EUROPEAN DATA PROTECTION SUPERVISOR

Prior Checking Opinion

"Anti-fraud reporting procedure"
Case 2013-0884

***

The anti-fraud reporting procedure set up by EACEA aims at analysing information about suspicions of irregularities or fraud in order to assess whether there are sufficient grounds for the Agency to transmit the information to European Anti-fraud Office (OLAF), which will further investigate potential fraud against the EU budget.

***

Brussels, 04 July 2016

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.eu.int Website: http://www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax : 32 2-283 19 50

1. Proceedings

On 19 July 2013, the European Data Protection Supervisor ("the EDPS") received from the Education, Audiovisual and Culture Executive Agency ("EACEA") a notification for prior-checking under Article 27(2)(a) of the Regulation (EC) n° 45/2001 ("the Regulation") regarding an anti-fraud reporting procedure for analysis and signaling suspicions of irregularities and/or fraud to the European Anti-fraud Office ("OLAF").

Additional information and factual changes to the procedure were provided to the EDPS at a further stage[1].

As this is an **ex-post case**, the deadline of two months for the EDPS to issue the Opinion does not apply.

2. Facts

The **legal basis** of the processing operation is Regulation n° 58/2003 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programs; Regulations n° 2185/96 and n° 1073/99[2]; Decisions C (2013) 2488, 2013/776/EU[3] and C(2013)9189[4]; the General Memorandum of Understanding between the Agency and its parent DGs, Staff Regulations, article 22; EACEA's Steering Committee decision of 9 June 2006[5]. The internal anti-fraud procedure[6] was also appended to the notification.

The **purpose** of the procedure is to signal and further analyse information about suspicions of irregularities and/or fraud in order to assess whether there are grounds to transmit the information to OLAF, which will further investigate potential fraud against the EU budget.

The procedure is described in a document called "*Procédure Anti-fraude - Signalement des suspsicions d'irrégularités/fraud*" (the "Anti-fraud reporting procedure"). In short, staff members are required to report to their Head of unit when being informed of any potential fraud. If the information is deemed serious, the Head of unit informs the anti-fraud officer of the R2 Unit (Finance, Accounting, Programming). If considered serious enough, the anti-fraud officer gathers the relevant services of the Agency. The conclusions of the meeting will either lead to a **non-case**, but which could still need to be followed as an operational issue within the operational unit(s) concerned, or to the confirmation of **possible irregularities or fraud**. In the latter case, EACEA establishes a plan of action. In this context, EACEA can

[1] Emails from EACEA of 20 May 2015, 3 June 2015 and 16 December 2015. See also EDPS requests for information in emails of 13 May 2015, 29 May 2015 and 30 October 2015. EACEA's DPO also provided additional info together with his comments on the draft prior checking Opinion sent to him by the EDPS on 18 May 2016 (cf. email of EACEA of 8 June 2016).

[2] Regulation n° 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission; Regulation n° 1073/99 of 25 May 1999 concerning investigations conducted by OLAF; the latter Regulation has been repealed and replaced by Regulation (EU) 883/2013 of 11 September 2013 concerning investigations conducted by OLAF.

[3] Commission Implementing Decision of 18 December 2013 establishing the 'Education, Audiovisual and Culture Executive Agency' and repealing Decision 2009/336/EC (2013/776/EU).

[4] Commission Decision of 18.12.2013 delegating powers to EACEA as last amended by the Commission Decision C(2016)1851 of 31.3.2016.

[5] EACEA's Steering Committee decision of 9 June 2006 laying down internal rules to prevent fraud, corruption and any illegal activity detrimental to the Communities' interest.

[6] Version of 28/02/2013.

only proceed with internal fraud/irregularity verifications (external verifications are reserved to OLAF). If, after verification, the suspicion of fraud is considered as sufficiently serious, following a prior consultation with the parent DG, a note (to which may be attached any relevant document) is transferred to OLAF with a request for investigation[7]. In the meantime, EACEA can take precautionary measures against the entity suspected of fraud or irregularities (e.g. identification of the affected contracts; reinforced control of the eligibility of expenditure; request for additional documents; launching of an audit; suspension of a payment, registration in EDES etc.). The latter is also part of another processing (Early Warning System that became EDES "Early Detection and Exclusion System" as of 01.01.2016) that is not covered by this notification. EACEA intends to file a separate notification in this respect.

The **personal information** processed in the context of external fraud/irregularity reporting cases may include name, address, email, phone numbers; position and responsibilities within various entities; personal data contained in the proposal/offer to and/or the agreement with the beneficiary of the funds, progress, interim and final reports required by the grant agreements (staff costs, time sheets, pay slips etc.); information on the conduct of the person giving rise to possible irregularities; personal data contained in the legal entity and bank account files; data on other grants/contracts managed by other services of the Commission involving the concerned entity or person.

In the context of internal fraud/irregularity reporting cases, the following information may be collected: name, address, email, phone numbers; CV, job description; information on the conduct of the person giving rise to possible irregularities; appraisal reports and probationary reports if they provide relevant information and evidence of the past and current behavior under scrutiny.

