 67(3) TFEU is a general provision on the Area of Freedom, Security and Justice (AFSJ), stating that the Union "*shall endeavour to* [...] *prevent and combat crime*". This provision is too general to serve as a direct basis for processing activities by the EIB under Article 5(a) - from this text alone, the EIB's behaviour would not be foreseeable. For example, data subjects would not be in a position to understand the extent to which personal data about themselves might be collected and further processed. Additionally, the notified processing operations also relate to the evaluation of data subjects in terms of "reputational risks" which do not rise to the threshold of "crime".

Article 325 TFEU establishes in its first paragraph that the "*Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures to be taken in accordance with this Article* [...]". The remainder of this Article sets out tasks for the Commission and the Member States and authorises the Union co-legislators to adopt the necessary measures to this end. Apart from the general provision in the first paragraph, there is no indication on specific actions to be taken. As with

[13] 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*".

[14] Article 5(b) authorises processing that is "*necessary for compliance with a legal obligation to which the controller is subject*".

Article 67(3) TFEU, this provision is too general to serve on its own as a direct legal basis for the EIB's processing operations in the context of AML-CFT under Article 5(a).

The controller mentions also Articles 75 and 215 TFEU. These two provisions authorise the Union to adopt legislation on the freezing of assets, but do not in themselves authorise any asset freezing or require the checking of customers against sanctions list. The EIB's processing operations can therefore not be based directly on these Treaty provisions. On the other hand, the regulations and decisions adopted on the basis of these provisions can constitute the legal basis for a part of the notified processing, namely the checks performed by the EIB in order to verify that the counterparty is not included in any relevant sanction list.[15] However, they do not cover the other parts of the processing relating to AML-CFT and reputational risks. The reference to such provision cannot therefore be deemed sufficient to justify processing activity as a whole but only a part thereof.

Having regard to the wider European AML-CFT legislation, the controller refers in the notification to Directives 2005/60/EC and 2006/70/EC as possible legal bases. These Directives lay down the legislative framework concerning the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter: "AML-CFT Directives"). As all directives, they are directed to Member States and as such are not directly applicable to the EIB. Furthermore, the Directive are not *per se* directly applicable because they need to be implemented at national level by national legislative provisions. The EDPS therefore excludes that the AML-CFT Directives can *directly* constitute the legal basis for the present processing operations.

In conclusion, most of the legal bases mentioned by the controller in the notification do not appear to be appropriate for the purpose of Article 5(a) of the Regulation. In the following, the EDPS will examine those possible legal bases that could legitimise the processing.

3.2.1.3. Possible legal bases

The EDPS considers that the legal basis for the purpose of Article 5(a) must be found in legal provisions which are directly applicable to the EIB, such as its Statute and the provisions adopted by EIB organs on the basis thereof. In particular, Article 18(1) of the EIB's Statute states that the EIB "*shall ensure that its funds are employed as rationally as possible in the interests of the Union*". This essential obligation implies for the EIB the duty to make sure, among others, that its resources are not used for money laundering or terrorism financing purposes. To the same extent, 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 Union. Such transactions would reflect adversely on the image of the EIB as a public institution administering EU funds and endanger the Bank's reputation itself.

Moreover, Article 12 of EIB Statute tasks the Audit Committee with verifying "*that the activities of the Bank conform to best banking practice*". AML-CFT verifications (i.e. CDD) undoubtedly form part of best banking practice in Europe and beyond, as recognised by

[15] In total, there are about 20 Regulations imposing restrictive measures including asset freezes in force, based on Article 215 TFEU or other, older, legal bases. While the provisions contained therein differ slightly, all acts based on these Articles include provisions essentially equivalent to Article 2 of Regulation (EC) 881/2002, which states that "[a]ll funds and economic resources belonging to, owned, held or controlled by a natural or legal person, entity, body or group listed [...] shall be frozen." and that "no funds or economic resources shall be made available, directly or indirectly, to, or for the benefit" of listed persons and entities. If funds are nonetheless made available to such persons or entities, those doing so are subject to sanctions such as fines (Article 10 of Regulation 881/2002) unless they "did not know, and had no reasonable cause to suspect" that their actions would infringe these provisions (Article 2(2) of Regulation 881/2002).

FATF[16] recommendations in this field. To a certain extent, measures aimed at avoiding business relationship with counterparties presenting integrity and reputational risks can also be seen as best banking practice.[17] The integrity/reputation risks assume even greater importance for public international financial institutions as the EIB than for national commercial banks. Particular attention is therefore required to avoid that the reputation of the EIB is put at risk by engaging in transactions with non reputable individuals.

