From: [redacted]

To: [redacted]; European Data Protection Supervisor <EDPS@edps.europa.eu>

CC: [redacted]

Sent at: 05/01/17 15:51:52

Subject: RE: 2015-0633 EDPS Inspection Report

Dear [redacted],

First of all, Happy New Year and all my best wishes for 2017!

We thank you for the extension granted for the implementation of your recommendations. After having consulted [redacted], please find attached the action plan and annexes proposed by IG/IN regarding investigations. We propose practical solutions to implement your recommendations that, we hope, will satisfy your requirements. Regarding recommendation 11 related to transfers on the basis of consent of the data subject, we would like to discuss further with you as explained in the attached document. In addition, we clarify some issues regarding Code of Conduct investigations in relation to recommendations 1 and 10.

After having received your feedback on these proposed solutions, we will amend our DP internal guidance accordingly for issuance as soon as practicable.

We remain available to clarify any point.

Kind regards,
[redacted]

[redacted]
Fraud Investigations Division
European Investment Bank
100, boulevard Konrad Adenauer
L-2950 Luxembourg
Tel. +352 43 79 89 548
Mob. +352 621 26 26 85
Fax. +352 43 79 64 000

From: [redacted]
Date: 9 December 2016 at 09:46:24 GMT+1
To: [redacted]
Cc: [redacted] "European Data Protection Supervisor" <EDPS@edps.europa.eu>, [redacted]

[redacted]

Subject: RE: 2015-0633 EDPS Inspection Report

Dear [redacted],

We refer to your email of 1 December 2016.

We regret that:

- the EIB has not informed us before the expiry date about any concerns and difficulties that EIB might experience in context of the smooth implementation of the EDPS recommendations
- none of the recommendations has been implemented so far;
- the action plan proposed for D@W procedures includes extended deadlines until 30/12/2018, i.e. more than two years from now, without providing us with a proper justification.

Although we understand that the implementation of some recommendations may need more time because they involve the EIB as a whole (e.g. those linked to the implementation of a new CMS), several recommendations could have been implemented within shorter period as their implementation should not cause a significant increase of work required (e.g. slight modifications of internal documents). More importantly, other recommendations should have been implemented as non-compliance may involve risks for the EIB.
We hope that EIB is fully aware of the importance to implement those recommendations that are related to the compliance with Regulation 45/2001.

As regards IG/IN investigations:

- ***Recommendations Nos. 1, 7, 10 and 11*** are easy to implement, as they require some slight adaptations to existing internal documents.
- ***Recommendations Nos. 2-5***: non-implementation of these recommendations leads to non-compliance with Regulation 45/2001 as regards information to the data subjects. This may put the EIB at risk (e.g. claims for damages, loss of reputation), for example, if a person under investigation decides to challenge a decision made by the EIB based on data processed unlawfully.
- ***Recommendations Nos. 6 and 9*** are features to be added to the new CMS, which we understand is not yet in operation.
- ***Recommendation No. 8***: this recommendation requires to document a legal analysis obligation and to adapt internal guidance accordingly. This will ensure that sensitive personal data transfers outside the EU institutions occur in compliance with Regulation 45/2001. Data transferred unlawfully to national investigating authorities may have an adverse effect on national investigations and may cause reputational damage to the EIB.

As regards D@W policy:

- ***Recommendation No. 12***: we note that the EIB will send us the prior checking notification on the selection of confidential counsellors by 31/01/2017.
- ***Recommendation Nos. 13 and 22***: these recommendations require a revision of the D@W policy. We understand that this review may take some time and have noted the deadline of 31/12/2017 for adoption. However, we would like to be informed about the ongoing process and receive an update of the prior checking notification (original case number: 2004-0067) as regards the harassment procedure in due time before the entry into force of the revised policy (cf. Article 27(2) of Regulation 45/2001).
- ***Recommendation No. 14***: we note that the EIB will implement this recommendation by 01/02/2017.

