OLAF Guidelines on Data Protection for Investigative Activities

Table of Contents

ARTICLE 1. DEFINITIONS 3

ARTICLE 2. DATA QUALITY REQUIREMENTS 4

ARTICLE 3. SPECIAL CATEGORIES OF DATA 4

ARTICLE 4. RECORDS OF PROCESSING OPERATIONS AND DATA PROTECTION IMPACT ASSESSMENT 4

ARTICLE 5. INFORMATION TO THE DATA SUBJECT 5

ARTICLE 6. TRANSMISSION AND TRANSFER OF PERSONAL DATA OUTSIDE OLAF 6

ARTICLE 7. THE RIGHTS OF ACCESS, RECTIFICATION, RESTRICTION, ERASURE AND OBJECTION 7

ARTICLE 8. COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT AND THE EDPS 8

ARTICLE 9. OTHER DATA SUBJECT REQUESTS 8

ARTICLE 10. RESTRICTION OF DATA SUBJECT RIGHTS 9

ARTICLE 11. LEGALITY CHECK OF DATA PROTECTION COMPLIANCE 9

ARTICLE 12. RETENTION OF PERSONAL DATA 10

INTRODUCTION

Under EU law, data protection is a fundamental right and OLAF is subject to the requirements of Regulation (EU) 2018/1725[1].

These Guidelines to Staff on Data Protection (GSDP) are internal rules which ensure that all OLAF staff performing investigative activities implements data protection requirements in a consistent and coherent way in accordance with Regulation (EU) 2018/1725 and Commission Decision (EU) 2018/1962[2], laying down internal rules on the provision of information to data subjects and the eventual restrictions of their rights.

The present guidelines cover OLAF activities conducted under Regulation (EU, Euratom) 883/2013[3] as defined in the investigative procedures: activities during selection, internal and external investigations, investigations complementary to or in support of the EPPO ongoing investigations, coordination cases and cases where the office supports the EPPO, on request.

The data protection pages of the OLAF intranet contain additional information concerning the processing of personal data by OLAF.

Article 1. Definitions

1.1. Data subject, personal data, processing of personal data: See definitions in Article 4 of Regulation (EU) 2018/1725. Legal and deceased persons are not considered as data subjects in accordance with Recital 6 of Regulation (EU) 2018/1725. Exceptionally, information in relation to single-member private limited companies/sole person companies may constitute personal data where it allows the identification of a natural person[4].

1.2. Special categories of data: see Article 10.1 of Regulation (EU) 2018/1725.

1.3. The Controller of OLAF's processing operations is the Office as represented by the Director General.

1.4. Delegated controller: the entity that carries out a processing operation on behalf of the Office, as applicable, is mentioned as such in each record of OLAF's processing operations. For investigative activity, the unit in charge of the OLAF case is acting as delegated controller, specific rules may apply. This entity is represented by:

- **The Head of Unit**, if only one unit is involved in the processing;

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ L 295, 21.11.2018, p. 39-98*.

[2] Commission Decision (EU) 2018/1962 of 11 December 2018 laying down internal rules concerning the processing of personal data by the European Anti-Fraud Office (OLAF) in relation to the provision of information to data subjects and the restriction of certain of their rights in accordance with Article 25 of Regulation (EU) 2018/1725 of the European Parliament and of the Council C/2018/8654*, OJ L 315, 12.12.2018, p. 41–46.*

[3] 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, *OJ L 248 18.9.2013, p. 1-22*.

[4] Judgment of the Court of Justice of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197.

- **The Director**, if two or more units in one directorate are involved in the processing; or

- **The Director-General**, if two or more directorates are involved in the processing.

1.5. Data Protection Officer (DPO): see Article 43 and 45 of Regulation (EU) 2018/1725 and Article 10.4 of Regulation (EU, Euratom) 883/2013.

1.6. Relevant data subject: natural persons who have relevance for an OLAF case, as listed in Art 3.2 of Commission Decision (EU) 2018/1962: Persons concerned as defined in Article 1.5 of, Regulation (EU, Euratom) 883/2013 and informants and witnesses as defined in the Guidelines on Investigation Procedure for OLAF Staff (GIP).