While the above provisions can in principle be used as legal bases, the EDPS believes that they are too general and vague to constitute in themselves a sufficient ground for the processing at stake. In other words, the general obligations pursuant to Articles 12 and 18(1) of the EIB Statute need to be implemented and made more concrete and specific. In particular, it is indispensable for the EIB to precisely identify and define what is to be considered as "best banking practice" under Article 12 for the purpose of AML-CFT processing.

In this respect, the EDPS takes note of the work undertaken by the EIB in order to set out a framework for the identification of best banking practice for the purpose of Article 12 of the Statute. In particular, the EIB Integrity Charter adopted by the Management Committee sets out the principle according to which the EIB Group shall carry out its tasks "*in compliance with generally accepted standards of good financial and administrative practice [...]*". Likewise, it states that OCCO shall contribute to "*ensuring that the EIB Group conforms with the applicable legislation, rules, regulations and generally accepted professional practices and standards [...]*". It further specifies that "*this concerns the prevention of money laundering, corruption, and the use of funds for terrorist purposes [...]*".

Furthermore, the EIB Management Committee declared that the EIB "*continues to submit itself voluntarily to the applicable requirements of core EU legislation and relevant standards applicable to the banking sector*" (emphasis added)[18], meaning primarily the AML-CFT Directives and the FATF recommendations. To this end, the Management Committee and the Board of Directors adopted a framework for compliance with best banking practices (the "Framework"), based on the Directives mentioned above and several other texts. The Audit Committee took the decision that best practices at the EIB are to be "*based on the principles laid down*" in them. The Audit Committee further issued a document outlining the procedure to be followed by EIB officers in performing AML-CFT checks (the "Procedure"). The Procedure is also complemented by [...] additional details concerning these checks. The Framework is based essentially on the Integrity and AML-CFT Procedure and the corresponding [connected documents]. The Framework was thereafter notified to the Board of Governors.

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 and ongoing monitoring, the EIB 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 the EIB. It should be borne in mind, however, that necessity is a question of degree, and the controller

[16] Financial Action task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations.

[17] See, e.g., Basel Committee on Banking Supervision, Compliance and the compliance function in banks, April 2005: "*The expression "compliance risk" is defined in this paper as the risk of legal or regulatory sanctions, material financial loss, or loss or reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self regulatory organisation standards, and codes of conduct applicable to its banking activities*" (emphasis supplied), see p. 7.

[18] Response of the Management Committee to the Annual Reports of the Audit Committee for the Year 2010, p. 1 (annexed to The Audit Committee's Annual Report To The Board Of Governors For The 2010 Financial Year).

must ensure that such monitoring does not exceed what is appropriate and proportionate to the aim pursued. These aspects will be analysed in Section 3.4 below.

In view of the above, the EDPS considers that the combination of the EIB Statute provisions and the related implementing provisions (i.e. Integrity Charter, the Framework, the Procedure and the [connected documents]) may constitute in principle a sufficient legal basis for the purposes of Article 5(a) of the Regulation. However, not all these documents are published, but only the Integrity Charter and the Procedure. Furthermore, the information included in the documents that are published (the Charter and the Procedure) is not comprehensive. For the sake of clarity and transparency, the EDPS recommends that the Procedure be integrated with some additional information concerning the type of controls carried out on physical persons, as detailed in the relevant Directives and/or [connected documents] (see, e.g., the information on Counterparty Key Persons, enhanced and simplified counterparty due diligence, PEPs', etc.). The EDPS is aware of the argument that providing too much detail in the published documents could facilitate attempts to circumvent AML-CFT measures. However, in the interest of legal certainty, EIB practices should be made more transparent. As for the level of detail, the 40 recommendations of the FATF and their interpretive notes[19] provide a standard of what can be disclosed without jeopardising the efficacy of AML-CFT measures.

3.2.2. Article 5(b)

For Article 5(b) to be applicable, it has to be established that the controller is subject to a legal obligation to collect and process data which leaves him no space for discretion. For the reasons in part already highlighted above, the EDPS takes the view that the provisions indicated by the EIB cannot be considered for the purpose of Article 5(b).