- ***Recommendation No. 15***: the implementation of the recommendation (centralisation of documents) should not wait until the adoption of the new policy. It can be implemented easily, at least for new cases.
- ***Recommendations Nos. 16-19***: The EIB makes the implementation of the recommendations depend upon the adoption of a new D@W policy, hence no implementation until 30/06/2018. However, non-implementation of these recommendations leads to non-compliance with Regulation 45/2001 as regards the information of data subjects. This may put EIB at risk (e.g. loss of reputation, claims for damages), for example if a staff member convicted of harassment decides to challenge the EIB decision in court. Therefore, the EIB should implement these recommendations based on the existing policy and not postpone the implementation until the adoption of the new policy.
- ***Recommendation No. 20***: it includes features to be added to the new CMS, which we understand is not yet in operation.
- ***Recommendation No. 21***: This practice can indeed be included in the revised policy but should be implemented as from now to new cases, otherwise non-compliance can put the legality of anti-harassment procedures and consecutive decisions at risk.
- ***Recommendations Nos. 23-24***: these recommendations on archiving/destruction should be implemented without waiting the adoption of a new D@W policy. The risk for the EIB here is the excessive retention of sensitive data in personal file or accidental destruction of data before due date, which may have consequences on the situation of individuals concerned.

* *
*

Therefore, we kindly ask the EIB to provide us with a **revised planning of implementation** with new deadlines taking into account the above-mentioned observations **by 9 January 2017**.

Could you please also draw the controllers' attention to the EDPS enforcement powers under Article 47 of Regulation 45/2001?

We are at your disposal for any questions.
Kind regards,

[redacted]

From: [redacted]
Sent: 01 December 2016 15:45
To: [redacted]
Cc: [redacted]
Subject: 2015-0633 EDPS Inspection Report

Dear [redacted]
I am refering to the deadline of 1st December 2016 - established on the EDPS Inspection Report to the EIB conclusion letter, addressed to [redacted] -, for the EIB to adopt measures in order to comply with the EDPS Recomendations.
Unfortunately it was not yet possible to adopt it all.
In what concerns Personnel and the Recomendations regarding D&W procedures I enclose an "Action Plan" and we would like to have your viwes on it.
In what regards IG-IN recomendations we still need an extension of the assigned period. Could you please give us more 6 months ?
Thanks in advance for your understanding

B regards
[redacted]

Les informations contenues dans ce message et/ou ses annexes sont reservees a l'attention et a l'utilisation de leur destinataire et peuvent etre
confidentielles. Si vous n'etes pas destinataire de ce message, vous etes
informes que vous l'avez recu par erreur et que toute utilisation en est
interdite. Dans ce cas, vous etes pries de le detruire et d'en informer la
Banque Europeenne d'Investissement.
The information in this message and/or attachments is intended solely for
the attention and use of the named addressee and may be confidential. If
you are not the intended recipient, you are hereby notified that you have
received this transmittal in error and that any use of it is prohibited. In
such a case please delete this message and kindly notify the European
Investment Bank accordingly.

Les informations contenues dans ce message et/ou ses annexes sont reservees a l'attention et a l'utilisation de leur destinataire et peuvent etre confidentielles. Si vous n'etes pas destinataire de ce message, vous etes informes que vous l'avez recu par erreur et que toute utilisation en est interdite. Dans ce cas, vous etes pries de le detruire et d'en informer la Banque Europeenne d'Investissement.
The information in this message and/or attachments is intended solely for the attention and use of the named addressee and may be confidential. If you are not the intended recipient, you are hereby notified that you have received this transmittal in error and that any use of it is prohibited. In such a case please delete this message and kindly notify the European Investment Bank accordingly.

