Data Protection at OLAF

Laraine Laudati

eucrim
European Law Forum: Prevention • Investigation • Prosecution

AUTHOR

Laraine Laudati

CITE THIS ARTICLE

Laudati, L. (2013). Data Protection at OLAF. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2013-002

Published in eucrim 2013, Vol. 8(1) pp 14 – 17

https://eucrim.eu

ISSN:

The European Anti-Fraud Office (OLAF) is charged with protecting the EU's financial interests by investigating fraud, corruption, and other illegal activities. OLAF's daily work involves the processing of large amounts of sensitive[1] personal data. As a service of the European Commission, OLAF is subject to Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies (data protection regulation) and is thus under the supervisory powers of the European Data Protection Supervisor (EDPS). OLAF conducts administrative investigations in full independence, both internally – concerning the EU institutions and bodies – and externally – concerning economic operators located in the Member States and third countries. In order to help protect its independence when conducting investigations, OLAF is the only service of the European Commission that has appointed its own Data Protection Officer (DPO); the Commission has appointed one DPO for all of the other services combined.

Investigations are handled by approximately 130 OLAF investigators and other case handlers who have widely different backgrounds and whose home Member States have varying traditions with respect to the processing of personal data. OLAF, with the help of its partner authorities, must gather evidence that may be located in Member States and third countries and it must thus exchange personal data with those authorities in the course of its investigations. Its final reports and recommendations, which contain personal data, are often sent to prosecutors and judicial authorities in the Member States who pursue criminal charges for the fraud that is the subject of the OLAF investigation. Accordingly, OLAF operates in a highly complex environment in which the demands of the data protection regulation touch the work of its investigators on a daily basis. OLAF is fully committed to fulfilling these demands.

The key players in an OLAF investigation (persons concerned, informants, whistle-blowers, and witnesses) are "data subjects" who have rights under the data protection regulation, which OLAF must respect. These include the rights of information about their data being processed and of access to such data. If they believe the processing of their data is illegal, they also have the right to object as well as rights of rectification, blocking, and erasure of their data.

This article shall describe how OLAF complies with data protection requirements in performing its investigative function. It begins by explaining OLAF's notification of its personal data processing operations to its DPO and its "prior checking" of the sensitive processing operations with the EDPS. The elements of the OLAF data protection "toolbox" which has been created to assist OLAF investigators ensure that they perform their daily tasks in full compliance with the requirements are next described. The challenges OLAF has faced in relation to transferring personal data to its partner Member State authorities and third country authorities are then considered. It will be shown that, through the continuous efforts of OLAF and the practical approach of the EDPS geared towards finding workable solutions, Regulation (EC) 45/2001 has proven sufficiently flexible in allowing OLAF to achieve compliance without undue administrative burden.

I. OLAF's Notifications and Prior Checks

The data protection regulation requires that the controller (defined as the organizational entity that determines the purposes and means of a processing operation) give prior notice to the DPO of any personal data processing operation for which it is responsible. The DPO is charged with maintaining a public register of all such notifications. OLAF's register is available on its "Europa" website.[2] It contains approximately seventy notifications of processing operations currently underway at OLAF.

The regulation requires that processing operations "likely to present specific risks," as defined therein, are subject to prior checking by the EDPS. Approximately half of OLAF's processing operations have been subject to prior checking, mainly because they relate to one of the specific risks listed, that is, "to suspected

https://doi.org/10.30709/eucrim-2013-002

offences, offences, criminal convictions or security measures" and/or that they are "intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct." The EDPS has issued prior checking opinions for these processing operations, all of which may be seen at the OLAF Europa website.[3] These opinions all contain recommendations that OLAF has implemented or, for a few of them, that are still in the process of being implemented. OLAF reports back to the EDPS on which steps it has taken to implement the recommendations, and once the EDPS is satisfied with the implementation, he closes the prior checking case.

The recommendations of the EDPS in his prior checking opinions have had an important influence on how OLAF observes data protection requirements. Through exchanges and discussions with the EDPS, OLAF has resolved key issues of how to apply the data protection regulation in the context of its investigations. For instance, OLAF initially had difficulty interpreting the "information" requirement, that is, the requirement that all data subjects receive certain information specified in the regulation. Given that case files contain the names of many persons, a large number of whom may have no relevance to the investigation, it would be an excessive burden for OLAF personally to inform all such persons, with no benefit to them. A practical solution was found with the EDPS: to provide a personalized privacy statement only to the key players in an investigation (persons concerned, informants, whistle-blowers, and witnesses). The non-relevant data subjects could access OLAF's privacy statements on the OLAF Europa website. This application of the information requirement to data subjects whose data is in OLAF case files has allowed OLAF to implement the requirement in a practical and feasible manner.

II. The OLAF Investigator's Data Protection Toolbox

Three elements have been developed to help OLAF's investigators comply with data protection requirements in their daily work: OLAF Instructions to Staff on Data Protection, OLAF workforms, and the OLAF Data Protection Module.

