European Data Protection Supervisor's prior checking Opinion on the whistleblowing procedure from the General Secretariat of the Council of the European Union (Case 2015-0349)

Brussels, 15 September 2015

1. Proceedings

On 17 April 2015, the European Data Protection Supervisor ("EDPS") received a notification for prior checking from the Data Protection Officer ("DPO") of the Council of the European Union ("the Council") regarding the procedure for reporting serious irregularities (whistleblowing).

According to Article 27(4) of Regulation 45/2001 (the "Regulation") this Opinion must be delivered within a period of two months, not counting suspensions for requests for further information[1], in other words, 15 September 2015.

2. The facts

The **purpose** of this procedure is to enable the reporting of serious irregularities, misconduct or negligence within the Council. This requires establishing reporting channels for whistleblowers, managing and following-up reports, and ensuring protection and adequate remedies for whistleblowers. Article 22(a), (b) and (c) of the Staff Regulations, as well as the Conditions of Employment of Other Servants of the European Union provide for the rules on whistleblowing.

The Council has drafted internal rules on reporting serious irregularities[2] (hereinafter internal rules). The rules set up procedures to be followed for reporting serious irregularities including what, when and to whom staff members should report.

The **personal information processed** is contained in the report submitted by the whistleblower and any subsequent document drawn up in response to that initial report. These documents may contain names, contact details and other personal data. In principle, special categories of data should not be included. When the report contains personal information that is clearly not relevant for examining the issues raised in the report, the information will be erased when appropriate after consulting the whistleblower to the extent that this is possible without the substantive examination being unduly delayed.

[1] The case was suspended for information from 30 April 2015 to 26 June 2015 and for comments of the DPO from 28 July 2015 to 3 September 2015. The EDPS shall thus render its Opinion before 21 September 2015.
[2] Draft Decision of the Secretary-General of the Council adopting internal rules for reporting serious irregularities - Procedures for the implementation of Articles 22(a), 22(b), 22(c) of the Staff Regulations and 66.8 of the Financial Regulation.

All individuals affected by a specific procedure concerning serious irregularities will be directly provided with a **privacy statement** as soon as practically possible. Deferral of information will be decided on a case by case basis.

The notification states that the categories of recipients to whom personal information will be **disclosed** are the hierarchical superiors (Director(s)-General, or deputy, the Director(s) and the Head(s) of Unit, Sector or Office concerned), the Appointing Authority, the Director-General for Administration and the Director of Human Resources and Personnel Administration. On a need-to-know basis, the information will be disclosed to the Director-General of Security, Safety, Communication and Information Systems, the Director of the Security Office, the Head of Unit and the members of the Legal Advisers to the Administration Unit, the Security Office and the Legal Service in charge of handling the file, as well as any other staff member responsible for any follow-up action that are to be designated by the Secretary-General.

The **retention period** for files which do not lead to the opening of an inquiry will be kept for a period of two years from the date on which the Director-General for Administration (DGA) or the Secretary General (SG) decides to close the file without follow-up. Files on the basis of which an administrative inquiry or disciplinary procedure is opened or files which are reported to OLAF should be kept in line with the retention periods foreseen for those files.

Regarding the **security measures** [...]

3. Legal analysis

3.1. Prior checking

The processing of personal data is performed by an institution of the European Union. Furthermore, the processing is partly done through automatic means. Therefore, the Regulation is applicable.

This processing activity is subject to prior checking since it presents specific risks. Indeed, the Council will process information on suspected offences and carry out an evaluation of the accused persons' conduct.[3]

3.2. Data retention

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 which the data are collected and/or further processed (Article 4(1)(e)).

In this case, the conservation period is two years from the date when the DGA/SG decide to close the file without follow up. The Opinion of WP Article 29[4] mentions, however, that personal data should be deleted promptly and usually within two months of completion of the

[3] Article 27 of the Regulation subjects to prior checking by the EDPS processing activities 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 contains a list of processing operations that are likely to present such risks including under point (a) the processing of data related to suspected offences and under point (b) processing intended to evaluate personal aspects relating to the data subject, including his or her conduct.