The entities and **persons** affected by the processing are external entities, e.g. beneficiaries, partners, contractors, involved in EU funding projects and their representatives or natural persons linked to them. In case of an internal fraud/irregularity investigation, the individuals concerned may be current or former staff members of EACEA. Whistleblowers, informants and witnesses are also listed in the notification.

General information is provided through a **specific privacy statement** to be published on EACEA's website and intranet. Moreover, when precautionary measures are adopted by the Authorising Officer (i.e. the Director/the Head of Department/the Head of unit of the operational unit managing the funds concerned), the concerned party is informed by a motivated decision about these measures. However, in order to protect the confidentiality of OLAF's investigation, if any, the Authorising Officer will not justify his decision on the investigation but on the elements having led to the suspicion[8]. When EACEA communicates suspicions of fraud on an individual to OLAF, it is up to OLAF to inform the individual about their investigation. In cases where EACEA concludes that there is no suspicion of fraud, EACEA does not specifically inform the individuals concerned either, referring, *a maiore ad minus* to OLAF practice to produce a privacy statement on their website, the supply of

[7] According to the notification and Article IV.D.2 of the Anti-fraud procedure, EACEA informs OLAF even when there is no suspicion of fraud. However, the controller indicated at a further stage (cf. email of 16 December 2015) that it was no longer the case, as the practice had changed in the meantime.
[8] See Section VI.1.A of the Anti-fraud reporting procedure.

specific information to the individuals involved in dismissed cases would involve disproportionate efforts[9].

The persons having access to the data and **recipients of the data** are, on a need-to-know basis, a restricted number of EACEA staff[10] and external law firms[11]. Regarding the parent DG, the recipients are the Director, the Head of unit where necessary and the anti-fraud officer. Within *OLAF*, the recipients are the Head of unit and selectors/investigators in charge of the case. The data may also be transferred to national authorities via OLAF (the latter being the only interlocutor of these authorities[12]) and to the EDES users in case of signalization of an entity in the EDES (ex-Early Warning System) database.

The **retention period** differs depending on the measures taken:

- Cases analysed by EACEA but not transferred to OLAF (no sufficient suspicion of fraud)[13]: 5 years after the implementation of the measures taken by the Authorising Officer to settle any operational issue, if any, or 5 years after dismissal in the absence of any measure.

- Cases transferred to OLAF but dismissed or closed by OLAF without recommendation: 5 years after the implementation of the precautionary measures taken in parallel by the Authorising Officer or 5 years after dismissal in the absence of measures by the Authorising Officer.

- Cases transferred to OLAF and closed by OLAF with follow-up recommendations: 5 years after the implementation of the actions recommended by OLAF in absence of measures taken by the Authorising Officer or 5 years after implementation of both set of actions if the Authorising Officer has taken additional or complementary measures.

[...]

3. Legal analysis

3.1. Prior checking

The processing of personal data is performed by an Agency of the European Union and is done, at least in part, through automatic means. Therefore, the Regulation is applicable.

[9] See EDPS Opinion of 3 October 2007 on OLAF treatment of non-cases (case 2007-205) and Opinion of 3 February 2012 on updated OLAF procedures (Cases 2011-1127, 2011-1129, 2011-1130, 2011-1131 and 2011-1132).

[10] i.e.
- the Director, the Head of department, the Head of unit and a limited number of agents of the unit managing the funds concerned, along with the anti-fraud officer, the legal officer and the ex-post Head of Sector.
- in very limited cases, the data may also be disclosed to Legal Service (Head of unit) and to other Directorates general (Head of units/anti-fraud officers) when the suspicion also concerns an entity or funds managed by these other services (*these two entities are not mentioned in the notification but were added at a later stage by EACEA - see email from EACEA of 16 December 2015*), as and the Head of the HR unit in case of an internal irregularity or fraud (*The notification also indicates IAC (the internal auditor), but the latter does no longer exist (cf. email from EACEA of 16 December 2015*).

[11] The service contract contains a confidentiality clause.

[12] See Section VII.A.1 of the Anti-fraud reporting procedure.

[13] As mentioned above (footnote No. 6), EACEA no longer informs OLAF of non-cases.

EACEA processes information on suspected offences related to potential fraud and evaluates personal aspects of individuals to decide whether the information should be transferred to OLAF. Thus, the processing activity presents specific risks and is subject to prior checking[14].

3.2. Legal basis

In December 2015, EACEA indicated some slight changes to the procedure (i.e.: modification of recipients, cases for which EACEA considers that there is no sufficient suspicion of fraud are no longer sent to OLAF for information, use of encrypted emails as additional security measure). However, these changes are reflected neither in EACEA's manual of anti-fraud procedure, nor in the notification.

Recommendation:
1. Update EACEA's manual of anti-fraud reporting procedure and the notification in order to reflect the factual changes in the procedure intervened since the date of the notification.

3.3. Special categories of data

Article 4(1)(c) of the Regulation states that personal data must be adequate, relevant and non-excessive in relation to the purposes for which they are collected and/or further processed.

