EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[…]
Director Human Resources
European Investment Fund
37B, Avenue J. F. Kennedy
L - 2968 Luxembourg

Brussels, 18 May 2016
WW/OL/sn/ D(2016)1057 **C 2015-0808**
Please use edps@edps.europa.eu for all correspondence

Subject: **Procedure on Access to the professional/personal data, physical or electronic, of staff members in the event of absence, departure from EIF service or death.**

Dear […],

On 28 September 2015, the Data Protection Officer (DPO) of the EIF has notified the EIF's procedure on "Access to the professional/personal data, physical or electronic, of staff members in the event of absence, departure from EIF service or death" to the EDPS for prior checking under Article 27 of Regulation (EC) 45/2001 ("the Regulation")[1].

As this was an ex-post case (i.e. the processing was already in place at the time of notification), the deadline of Article 27(4) of the Regulation does not apply. Given that the EDPS was in the process of developing Guidelines on eCommunications ("the Guidelines"), which also cover questions of access to (former) staff members' mailboxes in their absence, the EDPS decided to suspend all pending ex-post cases on this issue until the adoption of the Guidelines. Following adoption of the Guidelines on 16 December 2015[2], the case was unsuspended again.

As indicated in the notification, the procedure is identical to the equivalent procedure at the European Investment Bank, which has been notified to the EDPS as case 2013-0801. The content of the EDPS Opinions on these two notifications is largely identical.

[1] OJ L 8/1, 12/01/2001
[2] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-16_eCommunications_EN.pdf

The analysis below will only cover those aspects of the procedure where the EIF is not compliant with the Guidelines or which otherwise merit comments.

The Facts

The EIF's procedure on "Access to the professional/personal data, physical or electronic, of staff members in the event of absence, leaving the Bank or death" is based on Article 3.7, second subparagraph of the Code of Conduct for its staff, as further elaborated in Note to Staff No. 626 (this is strictly speaking an EIB document, but applies to EIF staff as well).

Information on the procedure is provided in Note to Staff No. 626. In case the procedure is used, the (former) staff member will be contacted where possible, explaining the reasons and purposes for the request and requesting her/his consent. If consent is not given, the matter will be referred to HR and the DPO will be consulted. Upon request of HR and in line with the instructions given by it, the EIB's IT-Sec (which manages the technical infrastructure for the EIF) will retrieve the information requested in line with relevant legal provisions.

This procedure only covers access to e-mails for business continuity purposes; the rules on accessing e-mails in administrative inquiries and disciplinary proceedings are covered elsewhere[3].

Legal Analysis

The procedure notified covers accessing staff members' mailboxes for purposes of business continuity. It therefore does not aim at evaluating staff members' conduct (Article 27(2)(b) of the Regulation); neither does it trigger any of the other criteria requiring prior checking under Article 27.[4] The notified processing operations are therefore **not subject to prior checking**.

That being said, the EDPS still has some observations to make against the background of the Guidelines.

Article 3.7, second subparagraph of the Code of Conduct authorises limited private use of EIF equipment by staff (identical to the EIB's Code of Conduct). It does not refer in any detail to the procedures for the EIF to access personal data of staff members in the event of absence, leaving the Bank or death. All available information and documentation of procedures appears to be included in Note to Staff No. 626. The EDPS recommends that the EIF should **clarify the status of Note to Staff No. 626, notably whether it only serves an information instrument, or whether it also serves as a legal basis for the procedure in itself. In the former case, the EIF should adopt a specific internal legal basis.**

Moreover, the (former) staff member's consent is not the appropriate ground for lawfulness in this situation (see also point 66 of the Guidelines). The reason for accessing an e-mail account is for business continuity and because it has been deemed necessary and proportionate for this purpose as part of the EIF's performance of its tasks in the public interest. The fact that, should the staff member refuse consent, the EIF may still go on to access the data indicates that this would not be valid consent.[5] The EDPS recommends the EIF to **amend the procedure and the information provided to staff accordingly. The information to staff should also include information on the right to object under Article 18 of the Regulation.**

[3] see EDPS case 2009-0459

[4] In some cases, the EIF may access staff members' mailboxes for purposes of evaluating their conduct in the framework of internal investigations. However, such uses are covered by the EIF's notification on fraud investigations, which has already been the object of a prior checking notification to the EDPS (EDPS case 2014-1163). Staff members are also instructed to flag private or confidential messages accordingly, reducing the risk that such messages will be accidentally accessed.

[5] See Article 29 Working Party Opinion 15/2001, p. 13 and Article 29 Working Part Opinion 08/2001, p. 3 for more information. To summarise, given the power imbalance between staff and employer, consent should only be used when there is a genuinely free choice for the staff member to make. This is not the case here.

Under Articles 11 and/or 12 (as applicable) of the Regulation, persons concerned have to be informed about the processing of their personal data (see also recommendations 17 and 18 in the Guidelines). These Articles provide a list of information items to be provided. Controllers have a certain leeway in how they provide this information, but usually a privacy statement is the best way to do so. In the case at hand, there is no specific privacy statement, but users are informed about some aspects of the processing in Note 626, which is made available to all staff. However, the information provided should be improved: The controller is currently only mentioned implicitly (mandatory item under Article 11(1)(a) / Article 12(1)(a)); there is no mention of the right to access[6] for data stored electronically (Article 11(1)(e) / Article 12(1)(e)); the right to recourse to the EDPS is not mentioned (Article 11(1)(f)(iii) / Articles 12(1)(f)(iii)). The EDPS recommends the EIF to **also provide the missing information to staff**, either in Note 626, a separate privacy statement, or when contacting (former) staff members about the impending access.

As the technical infrastructure of the EIF is provided by the EIB, the relationship between the EIF and EIB (notably EIB IT-Sec) should be clarified here. Independently of whether the EIB acts as a processor for the EIF or as a co-controller, their **respective tasks should be clearly delineated and documented**.

Conclusion

Please inform the EDPS about the implementation of the three recommendations highlighted in bold above **within three months** from the date of this Opinion.

Yours sincerely,

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: […], DPO, EIF

[6] The section entitled "access to personal data" of Note to Staff No. 626 is about the *EIF's* access to personal data of staff members, not about staff members' access to their *own* personal data.