EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Executive Director
European Union Agency for Network
and Information Security (ENISA)
PO Box 1309
781001 Heraklion
Crete
Greece

Brussels, 3 April 2017
WW/ALS/xx/ D(2016) xxx **C 2017-0109**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-check Opinion on ENISA's Whistleblowing Policy - Case 2017-0109

Dear Mr,

On 23 January 2017, the European Data Protection Supervisor ("EDPS") received a notification for prior checking relating to the Whistleblowing procedure from the Data Protection Officer ("DPO") of the European Union Agency for Network and Information Security ("ENISA") 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 information[1]. 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 which 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.

EDPS recommendations and reminders are highlighted in bold below.

[1] The case was suspended for further information from 9 February 2017 to 20 February 2017, and for comments from the DPO from 29 March 2017 to 30 March 2017. The EDPS shall thus render his Opinion no later than 4 April 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

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. ENISA's Whistleblowing Policy states, under 3.3(a) page 4, that OLAF shall be informed of the outcome of any such investigations conducted by ENISA. Furthermore, the privacy statement mentions [...] *Then the Head of Unit of ENISA'S Executive Director will provide the report to OLAF* (page 2).

In this regard, the EDPS points out that OLAF is the competent body to investigate fraud against the EU budget. However, since the scope of the whistleblowing procedure is not limited to cover potential fraud, there is a possibility that ENISA will receive information that it is not within the competences of OLAF but still within the scope of the whistleblowing procedure. 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, **ENISA should assess the need for transferring the personal information to OLAF on a case-by-case basis and adapt its Whistleblowing Policy and privacy statement accordingly**.

2. Data subjects' rights

The Whistleblowing Policy describes in Article 4.2 what kind of information the whistleblower is entitled to receive during the process. Point (d) states that the whistleblower should be kept informed, to the greatest extent possible, of progress in any investigation being undertaken, provided that this is consistent with the rights of any affected third party and with the protection of the investigation process itself.

In this regard, the EDPS would like to emphasize that there is no obligation under data protection law to provide this information and that it often relates to the personal information of other involved persons. **Therefore, the EDPS would like to remind ENISA that the persons involved should only receive personal information about themselves.**

In relation to section 13 A/ of the notification concerning the rights of the data subjects to block and erase data[3], the information provided by ENISA does not mention the time limit to block/erase personal data on justified legitimate grounds in relation to requests from data subjects. In this regard, **it is good practice that a decision should be taken within 15 working days. The notification should be adapted accordingly.**

* *
*

In light of the accountability principle, the EDPS trusts that ENISA will ensure that these considerations and recommendations are fully implemented. The EDPS has therefore decided to **close case 2017-0109.**

[3] See Articles 15 and 16 of the Regulation.

Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI

(signed)

Cc: Data Protection Officer ENISA