Article 2. Data Quality Requirements

2.1. All OLAF staff shall ensure that the personal data they are processing in the course of their work meets data quality requirements. In particular, they shall ensure that the personal data gathered are adequate, relevant and not excessive in relation to the general purpose and the particular purpose of the processing concerned. Names and other personal information should be included in the processing operation only if adequate and relevant, and should be strictly confined to what is necessary. This shall be analysed in concreto, on a case-by-case basis.

2.2. The investigation unit shall ensure that the processing of personal data is adequate, relevant and not excessive in relation to the general purpose of combating fraud and the particular purpose of the investigation.

2.3. OLAF staff should take all reasonable steps to ensure that personal data gathered from any source, and/or transferred to any recipient, are accurate and up-to-date.

Article 3. Special categories of data

3.1. OLAF staff shall not process special categories of data, except as specified in Article 3.3.

3.2. If such data are unduly captured in OLAF case files, or analyses databases or any other documentation, they shall be deleted as soon as they are detected; any original documents shall be returned to the sender.

3.3. In exceptional circumstances, such data may be processed in accordance with any of the reasons specified in Article 10.2 of Regulation (EU) 2018/1725. The investigation unit shall record any processing in the case management system specifying the justification thereof.

Article 4. Records of processing operations and data protection impact assessment

4.1. The controller shall give prior notice to the DPO of any new data processing operations at OLAF in view of establishing a data protection record in compliance with Article 31 of Regulation (EU) 2018/1725. This shall be done by means of the electronic data protection record register on the OLAF

intranet, and at least 4 months before the controller plans to implement the new processing operation.

4.2. Processing operations shall be subject to risk assessment and those identified as presenting high risks to the rights and freedoms of data subjects, shall be subject to a data protection impact assessment (DPIA) in accordance with Article 39 of Regulation (EU) 2018/1725. The DPO shall be consulted in this context.

4.3. Where following the outcome of the DPIA, the controller considers that the identified high risks cannot be mitigated by reasonable means considering the available technologies and cost of implementation, , the processing shall be submitted to the EDPS for prior consultation, in accordance with Article 40 of Regulation (EU) 2018/1725,. The EDPS may take up to 8 weeks with a possible extension of an additional 6 weeks taking into account the complexity of the intended processing to issue his opinion. Processing may not begin for these processing operations until the EDPS' opinion has been delivered and the Recommendations contained therein have been implemented.

Article 5. Information to the data subject

5.1. The right of all data subjects to receive information in accordance with Articles 15 and 16 of Regulation (EU) 2018/1725 is satisfied by publication of privacy notices on OLAF's website in accordance with Commission Decision (EU) 2018/1962.

5.2. The investigation unit shall provide a personalised privacy notice to relevant data subjects within one month from identifying a person as informant, witness or person concerned via direct contact in writing. If the data of the relevant data subjects is transmitted to another recipient or are used for communication with the data subject earlier than one month, the privacy notice shall be provided to them at the same time For this purpose, the investigation unit shall use the relevant OLAF work forms containing a privacy notice.

5.3. The provision of the privacy notice may exceptionally be restricted in accordance with Article 25 of Regulation (EU) 2018/1725, Article 3 of Commission Decision (EU) 2018/1962, adopted under Article 25 of Regulation (EU) 2018/1725 and Article 10 of the present guidelines concerning restrictions.

5.4. The restriction of the provision of information could be applied, if necessary, after an individual is identified as a person concerned and before the one-month deadline to inform him/her has expired. The restriction and the reason thereof shall be recorded in a note for the signature of the Head of the Unit managing the case. Taking into account the specific circumstances of the case, the investigative unit can submit such restriction to the Director or the Director-General.

Where a member of an institution or EU staff member staff is identified as a person concerned, such restriction shall be recorded at the same time as the decision not to inform the person concerned of his/her possible implication in an open investigation pursuant to Article 9.3 of Regulation (EU, Euratom) 883/2013, for the Director's signature. Taking into account the specific circumstances of the case, such decision not to inform and the restriction of the right to be informed can be submitted to the Director-General.