1. OLAF Instructions to Staff on Data Protection

The OLAF Instructions to Staff on Data Protection for Investigative Activities (ISDP) were adopted by the Director General in April 2013, replacing data protection guidelines that had originally been adopted in 2006.[4] The new instructions specify in practical terms what the investigator must do to satisfy data protection requirements in all aspects of his/her work. The main sections of the ISDP are: Definitions, Data Quality, Information to the Data Subject, Other Rights of the Data Subject, Transfers and Complaints. The ISDP implements many of the recommendations of the EDPS included in his prior checking opinions on OLAF investigations, his inspection reports, and his decisions on complaints made by data subjects against OLAF.

The data quality requirements specify that any personal data gathered must be adequate, relevant, and not excessive in relation to the purpose of the processing concerned, which must be analyzed on a case-by-case basis.

The ISDP defines "relevant data subjects" in an OLAF investigation as "natural persons who have relevance for an OLAF case, including: persons concerned, informants, whistleblowers and witnesses, as well as natural persons who are, exceptionally, named in a recommendation of an OLAF coordination case to a national judicial authority." As stated above, any data subject fitting this definition must receive a personalized privacy statement in the course of the investigation.

The requirements for making transfers of personal data to other EU institutions/bodies, Member State authorities, and third country authorities and international organizations are specified. The instructions set

forth the procedures to be followed at OLAF when handling requests from data subjects in exercise of their rights under the regulation – the rights of access, rectification, blocking, erasure, and objection – as well as complaints by data subjects. Procedures for deferring observance of data subjects' rights, when necessary and in the observance of the legal requirements of the regulation, are also set forth.

Finally, the instructions spell out exactly what the investigator must record in the Data Protection Module.

2. OLAF Workforms

OLAF workform templates have been developed, which investigators must use in carrying out the various steps of an investigation. OLAF has incorporated the concept of "privacy by design" in these workforms by including in the template any necessary data protection paragraphs. More specifically, any workform designed to be sent or otherwise provided to a relevant data subject contains a "privacy statement," including all of the information which the data protection regulation obliges the controller to provide to the data subject. Any workform designed to be sent outside of OLAF to any recipient other than a data subject, and which may contain personal data, includes a "transfer clause," specifying what use the recipient can make of the data and indicating how the data should be handled. Different transfer clauses are required, depending on the type of recipient – an EU institution or body, a Member State authority, or a third country authority or international organization – which reflect the differing requirements for each of them under the data protection regulation. Accordingly, by using the official OLAF workform to prepare case-related documents, the investigator automatically meets the requirements of providing a privacy statement to relevant data subjects and of including a transfer clause in its correspondence that contains personal data.

3. OLAF Data Protection Module

The electronic case files for all OLAF cases are stored in the Case Management System (CMS). A Data Protection Module (DPM) has been created within the CMS and is used to store information about compliance with all data protection requirements for each relevant data subject in each OLAF case. Investigators must list the names of all relevant data subjects when a case is open. As soon as a privacy statement has been provided to a relevant data subject, this must be recorded in the module. If a data subject submits a request for access, rectification, blocking or erasure, or an objection, the request and all OLAF responses must be recorded in the DPM. If OLAF must defer provision of a privacy statement or a reply to a request, the deferral must be recorded in the DPM, thereby making it easy to monitor deferrals and ensuring that the privacy statement or other information or responses are eventually provided once the reason for the deferral no longer exists. Complaints from data subjects and their replies are also stored in the DPM. OLAF's management, its DPO, and the EDPS can also use the DPM to gain an overview of the state of OLAF's compliance with data protection requirements in its case files.

III. OLAF's Transfers of Personal Data

OLAF may transfer personal data to EU institutions/bodies, Member State authorities, third country authorities and international organizations during the course of an investigation or upon its completion. During the investigation, it may be necessary to transfer a name and other personal information in order to request assistance from a partner authority or to reply to a request for assistance or otherwise assist a partner by, for example, sending interview records or mission reports. After an investigation is closed, it may be necessary to transfer personal data included in a final report when OLAF issues recommendations to be implemented by the recipient authority. The categories of data that may be transferred include identification

https://doi.org/10.30709/eucrim-2013-002

data, professional data, and case involvement data (data relating to the allegations and/or facts concerning matters under investigation by OLAF).

Articles 7, 8, and 9 of Regulation (EC) 45/2001 govern transfers of personal data to EU institutions/bodies, Member State authorities, and third country authorities/international organizations, respectively. Under Article 7, a transfer within or between EU institutions/bodies can be made, if necessary, for the performance of a task covered by the competence of the recipient. Under Article 8, a transfer to a Member State authority can be made, *inter alia*, if the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority. Under Article 9, a transfer to a third country authority or international organization is possible if an "adequate level of protection" is ensured in the country of the recipient or within the recipient international organization and if the data are transferred solely to allow tasks covered by the competence of the recipient to be carried out. If the recipient does not have an adequate level of protection, then it would be possible, exceptionally, to make a transfer by way of derogation if, *inter alia*, the transfer is necessary or legally required on important public interest grounds or for the establishment, exercise, or defense of legal claims. However, if systematic transfers are to be made to a third country authority or international organization that does not have an adequate level of protection, then the EDPS may authorize a set of transfers where the controller adduces adequate safeguards, e.g. through data protection clauses, for protection of the data subject's rights.

