EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Inspector General
Fraud Investigations Division

EIB Group Chief Compliance Officer

European Investment Bank (EIB)
100, Boulevard Konrad Adenauer
LU-2950 Luxembourg
LUXEMBOURG

Brussels, 29 November 2017
WW/ALS/sn/D(2017)2598 **C 2016-0381**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-check Opinion on the Whistleblowing Policy of the European Investment Bank - Case 2016-0381

On 19 April 2016, the European Data Protection Supervisor ("EDPS") received a notification for prior checking relating to the Whistleblowing Policy from the Data Protection Officer ("DPO") of the European Investment Bank ("EIB") under Article 27 of Regulation (EC) No 45/2001 (the "Regulation")[1].

As this is an ex-post prior check, the two-month deadline within which the EDPS must deliver his opinion does not apply. This case has been dealt with on a best effort basis.

Since the EDPS has issued Guidelines on how to process personal information within a whistleblowing procedure[2], the description of the facts and of the legal analysis will only mention those aspects that differ from these Guidelines or otherwise need improvement. For aspects not covered in this Opinion, the EDPS has, based on the documentation provided, no comments.

The EIB has informed the EDPS that a new whistleblowing policy is under preparation. Since the adoption of the new policy is not envisaged within the near future, the EDPS issues this

[1] OJ L 8, 12/01/2001, p. 1.
[2] Available on the EDPS website on the following link: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-07-18_Whistleblowing_Guidelines_EN.pdf

Opinion with the expectation that the EIB will implement the recommendations in the new policy.

Facts and analysis

1. Defined channels for whistleblowing reports

Whistleblowing procedures are intended to provide safe channels for anyone who becomes aware of and reports potential fraud, corruption or other serious wrongdoings and irregularities.

As described in the EIB Whistleblowing Policy and the notification, the reporting channels are different depending on the type of allegation. Cases of alleged fraud, corruption, money laundering and financing of terrorism, or any other unlawful activity that is detrimental to the financial interest of the Union, should be reported to the Inspector General of the Fraud Investigations Division in line with the EIB Anti-fraud policy.[3] Concerning cases of serious misconduct or serious infringement of the Staff Code of Conduct or the Integrity Policy and Compliance Charter, the Chief Compliance Officer is the person to contact.

The EDPS considers that the most effective way to encourage staff to report concerns are to ensure them that their identity will be protected. Whistleblowing channels should therefore be clearly defined. With more than one reporting channel in place, it might be unclear where to turn which could lead to the whistleblower using all the channels and consequently more people than necessary getting access to the reports. The EIB has however explained that they have not experienced any cases in the past where the whistleblower encountered difficulties to use and address the right channel. In view of the above, and considering the fact that EIB has well-established reporting channels, the EDPS sees no problem with the use of two reporting channels as long as it is clear to staff where to turn (see point 2. Information to data subjects below).

Furthermore, whistleblowing channels should in principle not be used when staff wish to exercise their statutory rights, i.e. by lodging a request or complaint to the Appointing Authority under Art. 90 of the Staff Regulations, or for harassment claims and personal disagreements when staff may address themselves to HR, Mediation Service, confidential counsellors or lodge a request for assistance under Art. 24 of the Staff Regulations.[4]

The Whistleblowing Policy and the notification both mention that cases of bullying, harassment and those concerning dignity at work are to be reported to the Director of Human Resources. Such cases should in principle not be covered by the whistleblowing channels since EIB has other procedures in place[5] but the EDPS understands the need to mention it in the Whistleblowing Policy to avoid misunderstandings. **The policy should however be amended so that it is clear that the whistleblowing channels are not appropriate for the abovementioned cases and refer to the relevant EIB procedure in place.**

2. Information to data subjects

Articles 11 and 12 of the Regulation provide a minimum list of information about the processing of personal data that should be provided to individuals involved in a case.