5.5. OLAF shall ask the competent Member State authority or other competent authorities to inform relevant data subjects that their personal data may be transferred to OLAF for coordination purposes, and suggest that this could be achieved by an appropriate change to their own privacy statement/notice. This shall be done with respect to each competent authority in each coordination case. OLAF shall publish the OLAF privacy notice relating to coordination cases on the OLAF Europa internet site.

5.6. In respect of dismissed cases after a selection and non-relevant data subjects, OLAF shall publish the OLAF privacy notices on the OLAF Europa internet site.

5.7. Where a case is opened in support to an ongoing EPPO investigation, or activities performed at the request of the EPPO, OLAF shall ask the EPPO to inform the data subject that OLAF processes their data at the request of EPPO in accordance with the relevant rules applicable to the EPPO investigation. The privacy notice of support cases shall be published on OLAF internet.

Where the support activity requested involves direct contact with individuals, OLAF will provide the privacy notice at the point of first contact on an individual basis.

5.8. In respect of staff of OLAF's partners in the Member States, OLAF shall ask the competent Member State authority to inform those staff working on OLAF cases that their names may appear in the OLAF case file.

Article 6. Transmission and transfer of personal data outside OLAF

6.1. OLAF may transmit personal data to EU institutions, bodies, offices and agencies (IBOAs) and to Member State authorities, and may transfer personal data to third country authorities, or international organisations, during the course of its activities. In the context of its activities, the Office may also transmit personal data to economic operators subject to Regulation (EU) 2016/679 and may transfer personal data to economic operators located in a third country to obtain information or conduct investigative activities as foreseen by Regulation (EU, Euratom) 883/2013.

6.2. The personal data transmitted and transferred shall be adequate, relevant and limited to what is necessary and proportionate in relation to the purposes for which they are transmitted and transferred and taking into consideration the specific requirements related to the intended recipient.

6.3. Personal data may be transmitted within EU IBOAs only if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient IBOA, which shall be determined on a case-by-case basis. Even if the transmission of information is foreseen in relevant legislation, the transmission of personal data is lawful only if it meets these data protection requirements.

6.4. Personal data may be transmitted to Member State and EEA authorities subject to Regulation (EU) 2016/679[5] only if the data are necessary for the

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–88*.

performance of a task carried out in the public interest or subject to the exercise of public authority, such as the general purpose of combating fraud, which shall be determined on a case-by-case basis for each transmission. Even if the transmission of information is foreseen in relevant legislation, it is lawful only if it meets these data protection requirements.

6.5. Personal data may be transferred to a third country and international organisations in accordance with the relevant provisions of Regulation (EU) 2018/1725 subject to case by case assessment.

- For cases where the recipient's country has an adequate level of protection (Article 47): The list of countries deemed by the Commission to provide an adequate level of protection is available at the website of DG Justice.

- For cases where the recipient's country does not have an adequate level of protection but appropriate safeguards have been implemented in accordance with Article 48: Such safeguards can be implemented via Administrative cooperation arrangements (ACAs) with public authorities containing data protection clauses and authorised by the EDPS following the entry into force of Regulation (EU) 2018/1725. For ACAs adopted under Regulation (EC) 45/2001, the specific data protection clause has to be used in accordance with the provisions of Article 50 of Regulation (EU) 2018/1725.

-For cases where the recipient'country is not covered by an adequacy decision nor by appropriate safeguards: Transfers are possible exceptionally, on the basis of the derogation specified in Article 50 of Regulation (EU) 2018/1725, that the "transfer is necessary for important reasons of public interest or for the establishment, exercise or defense of legal claims," which shall be determined on a case-by-case basis for every transfer.

The provisions of Article 50 should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary.

6.6. The competent unit, whenever making a transmission or transfer, shall perform a case by case assessment taking into consideration the relevant elements listed above and use an OLAF workform containing the appropriate transmission or transfer clause.

6.7. A record of the international transfers of personal data as well as the grounds for transfer and the case-by-case assessment of the transfer shall be maintained by the unit which performed the transfer.