Article 67(3) TFEU states that the Union shall endeavour to prevent and combat crime, but does not contain any specific obligation mandating the EIB to set out an AML-CFT scheme. The same applies to Article 325 TFEU which merely states the general principle that the Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through specific measures to be adopted by the Commission and Member States. Articles 75 and 215 TFEU are not directly relevant for the EIB for the reasons explained above in Section 3.2.1. The same applies to the AML-CFT Directives because they are not applicable to the EIB.

Article 12 and 18(1) of the Statute set general obligations for the EIB (i) to employ its funds as rationally as possible in the interest of the Union and (ii) to comply with best banking practices. As already highlighted, for Article 5(b) to apply, it has to be established that the controller is subject to a legal obligation to collect and process data which leaves him no space for discretion. The specific processing operations must be directly imposed by the Treaty or a legal act adopted on the basis thereof. The above provisions do not directly establish any specific obligation concerning AML-CFT processing. The EDPS therefore is not persuaded that Article 5(b) is applicable in the present case.

3.3. Processing of special categories of data

Article 10(1) 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 heath or sex life. The processing of these special categories of data is prohibited

[19] http://www.fatf-gafi.org/documents/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

unless one of the exceptions under Article 10(2) applies. Account should also be taken of Article 10(4) of the Regulation stating that "*"[s]ubject to the provision of appropriate safeguards, and for reasons of substantial public interest, exemptions in addition to those laid down in paragraph 2 may be laid down by the [EU Treaties] or other legal instruments adopted on the basis thereof or, if necessary, by decision of the European Data Protection Supervisor*".

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. In these cases, the EDPS reminds that the prohibition under Article 10(1) must be respected or otherwise it has to be evaluated in a restricted manner whether the application of an exception would be necessary. In any case, EIB staff in charge of the files must be made aware of this rule and avoid processing special categories of data unless one of the exceptions foreseen in Article 10.2 or Article 10.4 applies. This principle can take the form of a general provision to be included in the AML-CFT Explanatory Notes.

Article 10(5) 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 (suspected) offences may be processed as part of the counterparty acceptance process and the subsequent counterparty monitoring. The AML-CFT Framework does not appear to contain any specific reference to the fact that EIB would be collecting and processing data relating to offences under Article 10(5).

The EDPS therefore recommends that the EIB adopts a specific legal basis (a decision at the appropriate administrative level) authorising the EIB to process data under Article 10(5) in application of the relevant provisions of the Treaty or the Statute. 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. Appropriate safeguards to ensure necessity, proportionality and data quality should be set out in this respect (see also below 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. This includes that 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 (Article 4(1)(d)).

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 "*criminal and/or administrative investigation*", "*criminal records, criminal convictions or large civil court cases*" etc. have to be read as references to such data as far as they relate to compliance with AML-CFT obligations. Additionally, for some of the questions asked, the link to AML-CFT purposes is not always clear. This applies for example to allegations of "*dubious practices*" or "*other integrity risks*". The EDPS recommends that the EIB evaluates for each and every question

asked whether there is a clear and direct link to AML-CFT purposes and explain and justify these links to the EDPS. Questions that have no such link will have to be removed. Furthermore, the provisions imposing certain verifications should be interpreted in a balanced way in accordance with proportionality and other data protection requirements.

Some of the data categories can reasonably assumed to be of high enough 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, which might be based on press reports, this cannot be affirmed so easily. Here, the EIB 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 EIB 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.

Furthermore, the EDPS suggests that the EIB implements effective measures to guarantee a high level of data quality. These measures should for example cover the following essential areas[20]:

- case handlers performing the CDD should receive training on how to conduct it in a manner which is compliant with data protection requirements;
- identification of good and bad AML-CFT practices, in particular with regard to KYC, CDD practices, questionnaire filling, reporting and ongonig monitoring.
- avoidance of the use of profiling techniques;
- listing and delisting procedures and mechanisms for reassessment and periodic review;
- the principle of ensuring accuracy of public sources;
- a description of if and how the organisation makes a distinction between factual data, opinion data, intelligence data and the data collected for different categories of data subjects;
- strict and clear application of the purpose limitation principle, especially with regard to transfers.

The EDPS recommends that the EIB develops and implements effective measures to guarantee a high level of data quality as outlined above.

3.5. Conservation of data / Data retention

Personal data shall not be kept in a form which permits identification of data of data subjects for longer than is necessary for which the data are collected and/or further processed (Article (4)(1)(e)).

As outlined in the descriptive part of this opinion, data are kept for ten years. No further processing for scientific or statistical purposes is foreseen.

