The European Data Protection Supervisor's prior checking Opinion on the European Medicines Agency's procedure for reporting potential fraud and irregularities (Case 2015-0820)

Brussels, 16 December 2015

1. Proceedings

On 30 September 2015, the European Data Protection Supervisor ("EDPS") received a notification for prior checking from the Data Protection Officer ("DPO") of the European Medicines Agency ("EMA") regarding the procedure for reporting potential fraud and irregularities to be established at EMA.

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], i.e. before 4 January 2016.

2. The facts

The **purpose** of this procedure is the processing by the Anti-Fraud Office of EMA of reported information regarding irregularities and potential fraud cases that is brought to its attention by way of reported information (internal or external whistle-blowing) or that has reached it by other means. This process will allow the gathering of information on the reported conducts in order to assess and identify which cases should be transmitted to OLAF in accordance with Article 8 of Regulation (EU, Euratom) No 883/2013[2].

The **data subjects** are the Agency's staff members, interims, trainees, delegates and on-site contractors and every person mentioned in the fraud reporting process.

The **personal information processed** are contained in the reporting template and may include first name and surname of the person involved in the potential fraud, his/her relation to the alleged fraudster (e.g. family member), as well as data on the nature of the facts potentially constituting fraud. Data of third parties may also be implied, e.g. if a third person sent a letter to the reporting person with the facts in question, the Anti-Fraud Office may need to process the data contained in such a letter. The notification underlines that it is not possible to establish *ex ante* the categories of data that could be the subject matter of potential fraud or irregularities reported to the EMA.

A **Data Protection Notice** will be part of the reporting template published on EMA's website. Such a notice will also be published on the section of the website presenting the activities of the Anti-Fraud Office and making available information about reporting alleged fraud and irregularities. The Data Protection Notice will include information regarding the rights of data subjects (access, rectification, etc.), the procedures put in place to exercise them

[1] The case was suspended for request for information from 27 October 2015 to 27 November 2015.

[2] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999

and the time limit within which a reaction from the Anti-Fraud Office can be expected. Furthermore, the persons reporting the potential case and the persons involved in the case will be informed and regularly updated on the progress of the proceedings. However, the provision of certain information to some data subjects (e.g. the suspected fraudster) may be delayed in order not to jeopardise the proceedings and possible future OLAF investigation in accordance with Article 20 of the Regulation.

The notification states that the **recipients** of personal data might be OLAF, pursuant to the obligation set out in Regulation (EU, Euratom) No. 883/2013 to inform OLAF without delay. Moreover, in the initial phase of internal assessment of the reported information, the data can be communicated to HR, Audit or the relevant Head of Division and the Executive Director if there is a need to involve OLAF.

The **retention period** depends on whether OLAF opens an investigation or not. With regard to cases which will not be notified to OLAF and for which no further action is needed, the retention period will be three years. With regard to cases which are notified to OLAF, EMA will align its conservation period with those of OLAF (fifteen, eight or five years after case closure, as described in Article 13.2 of the OLAF Instructions to Staff on Data Protection for Investigative Activities[3]). Furthermore, the notification states that improper or pointless messages will be deleted immediately.

Regarding the **security measures** the notification states that paper documents related to potential fraud are stored in secure locations accessible only by the Anti-Fraud Officer and staff delegated by him/her. The functional mailbox of the Anti-Fraud Office where the potential cases of fraud are reported is accessible only by the Anti-Fraud Officer and staff delegated by him/her. A specific password protected fraud register/database will be created, which will be accessible only by the Anti-Fraud Officer and staff delegated by him/her.

3. Legal analysis

3.1. Prior checking

The processing of personal data is performed by an agency 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; EMA will process information on suspected offences related to potential fraud and evaluate personal aspects to decide whether the information should be transferred to OLAF.[4]

---

[3] "OLAF shall respect the following retention periods for personal data collected in the course of OLAF investigations or coordination cases:
- Dismissed cases: Five years after the date of dismissal;
- Cases closed without Recommendations: Eight years after the date of closure of the case;
- Cases closed with Recommendations: Fifteen years after the date of closure of the case."
http://ec.europa.eu/anti_fraud/documents/data-protection/2013/isdpfinal_2013.pdf

[4] 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.