6.8. Personal data shall be transferred securely using appropriate encryption or other secure means of transmission.

Article 7. The rights of access, rectification, restriction, erasure and objection

7.1. Requests from data subjects for access, rectification, restriction and erasure, and objections to the processing of their personal data, shall be forwarded to the Legal Advice Unit as soon as they are received, in view of assessing them in accordance with the present article. The reply to the data subject's request is provided by the competent delegated controller, to be identified in each case in accordance with Article 1.5 of the GDP

7.2. Any such requests received by OLAF staff orally should be recorded in a written note to the file and forwarded to the Legal Advice Unit.

7.3. The Legal Advice Unit shall request the data subject to submit his/her request/objection in writing and to provide proof of identity, when necessary, to confirm the identity of the data subject.

7.4. The Legal Advice Unit shall consult the responsible investigation unit(s) (or any other competent delegated controller) to prepare, on their behalf all replies to such requests/objections. Where appropriate, the Legal Advice Unit may also consult the DPO.

7.5. Where relevant, especially for the purposes of Article 2.3 of Commission Decision (EU) 2018/1962, the Legal advice unit shall consult other relevant parties such as other EU IBOAs and the competent authorities of the Member States.

7.6. Where OLAF is consulted on the application of a restriction by other Commission services or executive agencies pursuant to Article 2.4 of Commission Decision (EU) 2018/1962 or by other EU IBOAs on the basis of their internal rules, any such consultations shall be forwarded to the Legal Advice Unit.

7.7. A data subject requesting access to his/her personal data shall be given access to such personal data, including that provided by a whistleblower or informant. However, he/she may not be provided with the name of the whistleblower or informant, or any information that would allow identification of the whistleblower or informant.

7.8. The delegated controller can decide to implement restrictions on the rights referred to in point 7.1, based on the advice of the Legal Advice Unit. The delegated controller shall follow the procedures foreseen at Article 10.

7.9. The delegated controller shall reply within one month. The deadline can be extended by further two months in duly justified situations.

7.10. In instances where OLAF grants a request to erase, or rectify personal data or restrict their processing, any parties to whom the OLAF has transmitted or transferred the personal data, shall be informed, and where appropriate, they too shall erase or rectify the personal data in question or restrict their processing.

Article 8. Communication of a personal data breach to the data subject and the EDPS

8.1. OLAF staff shall immediately report any suspected security incident involving potential personal data breach using the dedicated secure reporting form and inform their manager.

8.2. When a data breach is identified, the Director General, the representative of the unit responsible for processing the affected personal data, and any other staff member delegated by the Director General, depending on the circumstances of the case, shall liaise with the DPO to assess whether the breach is likely to result in a risk to the rights and freedoms of individual persons, and if so, whether there is high risk to the rights and freedoms of individual persons.

8.3. Any identified risk or high risk shall be notified to the EDPS without undue delay by the staff member designated by the Director General in accordance with Article 34, together with an explanation for any delay in notification beyond 72 hours after the discovery of the breach.

8.4. Where the consultation under paragraph 2 results in the assessment that there is a high risk to the rights and freedoms of individual persons, OLAF shall assess whether any of the provisions of Article 35.3 of Regulation (EU) 2018/1725 apply. Where this is not the case, the respectively competent delegated controller shall assess the applicability of any of the restrictions foreseen by Commission Decision (EU) 2018/1962

8.5. Where no exceptions are identified under paragraph 4 and no restriction is necessary and justified, the data subject shall be informed by the delegated controller in accordance with Article 35 of Regulation (EU) 2018/1725. Any such information shall be provided in any manner, allowing for subsequent review and demonstration of compliance in the relevant case file.

8.6. Where the rights of the data subject foreseen in this Article are restricted in accordance with Article 6 of the Commission Decision (EU) 2018/1962, Article 10 of these rules shall also apply, including the obligation to document any such decision by the delegated controller.

8.7. Where the personal data concerned by a breach in line with paragraph 1 of this Article, have been transmitted by a controller to OLAF, or transmitted to another controller, that controller shall also be informed appropriately, taking the circumstances into account.