EDPS INSPECTION REPORT DATED 27 JULY 2016

Fraud investigations
Action plan for implementation of EDPS Recommendations

General recommendation		
1	Clarify the scope of EIB Investigation Procedures by including a reference to EIB Codes of Conduct in the introductory part (the current version only refers to EIB Anti-Fraud Policy) and by excluding harassment investigations from their scope.	IG/IN is not in charge of investigating Code of Conduct breaches; this is within the remit of the Office of the Chief Compliance Officer (OCCO). IG/IN has provided in the past assistance to OCCO on Code of Conduct cases but the full responsibility regarding Code of Conduct's breaches remains with OCCO. For this purpose, IG/IN considers that there is no need to clarify the scope of EIB investigation Procedures.
Information		
2	Draft a data protection statement meeting all the requirements of Articles 11 and 12 of the Regulation (information on the controller, the purpose of the processing - including the scope of IG/IN activities, the legal basis, the data processed, the recipients of the data, the retention period, the rights of the data subject and the origin of the data); Publish this data protection statement on the EIB website and intranet;	Comprehensive draft data protection statement available as annex 1. This statement is still subject to internal clearance at EIB before publication. Implementation date: The statement will be published on EIB and EIF's websites and intranets as soon the necessary internal clearance process and necessary IT development will be completed.
3	Complete the privacy statement used by IG/IN in their template for outgoing correspondence by including a link to the data protection statement referred to in Recommendation No. 2	The following sentence will be added in the privacy statement in parallel to the publication of the data protection statement on EIB's website: "*The related data protection statement may be accessed on the EIB group's website under the following link […].".*
4	Ensure that each person involved in a case (suspects, informants, whistleblowers and witnesses) is informed and provided with the data protection statement, according to Articles 11 and 12 of the Regulation, including during the assessment phase, unless a limitation under Article 20 of the Regulation applies. Adapt the DP Guidance for IG/IN accordingly.	IG/IN already inform relevant data subjects with whom it is in direct contact during the assessment phase about the processing of their data through the privacy statement, notably the informant, the whistleblower and witnesses already contacted at assessment stage. This practice will be duly reflected in the DP Guidance, also including others relevant data subjects such as person concerned if already identified at assessment stage, unless a limitation under Article 20 applies. Implementation date: Q1 2017
5	In cases where the EIB decides to apply a restriction of information, access, rectification etc. under Article 20(1) of the Regulation, or to defer the application of Article 20(3) and 20(4), such decision should be taken strictly on a case by case basis and duly documented in the file. Adapt the DP Guidance for IG/IN accordingly.	Awaiting the development of IG/IN's CMS, the following interim measure will be implemented: deferrals will be documented by preparing a note to the file to be stored in the case file in GED. See templates in annexes 2a and 2b. The procedure will be reflected in IG/IN internal procedures, including the DP Guidance. Implementation date: Q1 2017
6	Make sure that the future IG/IN CMS is featured in	This feature will be provided in IG/IN's CMS – see

	such a way so as to identify easily in each case file, (i) per each data subject whether information in accordance with Articles 11 and 12 of the Regulation was provided and (ii) whether there was a restriction or deferral of the information in accordance with Article 20 of the Regulation.	print screens in annex 3. Status of implementation: The procedure to procure IG/IN's CMS had to be cancelled because the selected provider was unable to perform the requested services. The process has to be relaunched.
Transfers		
7	Delete the last sentence of the template of the clause used by IG/IN when transferring data to other EIB entities (p. 6 of the DP Guidance for IG/IN dated 30 November 2015).	In order to prevent undue transfer of personal data within EIB, IG/IN will keep this sentence but will revise it as follows in order to take into account the EDPS' recommendation: *"Recipients cannot forward this note or disclose its contents to others without the Head of IG/IN's prior knowledge and authorisation."* Implementation date: already done
8	Before transferring personal data to entities outside the EIB, ensure that the conditions of Articles 8 or 9 of the Regulation (depending on the recipients) are fulfilled and keep documentation of any assessment made by the EIB in this respect. Adapt the DP Guidance for IG/IN accordingly.	Awaiting the development of IG/IN's CMS, the following interim measure will be implemented: a note to the file will be prepared, in case of transfers of personal data under Articles 8 or 9, and stored in the case file in GED. See template in annex 4. The procedure will be reflected in the DP Guidance. Implementation date: Q1 2017
9	When implementing the future CMS, make sure that it is featured in such a way as to identify easily, in each case, if personal data were transferred (internally and externally), to whom, the legal basis for the transfer and the data transfer document (with underlying documents to support, justify and explain the transfer).	This feature will be provided in IG/IN's CMS – see print screens in annex 5. Status of implementation: the procedure to procure a CMS had to be cancelled because the selected provider was unable to perform the requested services. The process has to be relaunched.
10	Update EIB Investigation procedures to IG/IN practice as regards the notification of investigation cases to OLAF and the recipients of the quarterly status report of ongoing investigations.	Notification to OLAF: as mentioned in the context of recommendation 1, IG/IN is not in charge of investigating Code of Conduct breaches; this is within the remit of the Office of the Chief Compliance Officer (OCCO). The notification to OLAF, as currently described in the Investigation Procedures, is therefore valid. Status report: The fact that status reports are also sent to external auditors will be added in the Investigations Procedures during its next review Date of implementation: the next review of the Investigation Procedures will start in 2018.
11	Modify the DP Guidance for IG/IN so as not to rely exclusively on data subject's consent for transfers.	IG/IN may have legitimate reasons to rely exclusively on a data subject's consent for transferring data on the basis of article 9(6)(a) of the Regulation, e.g. transfer of the contact details of a national authority member with his/her prior knowledge and consent to an EIB partner. IG/IN would then need to keep the possibility for certain cases to rely exclusively on article 9(6)(a) in its DP Guidance. In any case, the transfer will always be done only if the recipient has a legitimate reason to access the data.

