

PROTECTION OF YOUR PERSONAL DATA

Privacy statement concerning the implementation and follow-up, by the European Commission's Secretariat-General, of internal investigations conducted by the European Anti-Fraud Office

Table of Contents

- 1. Introduction**
- 2. Why and how do we process your personal data?**
- 3. On what legal ground(s) do we process your personal data?**
- 4. Which personal data do we collect and process?**
- 5. How long do we keep your personal data?**
- 6. How do we protect your personal data?**
- 7. Who has access to your personal data and to whom is it disclosed?**
- 8. What are your rights and how can you exercise them?**
- 9. Contact information**
- 10. Where to find more detailed information**

1. Introduction

The European Commission (hereafter 'the Commission') is committed to protecting your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to [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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

This privacy statement concerns the processing operation 'Implementation and follow-up, by the European Commission's Secretariat-General, of internal investigations conducted by the European Anti-Fraud Office (OLAF)', undertaken by the Secretariat-General, Unit C2 ('Ethics, Good Administration and Relations with the European Ombudsman') (hereafter, the data controller).

Regulation (EU, Euratom) No 883/2013¹ concerning investigations conducted by the European Anti-Fraud Office provides that the European Anti-Fraud Office informs the Commission whenever its staff conduct an investigation on Commission's premises. The European Anti-Fraud Office also informs the Commission whenever such investigations reveal that a Commission staff member, a staff member of an executive agency or a Member of the Commission may be a person concerned. Such investigations are called 'internal investigations'.

Various notifications by the European Anti-Fraud Office to the Commission enable the Commission to:

- take adequate, including precautionary², measures to protect the EU's interests,
- avoid that the Commission opens its own investigation into the same facts, and
- ensure that an appropriate financial, administrative and disciplinary follow-up is given to internal investigations concerning Commission staff conducted by the European Anti-Fraud Office.

As regards the means of notification, the Administrative Arrangements on Cooperation and a Timely Exchange of Information³ specify that the European Anti-Fraud Office addresses such notifications to the Secretary-General of the Commission. The latter forwards the information to the Director-General or Head of Service in the Commission to which the person concerned is assigned as staff member, as well as to the relevant Member of the Commission and, where appropriate, to the Director of the Investigation and Disciplinary Office. In case the person concerned is a Member of the Commission or its Secretary-General, the European Anti-Fraud Office addresses such information to the President of the Commission. This privacy statement and the above-mentioned processing operations are limited to the processing of personal data by the Secretariat-General and the (Cabinet of the) President of the Commission.

2. Why do we process your personal data?

Purpose of the processing operation:

The data controller collects and uses your personal information to:

- ensure that an appropriate follow-up is given, by the Commission, to internal investigations conducted by the European Anti-Fraud Office,
- enable the Commission to adopt precautionary measures where appropriate, and
- avoid that a parallel investigation is opened by the Commission into the same facts.

The administrative investigations covered include investigation of serious facts linked to the performance of professional activities which may constitute:

- a breach of obligations by Commission staff that is likely to lead to disciplinary and, in appropriate cases, criminal proceedings, or

¹ Regulation (EU, Euratom) No 883/2013 of the European Parliament and the Council of 11 September 2013, hereafter referred to as 'Regulation (EU, Euratom) No 883/2013.'

² Measures that are necessary to protect the financial interest of the Union or to avoid that potential evidence could be compromised.

³ Administrative Arrangements on Cooperation and a Timely Exchange of Information between the European Commission and the European Anti-Fraud Office, Ares(2018)6222271, jointly adopted by the Secretary-General of the Commission and the Director-General of the European Anti-Fraud Office on 4 December 2018 pursuant to Article 1(5) of Regulation (EU, Euratom) No 883/2013.

- an analogous breach of obligations by Commission Members.

Internal investigations include investigations which combine internal and external aspects.

The personal data processed under this processing operation may be further processed for the purpose of procedures before the EU Courts, national courts and the European Ombudsman.

Your personal data will not be used for an automated decision-making including profiling.

