LE CONTROLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Calot ESCOBAR
Registrar of the Court
Court of Justice of the European Union
L-2925 Luxembourg

Brussels, 07 July 2017
WW/XK/sn/D(2017)1466 **C 2017-0304**
Please use edps@edps.europa.eu for all correspondence

Subject Prior Checking Opinion on Initial Processing in the event of Whistleblowing

Dear Mr Escobar,

On 13 March 2017, the European Data Protection Supervisor ("the EDPS") received a prior checking notification from the Court of Justice of the European Union ("the Court") regarding initiating an internal whistleblowing procedure.

The Court sent the EDPS an Annex to the Decision of the Administrative Committee that establishes a general framework for initiating whistleblowing procedures ("the general framework"). Based on this document, written internal regulations have existed at the Court since February 2016[1].

On 18 July 2016, the EDPS adopted and published guidelines for processing personal data within an ethical whistleblowing procedure ("the EDPS guidelines")[2]. When preparing this notification, the Court consulted this document. The EDPS will identify and only mention those practices that are not consistent with the EDPS guidelines and the provisions of the regulation.

[1] *"This general framework is not intended to replace those internal provisions but, with a view to simplifying the existing internal provisions for initiating whistleblowing claims, to address them in a unique context... "*, page 1 of the Annex.
[2] https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

Legal Analysis

This Opinion concerns the processing of personal data carried out by the Court in the context of a whistleblowing claim. This Opinion does not concern the processing of data by the Court after the whistleblowing procedure has been initiated (administrative investigations and disciplinary proceedings), as they are separate subsequent processes[3].

The processing of personal data is carried out by a European Union institution and the processing is carried out, in part, by automatic means. Therefore, the Regulation is applicable.

1. Prior check (Article 27(2)(a))

All processing operations are to be prior checked by the EDPS because they present risks in relation to the processing of data in relation to suspected offences (Article 27(2)(a) of the Regulation) and in the evaluation of the conduct of suspected persons (Article 27(2)(b) of the Regulation)[4].

In this case, the notification only refers to Article 27(2)(a) of the Regulation.

Point of information: the notified processing operation is also subject to Article 27(2)(b) of the Regulation, a second reason for rendering the processing at issue subject to prior checking.

2. Data quality (Article 4(1)(d))

The notification and the information note indicate that "*the data subjects can contact the authority in charge of handling the whistleblowing claim to exercise their rights of access and rectification*".

It is essential that the Court takes reasonable measures to guarantee the rights of the data subjects and, consequently, ensure that the collected data are accurate, complete and up to date (Article 4(1)(d) of the Regulation). The data subjects must have direct access to a specific functioning mailbox so as to be able to exercise their rights in writing. In this way, the Court could ensure full confidentiality and discretion concerning the identity of data subjects and their requests.

Recommendation In the information note, the Court should indicate the specific functioning mailbox to which data subjects can write to invoke their rights of access and rectification.

---

[3] The processing of data within the context of administrative investigations and disciplinary proceedings is the subject of a separate notification to the EDPS (Case 2011-0806).

[4] Pursuant to Article 27 of the Regulation, the EDPS shall carry out a prior check on any processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Article 27(2) of the Regulation lists the areas likely to present such risks, in particular Article 27(2)(a) refers to the processing of data relating to suspected offences and Article 27(2)(b) refers to processing operations to evaluate certain aspects of data subjects' personalities, including their conduct.

3. Data retention (Article 4(1)(e))

The notification and the information note indicate that "*data are deleted, at the earliest, following a period of two years dating from the decision to refer the claim on to the appropriate whistleblowing procedure or to dismiss the claim*".

This two-year period is excessive and disproportionate in view of the purposes for which the data are retained, namely, for referring the claim on to the whistleblowing procedure or for dismissing the claim. This period does not appear to be justified given the purposes for which data are collected under Article 4(1)(e) of the Regulation. Moreover, the EDPS guidelines recommend that the EU institutions establish different retention periods for collected data depending on the manner in which the case is processed:

Firstly, when an initial assessment is carried out, but it is clear that the case should not be referred to the European Anti-Fraud Office (OLAF) or is not within 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 any case, personal information should be deleted promptly and usually within two months of completion of the preliminary assessment[5], since it would be excessive to retain such sensitive information.

Secondly, if it is clear after the initial assessment that a report should be remitted to OLAF, the EU institution should carefully monitor the actions that OLAF takes. If OLAF starts an investigation, it is not necessary for the EU institutions to keep the information for a longer period. If OLAF decides not to start an investigation, the information should be deleted without delay.

Should a longer retention period be considered necessary (for example, in the case of complaints lodged with the European Ombudsman or the EDPS, or in the event of legal action), access to personal information should nonetheless be limited (see security measures below). It is good practice to store these reports outside the main file management system in daily use.

When a whistleblowing procedure has been initiated, the Court may, inter alia, decide not to forward the case to OLAF and to close the case. There is no data retention period stated in the notification for cases not forwarded to OLAF and closed without internal administrative investigation.

Recommendation The Court should consider the possibilities of a case being processed according to the EDPS guidelines as set out above. In particular, the Court should delete collected data promptly and generally within two months of completion of the preliminary assessment.

[5] Article 29 Working Party Opinion 1/2006, WP 117, p. 12.

4. Security measures (Article 22)

Technical and organisational measures should be put in place by the data controller, particularly in order to prevent any unauthorised access to documents concerning the whistleblowing procedure or to prevent any loss or destruction of such documents. Pursuant to Article 22 of the Regulation, these measures should make it possible to "*ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected*". Data collected during a whistleblowing procedure are sensitive and therefore require special security measures.

The Court has provided the EDPS with a document on risk analysis pertaining to the initial processing of whistleblowing claims, as well as a document on security measures.

The notification and the document on security measures recommend that the processing should be both paper-based and computerised. The document on risk analysis reveals a certain number of "*events" in relation to "Legality and regularity*". Nonetheless, this analysis is incomplete and does not correspond entirely to the processing at issue.

Recommendation The Court must therefore complete the risk analysis by taking into consideration the full context of the notified data processing, and review and update accordingly its internal documentation on the selected security measures.

*** ***
*****

In light of the principle of "accountability", the EDPS considers that the Court will adopt and implement the recommendations provided in this Opinion, and make any necessary updates to its internal documentation[6].

The EDPS will now close this case.

Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI

(signed)

Cc : Mrs Sabine HACKSPIEL, Data Protection Officer

[6] For example, concerning its internal notifications under Article 25 of the Regulation. However, it is not necessary to update the notification received by the EDPS under Article 27 of the Regulation.