

Opinion on a notification for Prior Checking received from the OLAF Data Protection Officer regarding the Customs File Identification Database (FIDE)

Brussels, 17 December 2014 (2013-1003)

1. Proceedings

On 9 September 2013, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking relating to the processing of personal data in **the Customs File Identification Database (FIDE)** from the Data Protection Officer (**DPO**) of OLAF.

Questions were raised on 18 September 2013, to which OLAF replied on 15 November 2013. On 16 and 17 December 2013, the EDPS carried out an inspection at OLAF, which also included FIDE in its scope (separate case: 2013-1261). The draft Opinion was sent to the DPO for comments on 24 November 2014. The EDPS received a reply on 12 December 2014.

2. The facts

FIDE is an index of natural and legal persons suspected of or condemned for operations in breach of customs or agricultural legislation. It is based on Title Va of Regulation (EC) 515/1997, as amended by Regulation (EC) 766/2008.

FIDE is accessible to customs authorities. Its purpose is to enable these authorities to find out if persons or entities they are investigating are/have also been investigated or convicted in other Member States. Additionally, the Commission may use the system when opening a coordination file (Article 18 of Regulation 515/1997 as amended) or when preparing a Union mission in a third country (Article 20 of the same Regulation).

The data subjects can be grouped in the following categories, with different maximum (non-cumulative) conservation periods, all counting from the opening of the national investigation:

1. persons suspected of committing, having committed or having participated in operations in breach of customs or agricultural legislation (conservation period: maximum three years, yearly renewals necessary);
2. persons who have been the subject of a finding related to such operations but not (yet) convicted or ordered to pay a fine (conservation period: maximum six years);
3. persons who have been the subject of an administrative or judicial penalty for such operations (conservation period: maximum ten years).

The data originate from the national files of customs authorities.¹ For all three categories, data have to be deleted immediately when the person has been cleared of suspicion. If the underlying national databases have shorter conservation periods, the supplying Member State must remove the data from FIDE as well. In any case, the conservation period must never

¹ National authorities may upload their cases relevant for FIDE's aim as defined in Article 41a(2) of Regulation 515/1997 as amended.

exceed ten years. At the expiry of the relevant maximum period, files are automatically deleted.

Additionally, limited personal data are stored about the users of the system (authorised staff of OLAF and national designated competent authorities - e.g. name, access rights, authority they are attached to).

Files in the system can be created by authorised users.² The data fields for "person" entries are the following:

1. First name
2. Family name
3. Maiden name
4. Alias
5. Date of birth
6. sex
7. Area concerned (drop-down list, e.g. tobacco smuggling, cash seizures, etc.)
8. Status (as per the list of data subject categories above)
9. Reference number of the national investigation.

At least one data field out of 1, 2 and 4 must be filled; fields 7 to 9 are mandatory. The section on categories of data in the notification form states that no data falling under Article 10 are included in the system. Files may be updated (e.g. adding new aliases, changing the status) by the authority that entered them into the system.

Users of the system can query it using names and aliases of suspects (there is both an "exact" search and an "includes" search; in the latter case, there is a minimum length for the search string). It is not possible to search by the national reference number of a case.

In case of a hit, users are informed about which authority has information about the person in question as well as the case reference used by that authority. This information can then be used to contact the relevant authority for assistance or to provide information to them in line with applicable customs legislation.³

Data subjects can exercise their rights by contacting OLAF, which may apply restrictions. A privacy statement is available on OLAF's website.

Lists of authorities authorised to access and use FIDE (including the number of staff authorised in each authority) have been published.⁴

[...]

² The system distinguishes between "normal" users, whose draft files need to be validated by a "privileged" user before publication in the system and "privileged" users, whose cases are published without this additional verification step.

³ See Articles 4 to 16 of Regulation (EC) 515/1997, as amended.

⁴ OJ C 366 14/12/2013, pp. 11-32.

3. Legal analysis

3.1. Prior checking

The processing of personal data under analysis is carried out by a Union body in the exercise of activities which fall within the scope of Union law. The processing of the data is done through automatic means. Therefore, Regulation (EC) 45/2001 is applicable.

In principle, the EDPS does not prior-check tools as such, but procedures carried out by Union bodies. That being said, hosting FIDE and its use by OLAF constitute processing of personal data.

Article 27(1) of Regulation (EC) 45/2001 subjects to prior checking by the EDPS all "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 contains a list of processing operations that are likely to present such risks.

The notification mentions points (a) to (c) of Article 27(2) as such risks posed by the processing.