8.8. The DPO shall keep a register of all identified data breaches and shall receive relevant information on the handling by the delegated controller.

Article 9. Other data subject requests

9.1. Requests addressed to the controller from data subjects shall be forwarded to the Legal Advice Unit.

9.2. The Legal Advice Unit shall provide a reply to such requests.

9.3. The Legal Advice Unit shall consult the responsible investigation unit(s) and the DPO on all replies to such requests.

9.4. The data subjects can request clarification by the OLAF Data Protection officer.

Article 10. Restriction of data subject rights

10.1. The provision of an individual privacy notice to relevant data subjects and granting other data subject rights may be restricted on a case-by-case basis, for as long as one of the reasons listed in Article 3.3 of the Commission Decision (EU) 2018/1962 applies. The present article only implements the Commission decision (EU) 2018/1962 adopted under Article 25 of the EUDPR. All restrictions of any of the data subject rights shall be recorded in a written note, which will include the applicable restriction and the reason the restriction applies.

10.2. As soon as the reasons for the restriction of the right to be informed no longer apply, the investigation unit shall provide the privacy notice including information on the restriction applied, to the data subject concerned.

10.3. As soon as the reasons for the restrictions of other data subject rights as at Article 7, no longer apply, the controller shall provide the data subject concerned with a reply to his/her request. Where OLAF restricts those data subject rights to protect the rights and freedoms of others in accordance with Article 2.2 of Commission Decision (EU) 2018/1962, notably with reference to names of others or any other information that would allow their identification, the reply will maintain that restriction. . Only when the rights and freedoms of others are manifestly no longer adversely affected, OLAF may assess the need to maintain this restriction.

10.4. The DPO shall be notified without undue delay on the restrictions applied to the rights of the data subject and any supporting documents as specified under Articles 5, 7 and 8 of the present guidelines.

10.5. The Data Protection Officer may request a review of an ongoing restriction of the data subject rights at any time and the investigation unit is obliged to inform the DPO in writing of the outcome of the requested review and document the exchanges.

10.6. During the investigation phase, the investigation unit shall monitor the need to maintain any restriction to the right to be informed at intervals of six months. During the monitoring phase, the investigation unit shall monitor the need to maintain such restriction on an annual basis.

10.7. Due to the nature of the restriction, the obligation to monitor referred to in 10.6 does not apply where OLAF restricts data subject rights to protect the rights and freedoms of others in accordance with Article 2.2 of Commission Decision (EU) 2018/1962, notably with reference to names of others or any other information that would allow their identification. Only when the rights and freedoms of others are manifestly no longer adversely affected, OLAF may assess the need to maintain this restriction.

Article 11. Legality check of data protection compliance

11.1. In accordance with GIP, the Review team will check whether the investigation unit has complied with data protection requirements, by consulting any other relevant documents in the OLAF case file.

11.2. The Review team shall specify, in its opinion on the Final Report, where data protection requirements have not been met.

Article 12. Retention of personal data

12.1. OLAF may only retain personal data in a form, which permits identification of data subjects for as long as necessary for the purposes for which the data were collected or further processed. Relevant legal provisions, including, the Common Commission-level Retention List and the data protection register available online, establish the retention period relevant for each processing operation.

12.2. OLAF shall respect 15 years retention period for personal data collected in the course of OLAF investigations and coordination cases.

12.3. At the conclusion of the retention period, OLAF's Document management Centre shall act in accordance with the post-retention handling as defined by relevant rules and Controller decisions.

12.4. For investigation files, the retention period starts when the decision to close/finalise the case is taken. At the end of the retention period, OLAF's Document Management Centre shall proceed with the transmission of the paper and electronic files to the Historical archives. In cases, where initial information has been dismissed, a selection of specified documents shall be transmitted to the Archives.

12.5. In duly justified situations, and in particular where there are ongoing legal proceedings, the controller can decide exceptionally to extend the duration of the retention period of specific files for additional period. Such decision shall be registered in the file concerned.