---

[3] Available on the EIB's website on the following link:
http://www.eib.org/attachments/strategies/anti_fraud_policy_20130917_en.pdf

[4] See page 5 of the EDPS Guidelines on Whistleblowing. EIB is however subject to its own Staff Regulations available on the following link:
http://www.eib.org/attachments/general/eib_staff_regulations_2013_en.pdf

[5] The EDPS opinions on the EIB dignity at work policy available on the following link:
https://edps.europa.eu/sites/edp/files/publication/05-04-20_eib_dignity_en.pdf

The EIB has informed the EDPS that information to data subjects is available on the intranet (in the form of FAQs) as a summary of the main points of the Whistleblowing Policy, which is also published on the EIB website. A data protection statement for investigations in relation to fraud is furthermore available on the website. However, there is no data protection statement informing data subjects on how their personal data is processed when reporting cases of serious misconduct or serious infringement to the Chief Compliance Officer. **The EIB should therefore publish a data protection statement for investigations concerning serious misconduct or serious infringement including all mandatory items under Article 11 and 12 of the Regulation.**

Furthermore, information on whistleblowing procedures should be provided to the individuals concerned in a two-step procedure. This means that **all individuals affected**[6] **by a particular whistleblowing procedure should also be provided with the data protection statement as soon as practically possible,** unless an exception in Article 20(1) of the Regulation applies.[7]

Deferral of information should be decided on a case-by-case basis. The reasons for any restrictions should be documented, and made available to the EDPS if requested in the context of a supervision and enforcement action. These reasons should prove, for instance, that there is a high risk that giving access would hamper the procedure or undermine the rights and freedom of others. **The reasons should be documented before the decision to apply any restriction or deferral is taken. This logic applies to any restrictions of data subjects' rights (information, access, rectification, etc.). The EIB should update the Whistleblowing Policy in this regard.**

3. Conservation period

As a general principle, personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are collected and/or further processed (Article 4(1)(e)).

Neither the Whistleblowing Policy nor the notification include any information about how long personal information is kept. The EDPS considers that different conservation periods should apply depending on the information in a whistleblowing report and how the case is dealt with. For example, personal information that is not relevant in relation to the allegations should not be further processed. Concerning cases where an initial assessment is carried out and where it is clear that the case is outside the scope of the whistleblowing procedure, the report should be deleted as soon as possible or referred to the right channel if it for example concerns alleged harassment. In cases, where an initial assessment is carried out and where it is clear that the case is outside the scope of the whistleblowing procedure, personal information should be deleted promptly and usually within two months after the completion of the preliminary assessment, since it would be excessive to retain such sensitive information.[8] **The EIB should therefore establish different conservation periods depending on the outcome of the case.**

4. Security measures

[...]

[6] Affected individuals will usually include whistleblowers, witnesses, other members of staff/third parties and the accused person(s). Concerning when third parties should/should not be informed, please see example 5 on page 8 of the EDPS Guidelines on Whistleblowing.
[7] See page 7 of the EDPS Guidelines on Whistleblowing.
[8] See page 9 of the EDPS Guidelines on Whistleblowing for more information.

* *
*

Conclusion

In this Opinion, the EDPS has made recommendations to ensure compliance with the Regulation. Provided that the recommendations are implemented, the EDPS does not see any reason to believe that there is a breach of the Regulation.

For the following **recommendations**, the EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion:

- Amend the Whistleblowing Policy so that it is clear that the whistleblowing channels are not appropriate for cases concerning harassment and add a reference to the relevant EIB procedure in place;
- Draft a data protection statement for investigations concerning serious misconduct or serious infringement including all the requirements under Art. 11 and 12 of the Regulation and publish it on the EIB intranet;
- Provide all affected individuals with the data protection statement as soon as practically possible;
- Document the reasons for any restrictions to data subjects' rights (by adopting a motivated decision for example) and update the Whistleblowing Policy in this regard;
- Establish different conservation periods depending on the outcome of the case;
- [...]

Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI

Cc: Data Protection Officer, EIB