3.2. Data quality and special categories of data

According to Article 4.1(c) of the Regulation, personal information must be adequate, relevant and non-excessive in relation to the purposes for which they are collected and/or further processed. They must also be accurate and, where necessary, kept up to date (Article 4.1(d)).

There is a possibility that EMA, perhaps involuntarily, receives information that is of no interest or relevance to the investigation, also falling within special categories of data (see Article 10.1 of the Regulation).

Personal data and in particular special categories of data that are not relevant for the purposes of investigating fraud should not be further processed. Where reported and not necessary, they should be deleted. **EMA should therefore ensure that staff members are aware of the data quality requirements.**

3.3. Confidentiality

The EDPS stresses the importance of protecting the identity of whistleblowers, but also of preserving the confidentiality of all parties involved, including the accused persons and third parties.

The accused persons shall be protected in the same manner as the whistleblower, since there is a risk of stigmatisation and victimisation within their organisation. They will be exposed to such risks even before they are aware that they have been incriminated and the alleged facts have been investigated to determine whether or not they are substantiated.

In this regard, **EMA should ensure that the confidentiality of all parties involved, including the accused persons, is preserved. Consequently, EMA should limit the number of persons involved in the procedure to what is strictly necessary on a need-to-know basis.**[5]

3.4. Data retention

As a general principle, personal information must not be kept in a form which permits identification of persons for longer than is necessary for which the data are collected and/or further processed.[6]

The retention period for cases which will not be notified to OLAF and for which no further action is needed is three years. Such a retention period seems excessive, in particular with regard to the Opinion of Article 29 Working Party[7], which states that personal data processed by a whistleblowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. **The EDPS therefore invites EMA to re-evaluate the data retention period or provide further justification on the necessity to retain data for three years.**

---

[5] c.f. point 3.5 Transfer of data.

[6] See Article 4.1(e) of the Regulation.

[7] 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 See Article 29 Working Party Opinion 1/2006 on the application of EU data protection rules to internal whis

Concerning the conservation periods for cases notified to OLAF, the EDPS takes note of the fact that EMA has aligned its conservation periods with those of OLAF.

3.5. Transfer of data

In accordance with Article 7.1 of the Regulation, EMA is required to verify both that the recipients are competent and that the personal information is necessary to the performance of the related tasks.

The EDPS notes that the personal information transferred could lead to the identification of suspected persons, in particular through the description of the facts. Consequently, **the EDPS reminds EMA 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.** While for OLAF, this will be obvious in most cases; internal transfers should be duly assessed as to their necessity. In this regard, the EDPS considers that the description of potential recipients is too vague. **EMA should justify why a transfer of data, in particular to HR and Audit, is necessary**.[8] Moreover, it is good practice to internally document such transfers and their necessity.

3.6. 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. The Data Protection Notice attached to the notification includes the required information and will be made available on two different pages of the EMA website. The EDPS welcomes the fact that EMA in addition to this will inform and regularly update persons involved in a case on the progress of the proceedings. Since this could include information regarding other persons, **the EDPS would like to remind EMA that the persons involved should only receive information about themselves.**

Furthermore, the EDPS considers it **good practice to provide all persons involved with a specific privacy statement as soon as practically possible.** In the case of the persons accused, there may be reasons to defer this information under Article 20 of the Regulation. In case EMA uses Article 20 to restrict the rights of data subjects, this restriction and the reasons for it should be documented internally.

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. EMA should:

- Ensure that staff members handling information on potential fraud and irregularities are aware of the data quality requirements (point 3.2.);

[8] c.f. point 3.3 Confidentiality.

- EMA should ensure that the confidentiality of all parties involved, including the accused persons, is preserved. Consequently, EMA should limit the number of persons involved in the procedure to what is strictly necessary on a need-to-know basis (point 3.3.);

- Re-evaluate the data retention period or provide further justification on the necessity to retain personal data for three years regarding cases which will not be notified to OLAF and for which no further action is needed (point 3.4.);

- 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 and justify why a transfer of data, in particular to HR and Audit, is necessary (point 3.5.);

- Ensure that when informing persons involved in a case about the progress of the proceedings they only receive information about themselves (point 3.6.).

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

Done at Brussels, 16 December 2015

(signed)

Wojciech Rafał WIEWIÓROWSKI