[4] See Article 29 Working Party Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, page 12, recommending two months from the closure of the investigation; available here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

investigation of the facts alleged in the report. In this regard, a retention period of two years for files that are closed without follow up[5] seems excessive and the EDPS invites the Council **to re-evaluate the data retention period or provide further justification on the necessity to retain data found irrelevant for two years.**

3.3. Transfer of data

In accordance with Article 7(1) of the Regulation, the Council is required to verify both that the recipients are competent and that the personal information is necessary for the performance of the related tasks.

The Council has mentioned several categories of data to which information might be disclosed. Since the personal information transferred could indirectly lead to the identification of suspected persons, the EDPS reminds the Council to verify on a case by case basis whether a transfer is necessary for the legitimate performance of tasks covered by the competence of the recipient.

3.4. Information to the data subject

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

Information on whistleblowing procedures should be provided to the individuals in a two-step procedure. A privacy statement should be published on the website of the Council and the persons involved in a particular whistleblowing procedure should also be provided with a specific privacy statement as soon as practically possible. The Council has indicated that they will inform the affected persons involved but does not mention any publication on their website. Therefore, **the Council should publish a general privacy statement regarding whistleblowing procedures on their website.**

Furthermore, in the document "Information to data subjects" (point 5) the Council only refers to their Internal Decision[6] when describing the procedures for safeguarding data subjects' rights. Since the controller should provide the individual with information on the existence of the right to access and the right to rectify[7] and because the processing is sensitive, the EDPS recommends that the Council **add more detailed information on how data subjects' can exercise their rights.**

3.5. Rights of access and rectification

Under Article 13 and 14 of the Regulation, data subjects have the right to access their personal data and to have inaccurate data rectified. These rights may be restricted under the conditions set out in Article 20 of the Regulation.

When replying to data subjects' access requests, special attention should be given to the definition of the concept of personal data. The Council should bear in mind that personal data

---

[5] This concern cases where the accusations has been assessed and found false or irrelevant and the closure takes place upon completion of the investigations of the facts alleged.

[6] 2004/644/EC: Council Decision of 13 September 2004 adopting implementing rules concerning Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[7] Article 11(1)(e) and Article 12(1)(e) of the Regulation.

do not only relate to information on an individual's private life in a strict sense, but also to information regarding an individual's activities, such as his or her working relations and economic or social behaviour. Information can relate to an individual because of its content, the purpose of its use or the result of its use. This needs to be considered when determining the scope of the data subject's right to access.

When considering access rights, the Council should also consider the status of the requester (the accused person, whistleblower/informant, witness, staff member or outside informants) and the current stage of the investigation.

3.6. Confidentiality

The EDPS welcomes the guarantees foreseen in the internal rules concerning protection for staff members (whistleblowers). In this regard, the EDPS stresses that preserving the confidentiality of whistleblowers, the accused persons and the third parties are of utmost importance.

The reasons why the confidentiality of the accused person should be protected in the same manner as the whistleblower is because of the risk of stigmatisation and victimisation of that person within the organisation to which he/she belongs. The person will be exposed to such risks even before he/she is aware that he/she has been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated. In this regard, the Council should **add information on the protection of the accused person to the internal rules.**

3.7. Security measures

[...]

4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation providing that the recommendations contained in this Opinion are fully taken into account. The Council should:

- Re-evaluate the data retention period or provide further justification on the necessity to retain data for two years regarding files where the accusations are found irrelevant (point 3.2.);
- Publish a general privacy statement on the website with regard to the whistleblowing procedures (point 3.3.);
- Amend the information to data subjects as to include information on the existence of the right to access and the right to rectify (point 3.3.);
- Make clear in the internal rules that the identity of the accused person also should be protected (point 3.6.);
- [...]
- [...]

Please inform the EDPS of the measures taken based on the recommendations of this Opinion within a period of 3 months.

Done at Brussels, 15 September 2015

(**signed**)

Wojciech RAFAŁ WIEWIÓROWSKI