Point (a) relates among others to processing personal data related to suspected offences, offences and criminal convictions. Making such data available to competent authorities in the Member States is the main aim of FIDE.

The notification also mentioned point (b) of this Article, which relates to processing operations intended to evaluate the data subject. FIDE only tells its users whether a certain person/entity is/has been under investigation by customs authorities in the Member States. This is a statement of fact: an investigation either exists/existed or not. FIDE on its own does not allow any further evaluation.

Point (c) relates to processing operations allowing linkages between data processed for different purposes not provided for in national or Union legislation. Whereas "linking" (by creating an index) different databases is the aim of FIDE, this is expressly provided for in Union legislation (Regulation (EC) 515/1997 as amended, Title Va). Article 27(2)(c) therefore does not apply. In any case, FIDE is subject to prior checking under Article 27(2)(a).

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case however the processing operation has already been established. Any recommendations made by the EDPS still have to be implemented accordingly.

The notification of the DPO was received on 9 September 2013. As this is an ex-post case, the deadline of two months does not apply. This case has been dealt with on a best-effort basis. On 18 September 2013, the EDPS asked questions about the notification; replies were received on 15 November 2013. On 16 and 17 December 2013, the EDPS carried out an inspection at OLAF, which also included FIDE in its scope. On 27 November 2014, a draft Opinion was sent to the DPO for comments; on 12 December 2014, the DPO confirmed that OLAF had no comments.

3.2. Lawfulness of the processing

The grounds for lawfulness are listed in Article 5 of the Regulation. Article 5(a) lists processing that is "*necessary for performance of a task carried out in the public interest on*

the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof".

FIDE is established by Title Va (Articles 41a to 41d) of Regulation (EC) 515/1997, as amended, which sets out the purposes of the system as well as specific rules on its use, conservation periods and other aspects.⁵ The system serves to facilitate cooperation between competent Member States' authorities in customs investigations, safeguarding financial interests of the Member States and the Union.

The processing is thus in principle lawful under Article 5(a) of the Regulation.

3.3. Controllership

Article 2 (d) of the Regulation defines "*controller*" as the "*Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data.*" The assessment of who is the controller shall be based on who actually does this.

The notification only referred to an official at OLAF as the person responsible for the processing. The EDPS notes that OLAF as an organisation is the controller; while where necessary an official can be considered as the "controller in practice" or be indicated as a contact point, final accountability remains with the organisation as such.

Additionally, it is clear from the description of the processing operations that the competent authorities in the Member States should also be considered controllers besides OLAF.

The setup of the systems implies that some of the tasks of a controller cannot be fulfilled by OLAF but only by the competent authorities in the Member States. For example, Article 4(2) of the Regulation obliges the controller to ensure that the principle of data quality is respected. OLAF can contribute to this by setting up the system in a way that no clearly irrelevant data may be processed and by providing information on its proper use, but the actual uploading and amending of data, the decision on whether or not to extend storage for "suspicion" cases, as well as the assessment *in concreto* which data should be uploaded is done by the competent authorities in the Member States. Similarly, as competent authorities are the only ones capable of changing data uploaded by them, the right to rectification which, according to Article 14, is incumbent on the controller needs to be ensured by them. This shows that they cannot be regarded as mere users of the system.

In this regard, FIDE mirrors other large-scale IT systems, such as the Schengen Information System or the Customs Information System, in which a Union body is responsible for the setting up and the operational management, but does not upload the actual data to the system. OLAF is the party setting up FIDE giving concrete form to the authorisation in the legal basis. In this sense, it (partly) determines the means and purposes of processing. The competent authorities in turn are more than just users of the system and partly determine the purpose of the processing. It is thus appropriate to consider the competent authorities connected to the systems and OLAF as co-controllers of the systems. This has implications for liability as well, with each controller being responsible for its own processing operations. OLAF is responsible for the management of the central system, including its security. The competent authorities in the Member States are responsible for the uploading and amending of data and their own use of the systems.

⁵ For matters not specifically regulated in Title Va, the rules of Title V on the Customs Information System applies *mutatis mutandis* (see Article 41a(1) of Regulation (EC) 515/1997).

Recommendation: The co-controllership between OLAF and the national competent authorities as developed above should be reflected in the notification form and the information to data subjects.

3.4. Processing of special categories of data

Personal data relating to offences, criminal convictions or security measures may only be processed if authorised by the Treaties or other legal instruments based on them (Article 10(5)) of the Regulation).