While not directly applicable, the retention periods in Directive 2005/60/EC and the national legislation implementing it can provide guidance for appropriate retention periods. Article 30 of this Directive sets out that such data shall be stored "*at least five years*". A vast majority of

[20] See in this respect Article 29 Working Party Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, pp. 15-16.

Member States implements a retention period of five years.[21] The EDPS has not received clear evidence as to why the EIB would need a significantly longer retention period, when overwhelming practice suggests that a retention period of five years is sufficient. The controller has however expressed concerns that 5 years retention would not be enough in cases where documentation would be requested after this period for example in the context of Court litigations, in particular in third countries. The EIB also maintained that, as a matter of fact, it has only limited experience to date in the field of AML-CFT and therefore is not in a position to evaluate whether a 10 year conservation period is sufficient or excessive. Experience may thus teach that this period should be changed. Considering these reasons, the EDPS suggests that when the EIB has experienced the first 10 years of practice in the field of AML-CFT an evaluation of the necessity of the 10 years period should be conducted. On the basis of such evaluation, EIB should be able to demonstrate whether such longer conservation period is indeed necessary.

3.6. Transfer of data

Transfers of data to recipients which are subject to the Regulation are governed by Article 7 thereof; transfers to recipients subject to the national laws implementing Directive 95/46/EC are regulated by Article 8 of the Regulation, while transfers to recipients not subject to such laws have to follow the rules set out in Article 9 of the Regulation.

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*". Article 7 transfers occur both within the EIB and to other Union institutions or bodies. Internal transfers may happen to the extent necessary for reaching funding decisions and internal control functions. According to information obtained from the EIB, transfers to other EU institutions and bodies would mostly concern transfers to OLAF, while the Court of Auditors could also receive data. Insofar as these transfers relate to the investigation of specific cases, they are in principle covered under 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.

Transfers to the FIUs of Member States will be subject to either Article 8 or Article 9 of the Regulation, depending on the implementation of Directive 95/46/EC in the Member State in question: while the scope of the Directive itself excludes law-enforcement activities, many Member States have chosen to implement the Directive on a horizontal basis with one law covering all sectors. With respect to those Member States, transfers to their national FIUs fall under Article 8. Article 8(a) allows transfers of personal data to such recipients "*if the recipient 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*".

In the view of the EDPS this provision should be construed as meaning that if the information is not being sent at the recipient's request, it is the sender's task to verify that the transfer is necessary. Thus, where the EIB sends personal data to investigative bodies in a Member State, it should establish that those data are necessary for the performance of a task carried out in the public interest. This provision covers transfers to FIUs if there are reasonable grounds for suspecting money laundering or terrorist financing in accordance with the principle

[21] 25 out of 27 Member States adopted a retention period of 5 years; only Spain and Slovenia adopted a retention period of 6 years. See Commission Staff Working Paper: Compliance with the anti-money laundering directive by cross-border banking groups at group level, SEC (2009) 939 final, pages 50-51.

established in Article 22 of Directive 2005/60/EC. A case by case analysis is however required to establish necessity *in concreto*.

Regarding Member States which excluded such activities from the scope of their laws implementing Directive 95/46/EC, Article 9 is applicable. Article 9(1) authorises such transfers only if there is an adequate level of protection in the recipient country. As these recipients are both Member States of the EU and signatories of Council of Europe Convention 108[22], there is, in principle, a presumption of adequate level of protection. Additionally, in specific cases, the derogation in Article 9(6)(d) ("*necessary* [...] *on important public interest grounds*") could be used. However, the exception should be interpreted restrictively and subject to a case by case analysis.

According to the notification, no other transfers under Article 9, e.g. to third countries, are foreseen.

3.7. Rights of access and rectification

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, the EIB mentioned that these rights might be limited in accordance with Article 20(1) (a), (b) and (c) of the Regulation.

According to the EIB, the case of Article 20(1) (a) (prevention, investigation, detection and prosecution of criminal offences) would be the most common reason to deny access. The EDPS highlights that 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. Appropriate procedures should be put in place to allow the exercise of these rights in these cases.

In any case, paragraph 3 of Article 20 has to be considered and respected by the EIB: *"[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."* Concerning the right to information, this provision has to be read jointly with Articles 11, 12 and 20 of the Regulation (see below point 2.2.9).

Moreover, 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 process, 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 EIB 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.

[22] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.