3. On what legal ground(s) do we process your personal data

The processing of your personal data is lawful, because it is necessary for:

- the performance of a task carried out in the public interest' (Article 5(1)(a) of Regulation (EU) 2018/1725), and
- compliance with a legal obligation to which the controller is subject (Article 5(1)(b) of Regulation (EU) 2018/1725).

The basis for this processing operation is laid down in Regulation (EU, EURATOM) n°883/2013 of the European Parliament and of the Council of 11 September 2013, and the above-mentioned Administrative Arrangements⁴, as follows:

- The processing of information for the purpose of granting access by staff of the European Anti-Fraud Office to Commission premises is based on Article 4(4) of Regulation (EU, Euratom) No 883/2013 and Point 4(1) of the above-mentioned Administrative Arrangements.
- The processing of information obtained in the course of an internal investigation conducted by the European Anti-Fraud Office is based on Article 4(6) of Regulation (EU, Euratom) No 883/2013 and Point 3.1(b) of the above-mentioned Administrative Arrangements.
- The processing of such data (information obtained in the course of an internal investigation) with a view to the adoption of possible precautionary measures by the Commission is based on Articles 4(6) and 7(6) of Regulation (EU, Euratom) No 883/2013 and Points 7.1 – 7.4 of the above-mentioned Administrative Arrangements.
- The processing of personal data contained in reports and recommendations drawn up following internal investigations and any relevant related documents is based on Article 11(4) of Regulation (EU, Euratom) No 883/2013 and Point 14 of the above-mentioned Administrative Arrangements.
- The processing of personal data contained in a transmission of information, by the European Anti-Fraud Office, of the dismissal of a case, when this information is relevant to Commission services for taking appropriate action, is based on Article 5(5) of Regulation (EU, Euratom) No 883/2013 and Point 1.4 of the above-mentioned Administrative Arrangements.
- The processing of personal data contained in transmissions of information from the European Anti-Fraud Office concerning exchanges with the judicial authorities of a Member State relating to an internal investigation, is based on Article 12(2) of Regulation (EU,

⁴ Which refer to Commission Decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF), Official Journal L 136 of 31.5.1999., p. 20.

Euratom) No 883/2013 and Points 12 and 14(3) of the above-mentioned Administrative Arrangements.

This processing operation in individual and limited cases may involve the processing of personal data concerning health (special category under Article 10 of Regulation (EU) 2018/1725) on the basis of Article 10(2)(g) of Regulation (EU) 2018/1725 and personal data related to 'criminal convictions and offences' (Article 11 of Regulation (EU) 2018/1725), as received by the European Anti-Fraud Office. The data controller processes these personal data only to the extent they are necessary for the purpose of ensuring an adequate follow-up to the investigations of the European Anti-Fraud Office.

4. Which personal data do we collect and process?

The European Anti-Fraud Office informs the Secretariat-General of the Commission when it becomes apparent that a Member of the Commission or a staff member of the Commission may be a person concerned in an investigation. In that case, the European Anti-Fraud Office transmits to the Secretary-General the following information:

- the reference number of the internal investigation;
- the nature of the source of information;
- the name, function, personnel number (where applicable), position and function inside the administration (where applicable) of the person(s) concerned;
- a brief description of the case (suspected instances of fraud, corruption or other serious misconduct);
- whether the person concerned has been informed of the investigation;
- suggested precautionary measures;
- any other information that may assist the Commission in deciding whether to take measures to protect its interests.

In addition, the European Anti-Fraud Office may at any time forward to the Secretary-General of the Commission the information obtained in the course of internal investigations, in particular when the elements gathered suggest that the Commission could take appropriate steps to safeguard its interests.

The European Anti-Fraud Office also informs the Secretary-General of the Commission whenever a case is closed with recommendations for financial, administrative or disciplinary follow-up, or closed without further action, and when the European Anti-Fraud Office forwards information to the judicial authorities within the framework of, or following an internal investigation.

Whenever this is necessary in order to safeguard the European Union's interests, the European Anti-Fraud Office may also transmit information to the Commission regarding investigations combining external and internal aspects. Reference thereto is made in Article 7(4) of Regulation (EU, Euratom) No 883/2013. This information may contain personal data of individuals external to the Commission, such as the names of those individuals, their function, and a description of the facts forming the subject of the investigation.