[LOGO]

[DATE]

EUROPEAN INVESTMENT BANK GROUP ("EIB Group")
INSPECTORATE GENERAL – FRAUD INVESTIGATIONS DIVISION

PRIVACY STATEMENT FOR INVESTIGATIONS

1. DESCRIPTION OF THE PROCESSING OPERATION

Investigations run by the EIB Group's Fraud Investigations Division ("IG/IN") are administrative investigations for the purpose of detecting and preventing fraud, corruption and any other prohibited conduct[1] affecting EIB Group's activities.

The legal basis for this processing operation is:

- Article 325 of the Treaty on the Functioning of the European Union ("TFEU");
- Article 18 of the EIB Statute and articles 2 and 28 of the EIF Statutes;
- Regulation (EU, EURATOM) No 966/2012 of the European Parliament and of the Council;
- EIB Board of Governors Decision of 27 July 2004 concerning EIB's cooperation with OLAF;
- Policy on preventing and deterring prohibited conduct in European Investment Bank activities and Policy on preventing and deterring prohibited conduct in European Investment Fund activities ("EIB and EIF Anti-Fraud Policies").

2. WHAT PERSONAL INFORMATION DO WE COLLECT, FOR WHAT PURPOSE, AND THROUGH WHICH TECHNICAL MEANS?

In the context of its investigations, IG/IN collects identification data, professional data and case involvement data. This data may be used to assess allegations of prohibited conduct and determine whether any misconduct or wrongdoing was committed. It may also be used for contact purposes.

The data may be collected by any of the means provided in the EIB and EIF Anti-Fraud Policies, including by accessing any relevant information, documentation and premises of the EIB Group and/or of the projects financed by the EIB Group, and by asking oral information from any relevant person.

The evidence collected is relevant to the matter under investigation and collected for the purpose of the investigation, it will include inculpatory and exculpatory evidence.

3. WHO HAS ACCESS TO YOUR INFORMATION AND TO WHOM IS IT DISCLOSED?

Responsible IG/IN staff has access to your data. In addition, your data may be transferred to designated persons in the EIB Group, EU institutions, bodies offices and agencies, international organisations and/or the relevant authorities in Member States, candidate countries or third countries in order to ensure the appropriate conduct of the investigation.

4. HOW DO WE PROTECT AND SAFEGUARD YOUR INFORMATION?

In order to protect your personal data, a number of technical and organisational measures have been put in place.

IG/IN premises are part of a secured physical area only accesible to IG/IN staff and security services in order to prevent any unauthorised access to equipment and data. The IT systems used by IG/IN are subject to the IT security policy of the EIB which includes measures to protect the EIB IT infrastructures and systems. In addition, administrative measures include the obligation that service providers signed non-disclosure and confidentiality agreements.

5. HOW LONG DO WE KEEP YOUR DATA?

[1] Prohibited conduct is defined in EIB and EIF Anti-Fraud Policies available on [hyperlink].

Your personal data may be retained in IG/IN's case files for at least five years and up to ten year after the closure of the investigation. If the related allegations were not subtantiated, your personal data may be retained for up to five years maximum from the closure of the case.

6. HOW CAN YOU VERIFY, MODIFY OR DELETE YOUR INFORMATION?

You are entitled to access, rectify and (in certain circumstances) block the data we hold regarding you. You may exercise these rights by contacting the data processing controller at the following address: Investigations@eib.org. Upon request and within three months from its receipt, you may obtain a copy of your personal data undergoing processing. Exemptions under Article 20(1) of Regulation 45/2001 may apply.

7. RIGHT OF RECOURSE

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) at any time if you consider that your rights under Regulation 45/2001 have been infringed as a result of the processing of your personal data by IG/IN.

Before initiating this procedure data subjects may contact first the Head of IG/IN (Investigations@eib.org), responsible for the processing, or the Data Protection Officer of the EIB (DataProtectionOfficer@eib.org).

European Investment Bank

Luxembourg, xxx
IG/IN/XXXX/

STRICTLY CONFIDENTIAL

Note to File xxxx

Subject: Restriction or deferral of information under Article 20 of Regulation 45/2001

Ref.: Case […]

1. Background information

This note documents the application of a restriction and deferral of information in the context of the case under reference. The relevant data subject(s) is/are *[name and type of data subject].*

2. Decision

2.1 After having performed an analysis of this specific case [*and requested OLAF's opinion*], it is IG/IN's conclusion that informing the above-mentioned data subject(s) about the processing of his/her/their data in the context of IG/IN's case xxx/IN/xxx could be detrimental to the investigation.