EDPS prior checking opinions relating to OLAF investigations have emphasized that, for transfers under Articles 7 and 8 of Regulation (EC) 45/2001, notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted. He also emphasized that even if a transfer of information is foreseen in other relevant legislation, the transfer is only lawful if it also meets the requirements established in the data protection regulation. Further, he recommended that an analysis of the necessity of the transfer has to be carried out *in concreto* on a case-by-case basis, that the proportionality factor must be taken into account, and that a note to the file should be made specifying the need for the transfer.

For transfers under Article 9, Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[5] provides that the Commission may find that a third country ensures an adequate level of protection by means of domestic law or international commitments as regards protection of private lives, basic freedoms, and individual rights.[6] However, OLAF must transfer data to authorities in a number of countries where the Commission has not yet concluded that an adequate level of protection exists. Thus, in 2005, it initiated a consultation with the EDPS on how it could make such third country transfers while respecting data protection requirements. The EDPS concluded, in a 2006 decision, that OLAF would need adequate safeguards in a specific legal framework for "repeated, mass or structural" transfers, which could be included in memoranda of understanding with OLAF's partners. For occasional transfers, OLAF could rely on the exception mentioned above, but this could not be relied upon for systematic use because it would not ensure that the rights of the data subject are protected.

OLAF thereafter developed a first model Administrative Cooperation Arrangement (ACA), with an annex containing data protection clauses designed to provide adequate safeguards. In December 2006, the EDPS indicated that the data protection clauses provided a good basis for moving forward in addressing the need for adequate safeguards. In 2010, OLAF undertook the simplification of the data protection clauses and submitted a revised version to the EDPS. The revised data protection clauses include definitions, joint obligations, OLAF obligations, partner obligations, resolution of disputes, and suspension and termination clauses. Following extensive discussions with the EDPS on the revised clauses, the EDPS made recommendations in letters dated 3 April 2012[7] and 16 July 2012[8] and OLAF has implemented those recom-

mendations. The EDPS is expected to react on the final version of the model data protection clauses in the near future. On the basis of these clauses, several new ACAs have been concluded.[9]

IV. Conclusion

This article has presented an overview of how OLAF has implemented data protection requirements in the context of its investigations. Notwithstanding the enormity of the task of ensuring that each relevant data subject's rights are observed in the course of each OLAF investigation – by the approximately 130 investigators and other case handlers from all EU Member States – OLAF has, through good collaboration with the EDPS, found practical solutions. Through its use of "privacy by design" in its workform templates, its DPM, and its ISDP as well as the data protection training of its staff, OLAF has developed a system which ensures observance of the rights of the many data subjects whose personal data it processes during its investigations.

---

1. The data is sensitive because it may include allegations and facts concerning the possible involvement of individuals in matters under investigation by OLAF. This is to be distinguished from "special categories of data" within the meaning of Article 10 of Regulation (EC) 45/2001, which is sometimes referred to as sensitive data.↩
2. "Europa" is the public website of the European Union. OLAF's register may be viewed at the following URL within the Europa website: http://ec.europa.eu/anti_fraud/dataprotectionofficer//register/index.cfm?TargetURL=D_REGISTER↩
3. The EDPS' opinions concerning OLAF's prior checks may be viewed at the following URL: http://ec.europa.eu/anti_fraud/about-us/data-protection/processing-operations/prior_checking_en.htm.↩
4. The ISDP may be viewed at the following URL: http://ec.europa.eu/anti_fraud/about-us/data-protection/index_en.htm.↩
5. O.J. L 281, 23.11.1995, p. 31.↩
6. To date, the Commission has made adequacy findings for the following: Andorra, Argentina, Canada, Eastern Republic of Uruguay, Faeroe Islands, Guernsey, Isle of Mann, Israel, Jersey, New Zealand, Switzerland, and the PNR and Safe Harbour provisions for the USA.↩
7. The letter is published on the EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2012/12-04-03%20Model%20Data%20Protection%20Clauses_OLAF_D-746_EN.pdf.↩
8. This letter analyses the data protection clauses under Article 9(6) of Regulation 45/2001, and not for an authorisation for massive or structural transfers under Article 9(7). The letter states that OLAF should notify the EDPS in cases where the transfers become massive or structural, to request an authorisation under Article 9(7). The letter is published on the EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2012/12-07-16Model%20Data%20Protection%20Clauses_OLAF_D-1051_EN.pdf.↩
9. A list of all ACAs that OLAF has entered into can been viewed at: http://ec.europa.eu/anti_fraud/documents/international-cooperation/aca_third_countries_and_dp_annex_en.pdf.↩

legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union

https://doi.org/10.30709/eucrim-2013-002