Article 14 of the Regulation provides the data subject with a right to rectify inaccurate or incomplete data. Given the sensitivity, in most situations, of these cases, this right is of key importance, in order to guarantee the quality of the data used, which, in this specific case, is connected to the right of defence. Any restriction, as provided in Article 20 of the Regulation, has to be applied in the light of what has been said regarding the right of access in the paragraphs above.

3.8. Information to the data subject

The information to be provided to data subjects must comprise at least the following (see Articles 11 and 12 of the Regulation):

- Identity of the controller;
- Purposes of the processing operation;
- Recipients or categories of recipients;
- Categories of data collected;
- Existence of the rights to access and rectification;
- Legal basis for the processing;
- Retention periods;
- The right to have recourse to the EDPS;
- For data collected from the data subject, whether replies are voluntary or mandatory as well as possible consequences of failure to reply;
- For data not collected from the data subject, the origin of the data, except where the controller cannot divulge this for reasons of professional secrecy.

The EIB will publish the rules and procedures on AML-CFT (i.e. the Integrity and AML-CFT Procedure) on its website and include a notice on the applicability of Regulation 45/2001 in its funding contracts. While this latter notice can serve to raise awareness of the applicable data protection legislation, it is not on its own sufficient, not least because it would reach data subjects at a too late stage (well after processing has begun).

Concerning the 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 affective manner. As a matter of fact, not all possible data subjects would read the information published on the website. The EDPS therefore considers that 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 persons concerned (for example within the organisation).

Having regard to the substance of the Procedure, the EDPS notes that, as it currently stands, the Integrity and AML-CFT Procedure fails to inform data subjects about the (categories of) recipients of data, to mention a clear legal basis for the processing and to provide a complete list of data categories. Neither does it inform about the possible consequences of declining to provide information (when it is collected from the data subjects directly) nor about the sources of data collected from other sources.

Additionally, the reference to exercising data subject rights "*by contacting the OCCO and/or the European Data Protection Supervisor*" should be replaced by a reference along the lines of "data subjects can exercise their rights by contacting the controller; they have the right to

recourse to the European Data Protection Supervisor at any time", making the distinction between their roles clearer. It should also include contact information for the controller. All the shortcomings mentioned in this heading must be rectified.

3.9. Automated individual decisions

Article 19 of the Regulation provides that "*[t]he data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken*".

The EDPS reminds the EIB that all expert systems should be used as an information and warning element to support decision making of the Board of Directors and may not replace the final decision to be taken after human analysis.

3.10 Security measures

After careful analysis of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

4. CONCLUSION

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations contained in this Opinion are fully taken into account. In particular, the EIB should:

- ensure that EIB staff in charge of the files be made aware of the rules concerning special categories of data under Article 10 of the Regulation and avoid processing of special categories of data unless one of the exceptions foreseen in Article 10.2 or Article 10.4 applies. This can take the form of a general provision to be included in the AML-CFT [documents];
- integrate the Procedure with additional information concerning the type of controls carried out on physical persons, as detailed in the relevant EU Directives and/or the [connected documents] (see, e.g., the information on Counterparty Key Persons, enhanced and simplified counterparty due diligence, PEPs', etc.);
- establish a legal base authorising the EIB to process data under Article 10(5) by means of a decision adopted at the appropriate administrative level. 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;
- Evaluate for each and every question asked [...] whether there is a clear and direct link to AML-CFT purposes, explain and justify these links to the EDPS and [avoid] questions that have no such link;
- Develop and implement effective measures to guarantee a high level of data quality as discussed in Section 3.4;
- conduct an evaluation of the necessity of the 10 years conservation period when EIB has experienced 10 years of practice in the field of AML-CFT and report to the EDPS about the necessity thereof;

- Use restrictions on the rights of access and rectification only on a case-by-case basis and only as long as necessary for; appropriate procedures should be put in place to allow for the exercise of these rights after the fact in these cases;
- Replace the reference to exercising data subject rights "*by contacting the OCCO and/or the European Data Protection Supervisor*" by a reference along the lines of "data subjects can exercise their rights by contacting the controller; they have the right to recourse to the European Data Protection Supervisor at any time";
- Rectify the current deficiencies in the information supplied to data subjects as described in Section 3.8;
- Provide information to data subjects in a separate privacy notice to be published on the EIB's website and to be sent to new counterparties at the beginning of the counterparty acceptance process, with a request to forward it to the identified or identifiable persons concerned (for example within the organisation).

Done at Brussels, 7 February 2013.

(**signed**)

Giovanni BUTTARELLI
Assistant European data Protection Supervisor