There is a possibility that EACEA, perhaps involuntarily, receives information that is of no interest/relevance to the investigation, also concerning special categories of data under Article 10(1) of the Regulation (even if the notification states that no such data are processed).

Personal data and in particular special categories of data that are not relevant for the purposes of investigating fraud, should not be further processed.

Reminder:
EACEA should ensure that staff members are aware that data which are not relevant to the investigation should not be further processed.

3.4. Retention

According to Article 4 (1)(e) of the Regulation, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

With regard to the cases which will not be sent to OLAF and for which no further action is needed, a retention period of 5 years seems excessive on the basis of the information available.

Recommendation
2. EACEA should provide further justification about the necessity to retain data for 5 years or to re-assess the necessity and set up a necessary and proportionate retention period for

[14] According to Article 27 of the Regulation are subject 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.

cases not relevant to be transferred to OLAF and for which no internal action is taken by EACEA.

3.5. Information to the individuals involved

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

As to the **contents**, which must comply with Articles 11 and 12 of the Regulation, the EDPS underlines the following issues:

- *Identity of the controller* - EACEA, and not the Director of the Agency, is the controller. The Director, together with the Head of Unit R2 "Finance, accounting, programming" and the anti-fraud coordinator, are the organizational entities entrusted with the processing of personal data.
- *Categories of data processed*: The privacy statement does not say anything in this respect.
- *Recipients* - The list of recipients in the notification does not match the list of recipients in the data protection statement.
- *Rights of access and rectification* - EACEA should not only mention the existence of these rights but also explain how individuals can exercise their right of access and rectification. Thus, EACEA should mention the contact information of the person/service in charge of the processing operation, such as a functional email address. In addition, it is good practice to include information on time limits within which a reaction can be expected (e.g. 3 months for access request, without delay for rectification, etc.).
- *Right to recourse to the EDPS* - Individuals have a right to recourse to the EDPS at any time[15]. However, the data protection statement refers to a two-steps procedure with a possibility to submit their case to the EDPS "*should the conflict not be resolved by the Controller or the Data Protection Officer*." This wording may give the impression that the individuals concerned are obliged to go to the controller or DPO first. EACEA should clarify this point by making clear that individuals concerned are recommended to try to resolve the conflict with the controller or DPO before filing a complaint with the EDPS but that they have the right to recourse to the EDPS at any time.
- *Time-limits for storing the data* - EACEA should further explain the starting point of the retention period (the current text only refers to "a maximum period of 5 years"). In addition, the retention period should be adapted, if need be, as regards non-admissible cases for which no measures are taken (see above recommendation No. 2).

As to the **availability** of the information, besides the publication of a data protection statement on EACEA's website and intranet, EACEA informs individuals when precautionary measures are taken as a result of a suspicion of fraud or irregularity. However, they are not informed on the investigation but only on the measures taken as a consequence.

As the controller of the processing operation before the possible transfer of the file to OLAF, EACEA should, as a matter of principle, ensure that data subjects are informed when opening a case and until the data is transferred to OLAF. It might be however necessary to restrict the right of information of data subjects, as such restriction might be a necessary measure to safeguard any of the exceptions under Article 20 of the Regulation.

[15] Article 11(f)(iii) and 12(f)(iii) of the Regulation.

For cases that are transferred to OLAF (serious suspicions of fraud), the EDPS understand that EACEA defers the obligation to inform to OLAF so as to avoid undermining OLAF's investigation (exception based on Article 20(1)(a) of the Regulation). By contrast, for non-cases, EACEA should inform the individuals concerned and cannot invoke disproportionate efforts in the respect. It could however momentarily defer the information, for example if new elements as regards potential fraud are expected in relation to the individual (Article 20(1)(a) of the Regulation) in question or if there are risks of retaliation of the individual under examination against anyone that may have denounced suspicions to EACEA (Article 20(1)(c) of the Regulation. Any decision to restrict the right of information should be taken on a case-by-case basis, duly documented[16] and regularly re-assessed.

Recommendation

3. Adapt or complete the contents of the data protection statement as regards the identity of the controller, the categories of data processed, the list of recipients, the exercise of the rights of access and rectification, the right to recourse to the EDPS and the time-limits for storing the data.

Reminder

Inform individuals concerned when opening an anti-fraud reporting case (privacy statement attached), unless an exception to the right of information applies, in which case the exception will have to be duly documented.

3.6. Transfers

Reminder

Comply with the requirements of Article 8(b) of the Regulation when transferring data to external law firms representing third parties and of Article 23 of the Regulation when transferring data to law firms representing EACEA's interests.

[16] See EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, 25 February 2014 - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf, especially pages 27 and following.

3.7. Security measures

[...]

* *
*

In order to comply with the Regulation, EACEA should implement the above-mentioned recommendations and inform the EDPS of the measures taken based on the recommendations of this Opinion within a period of **four months**.

Done at Brussels, 04 July 2016

(signed)

Wojciech Rafał WIEWIÓROWSKI