



WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Ms Verena ROSS
Executive Director
European Securities and Markets
Authority (ESMA)
103, rue de Grenelle
F-75007 Paris
FRANCE

Brussels, 11 January 2017
WW/ALS/sn/D(2017)0063 C 2016-1042
Please use edps@edps.europa.eu for all
correspondence

Subject: Prior-check Opinion on ESMA's Whistleblowing Policy - Case 2016-1042

Dear Ms Ross,

On 10 November 2016, the European Data Protection Supervisor ("EDPS") received a notification for prior checking relating to the Whistleblowing procedure from the Acting Data Protection Officer ("DPO") of the European Securities and Markets Authority ("ESMA") under Article 27 of Regulation (EC) No 45/2001 (the "Regulation").

According to Article 27(4) of the Regulation, this Opinion must be delivered within a period of two months, not counting suspensions for requests for further information¹. Since the EDPS has issued Guidelines on how to process personal information within a whistleblowing procedure², the description of the facts and of the legal analysis will only mention those aspects which differ from these Guidelines or otherwise need improvement.

EDPS recommendations and reminders are highlighted in bold below.

Description and assessment

1. Transfer information on a case-by-case basis

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.

¹ The case was suspended for comments from the DPO from 14 December 2016 to 5 January 2017. The EDPS shall thus render his Opinion no later than 1 February 2017.

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

ESMA's Whistleblowing Policy mention under *6. Reporting Procedures* that the recipient of the information is obliged to transmit the information without delay to OLAF.

The EDPS points out that OLAF is the competent body to investigate fraud against the EU budget. Since the scope of the whistleblowing procedure is not limited to cover potential fraud, there is a possibility that ESMA will receive information that it is not within the competences of OLAF. In accordance with Article 7(1) of the Regulation, the transfer of personal information should only take place when necessary for the legitimate performance of tasks covered by the competence of the recipient. Therefore, the **ESMA should assess the requirements for transferring the personal information to OLAF on a case-by-case basis and adapt its guidelines and the privacy statement accordingly.**

2. Ensure confidentiality of all persons implicated in a whistleblowing report

The EDPS welcomes the fact that ESMA guarantees the protection of the identity of the whistleblower together with the staff members implicated by a report. One way of doing so is to limit the access to the reports. In the notification, potential recipients are mentioned, strictly on a need-to-know basis, such as the Ethics Officer, HR, Head of Unit concerned, Head of Department concerned, officers appointed for the internal administrative investigation and the Executive Director. Internal access to the information processed must be granted on a strictly need to know basis and it must be given only to staff who has a need to have access. In addition, the Whistleblowing Policy mentions Team Leaders, together with Head of Units and Head of Department, as immediate hierarchical superiors to whom a report may be sent. The Team Leaders are therefore also considered as possible recipients. **The EDPS points out that it is crucial to keep as few people as possible involved in order to protect the confidentiality of personal information processed within a report. Furthermore, in light of the above, ESMA should align the notification, the Whistleblowing Policy and privacy statement as regards the recipients of the information.**

3. Information to data subjects

According to Article 11(1)(c) of the Regulation, the data subject has the right to receive information about the recipients or the categories of recipients of the data. This is clear from the Whistleblowing Policy except as regards Team Leaders (see above point 2.). The privacy statement does not, however, clarify the reporting channels and which members of ESMA staff will have access to the information. Since the information in the Policy could be overlooked, **ESMA should also include detailed information about the recipients in the privacy statement and, as mentioned above, align it with the notification and the Whistleblowing Policy.**

4. Security measures

[...]

* *
*

In light of the accountability principle, the EDPS trusts that ESMA will ensure that these considerations and recommendations are fully implemented. The EDPS has therefore decided to **close case 2016-1042.**

Yours sincerely,

(signed)

Wojciech Rafał WIEWIÓROWSKI