[*Please add justification as the case may be. E.g:*
- *Risk of destruction of evidence if data subject becomes aware of investigation*,
- *Risk of flight from jurisdiction if data subject become aware of the investigation*,
- *Risk that data subject will inform a person concerned*,
- *Risk of likely damage to the effective development and pursuit of the case]*

3.2 The information is therefore restricted under *[please precise under which legal basis:*
Art 20(1)

(a) the prevention, investigation, detection and prosecution of criminal offences;
(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;
(c) the protection of the data subject or of the rights and freedoms of others;
(d) the national security, public security or defence of the Member States;
(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).]

4. Follow-up actions

Under article 20(3) of Reg. 45/2001, the data subject shall be informed of the principal reasons on which this restriction is based and of his/her right to have recourse to the EDPS. *[Provision of this information is deferred as such information would deprive the restriction of its effect in line with article 20(5) of Reg. 45/2001.]*

[redacted]

[To be annexed: consultation of OLAF, if any.]

European Investment Bank

Luxembourg, xxx
IG/IN/XXXX/

STRICTLY CONFIDENTIAL

Note to File

xxxx

Subject: Request of access to data under Reg. 45/2001 by xxxx

Ref.: [case reference]

1. Background information

On *[date],* IG/IN received a request for *[access, rectification, blocking, erasure]* by *[data subject's name]* who is *[informant, whistleblower witness, person concerned]* in the context of the case under reference.

2. Decision

2.1 After having performed an analysis of this specific case [*and requested OLAF's opinion*], it is IG/IN's conclusion that giving access to his/her personal data relevant to case [*ref.]* to [*data subject's name*] [*could be detrimental to the investigation OR is not detrimental to the investigation*].

[*Please add justification as the case may be. E.g:*

- *Risk of destruction of evidence if data subject becomes aware of investigation,*
- *Risk of flight from jurisdiction if data subject become aware of the investigation,*
- *Risk that data subject will inform a person concerned,*
- *Risk of likely damage to the effective development and pursuit of the case]*

2.2 As regards IG/IN's file, the requested access is therefore [*fully restricted OR partially restricted OR deferred as permitted under article 20(1) of Reg. 45/2001*] OR [*fully granted*].

[If access is denied, please precise under which legal basis:
Art20(1)

(a) the prevention, investigation, detection and prosecution of criminal offences;
(b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters;
(c) the protection of the data subject or of the rights and freedoms of others;
(d) the national security, public security or defence of the Member States;
(e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).]

3. Follow-up actions

[The case file shall be reviewed and access shall be granted to the personal data held regarding Mr/ Ms xx. The personal data provided to Mr/Ms xx shall not allow identifying any informant or whistleblower.]

OR

[Under article 20(4) of Reg. 45/2001, the staff member shall be informed of the principal reasons on which this restriction is based and of his right to have recourse to the EDPS. Provision of this information may be deferred for as long as such information would deprive the restriction imposed of its effect.]

[redacted]

To be annexed: Request of access and consultation of OLAF, if any.

European Investment Bank

Luxembourg, xxx
IG/IN/XXXX/

STRICTLY CONFIDENTIAL

Note to File

xxxx

Subject: Transfer of data under Articles 8 and 9 of Regulation 45/2001

Ref.: Case […]

1. Background information

This note documents the transfer of *[describe the data]* to *[name of the recipient + category: Member State or EEA authority subject to Directive 95/46/EC, Member State or EEA authority not subject to Directive 95/46/EC, third country authority, international organisation or bilateral agency]* in the context of the case under reference. The data is related to *[name and type of data subject].*

2. Decision

2.1 After having performed an analysis of this specific case [*and requested OLAF's opinion*], it is IG/IN's conclusion that transferring the above described data is necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, such as the general purpose of combating fraud. In addition, the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

The transfer falls within:

[*insert the legal basis:*
- *Article 8 of Regulation 45/2001: recipient is subject to Directive 95/46/EC*
- *Article 9(1) and (2) of Regulation 45/2001: Recipient provides adequate level of protection*[1]
- *Article 9(7) of Regulation 45/2001: Recipient has a MoU with IG/IN including data protection provisions*
- *Article 9(6)(a) of Regulation 45/2001: Data subject provided its writing consent*[2]
- *Article 9(6)(d) of Regulation 45/2001: Transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims]*

3. Follow-up actions

On the basis of the above, the data can be transferred using the relevant transfer clause.

[redacted]

[To be annexed: consultation of OLAF, if any.]

[1] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[2] Autorisation by data subject to be annexed