This condition is fulfilled for FIDE, as the processing of data related to (suspected) offences and convictions is explicitly mentioned in Article 41b of Regulation (EC) 515/1997, as amended.

The section on categories of data in the notification form states that no data falling under Article 10 are included in the system. This is not the case, as it is correctly acknowledged in the notification's section on grounds for prior checking. Even though there is no detailed information on the (suspected) offences included in the system, the fact alone that a person appears in it means he/she is or has been investigated or convicted for a breach of customs or agricultural legislation; this information already falls under Article 10(5).

Recommendation: correct the section on categories of data in the notification form and provide an updated version to the EDPS.

3.5. Data Quality

Data must be adequate, relevant and non excessive in relation to the purposes for which they are collected and/or further processed (Article 4(1)(c)).

The categories of data which can be included in the system are adequate, relevant and not excessive for the purpose of finding out if other authorities are/have been investigating the same person; dates of birth can help to distinguish between persons sharing the same name. The inclusion of the gender of persons concerned is also not excessive. No information on the content of investigations / convictions (beyond the area concerned) is made available in case of a hit. Such information would need to be obtained using the mutual assistance mechanisms of Regulation (EC) 515/1997 as amended, or bilateral cooperation, both of which are outside the scope of this prior check Opinion.

The data subject has the right to access and the right to rectify data (although some restrictions may apply, see 3.7 below), which also makes it possible to ensure the quality of data.

As the content of the system is provided by the competent authorities in the Member States, it is in the first place up to them to ensure that the content of files included in the system is accurate and up-to-date. Nonetheless, OLAF should make sure that Member State authorities are aware of their obligations (notably under Article 41d(2) of Regulation (EC) 515/1997), for example by providing regular reminders, disseminating best practices or other measures.

3.6. Conservation of data

As a general principle, personal data should not be kept in a form which permits identification of data of data subjects for longer than is necessary for the purpose which the data are collected and/or further processed (Article 4(1)(e) of the Regulation).

In the case of FIDE, the maximum conservation periods are set out in the Regulation establishing it. At the end of the maximum conservation period, data are automatically deleted. Combined periods must not exceed ten years. In line with Article 41d(2), personal data are also to be deleted immediately (i.e. before the expiry of the standard conservation period) when the data subject has been cleared of suspicion under the law of the Member State which included the information in the system or if the conservation period of the underlying national database expires.

3.7. Rights of access and rectification

The privacy statement informs data subjects that they have the rights to access and rectify their data and provides contact information for the controller to this end, noting that restrictions under Article 20(1) points (a) to (c) may apply.

Points (a)⁶ and (b)⁷ are the most relevant cases here. Given the content of FIDE, such restrictions might be necessary, notably for requests received when a case is still in the suspicion stage. Denying access and/or rectification should always be based on a case-by-case analysis.

3.8. Information to the data subject

Article 12 of the Regulation establishes which information is to be given to the data subject if data are not directly collected from him/her. Article 12(2) allows abstaining from personalised information under certain conditions.

OLAF has published a privacy statement concerning FIDE on its website. Lists of authorities having access to FIDE have been published in the Official Journal of the European Union.

With the information available to OLAF, which notably excludes address information, it would be difficult for OLAF to contact persons included in it individually. It is therefore acceptable for OLAF not to provide personalised information to all persons listed.

Nonetheless, OLAF should invite Member States to include a reference to FIDE in the information they provide to data subjects under their respective national rules (both general and personalised). Including a link to the lists of authorities having access in OLAF's privacy statement could also increase transparency.

Recommendation: invite Member States to include a reference to FIDE in the information they provide to data subjects under their respective national law (both general and personalised). Include a link to the lists of authorities having access to FIDE in OLAF's privacy statement.

3.9. Security measures

[...]

4. Conclusion:

⁶ Allowing restrictions when they are "a necessary measure to safeguard [...] the prevention, investigation, detection and prosecution of criminal offences;"

⁷ Allowing restrictions when they are "a necessary measure to safeguard [...] an important economic or financial interest of a member State [...]"

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing that the recommendations contained in this Opinion are fully taken into account. To recall, the EDPS recommends that OLAF should:

- Mention the joint controllership between OLAF and the national competent authorities in the notification form and the information to data subjects;
- correct the section on categories of data in the notification form and provide an updated version to the EDPS;
- include a link to the lists of authorities having access in OLAF's privacy statement.

The EDPS expects that OLAF implement the recommendations accordingly and will close the case.

Done at Brussels, 17 December 2014

(signed)

Giovanni Buttarelli
European Data Protection Supervisor