Furthermore, the processing of the names of Commission and European Anti-Fraud Office staff exchanging information regarding investigations communicated by the European Anti-Fraud Office is necessary to ensure a proper and swift follow-up of the transmission of information.

5. How long do we keep your personal data?

In accordance with the Common Commission-level retention list for European Commission files⁵, the data controller located within the Secretariat-General of the Commission may retain your personal data in its files for a maximum period of 15 years after closure of the file of which they form a part.

A file is considered closed after the procedure to which the notification pertains has been finalised and there are no more legal consequences possible or actions to be taken.

6. How do we protect your personal data?

All data in electronic format (e-mails, documents, uploaded batches of data etc.) are stored on the servers of the European Commission; the operations of which abide by [Commission Decision \(EU, Euratom\) 2017/46](#) of 10 January 2017 on the security of communication and information systems in the Commission.

More specifically, a number of technical and organisational measures have been put in place in order to ensure the confidentiality of the data collected, avoid unauthorised access, and preserve the presumption of innocence of the persons concerned and the on-going European Anti-Fraud Office investigation. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed.

Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation, encrypting tools, the marking of documents and the control of access to the electronic and paper documents. The information is communicated on a strict need-to-know basis and addressees are reminded of the security measures to comply with when handling such documents.

7. Who has access to your personal data and to whom is it disclosed?

Personal data processed under this processing operation are only accessible to the Commission staff responsible for carrying out this processing operation and to authorised staff according to the 'need to know' principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The staff responsible for the processing and other authorized staff are Commission Members and Commission staff, typically:

- the hierarchy;
- the President of the Commission and his/her Cabinet Member(s);
- the Commissioner responsible for Human Resources and Security and his/her respective Cabinet Member(s);

⁵ [SEC\(2019\)900](#).

- the Commissioner responsible for the Directorate-General to whom the person concerned pertains and the respective Director-General;
- the Director-General of the Commission's Paymaster's Office where appropriate;
- authorised staff in the Investigation and Disciplinary Office of the Commission where appropriate;

Where necessary, authorised staff in European Union Delegations and Representations or in Executive Agencies may also obtain access to the personal data of the person concerned, if the latter pertains to those entities.

The processing of personal data is without prejudice to the principle of presumption of innocence of the person concerned. Access to personal data is granted to recipients only on a strict need-to-know basis, for the sole purpose of taking any action needed to protect the interests or the security of the Commission.

Your personal data may also be transmitted to the European Anti-Fraud Office, to the European Court of Justice, to the relevant national court(s) and/or to the European Ombudsman to the extent this is necessary for the purpose of giving appropriate follow-up to investigations conducted by the European Anti-Fraud Office.

As regards the treatment of your personal data by the above-mentioned institutions and bodies, including the European Anti-Fraud Office in the framework of its investigative function, please refer to their respective privacy statements.

8. What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access your personal data and to rectify them in case your personal data are inaccurate or incomplete. Under certain conditions, you have the right to restrict the processing of your personal data, to object to the processing and the right to data portability.

You can exercise your rights by contacting the data controller, or in case of conflict the Data Protection Officer and, if necessary, the European Data Protection Supervisor using the contact information given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

Any request for access to personal data will be handled within one month. Any other request mentioned above will be addressed within 15 working days. The period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Please note that the data controller may apply the following statutory exceptions to your rights:

- if the data controller has not obtained your personal data directly from you, pursuant to Article 16(5)(b) and (d) of Regulation (EU) 2018/1725 the data controller does not have to individually inform you of the processing of your personal data, where:

- the provision of such information proves impossible or would involve a disproportionate effort, or is likely to render impossible or seriously impair the achievement of the objectives of the processing, or
 - the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union law;
- pursuant to Article 19(3)(b) of Regulation (EU) 2018/1725, the data controller does not have to erase your personal data, as long as their processing is necessary ‘for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest’.

Where necessary and proportionate, the data controller may, pursuant to Commission Decision (EU) 2018/1962⁶, restrict the application of rights and obligations, laid down in Articles 4, 14 to 20 and 35 of Regulation (EU) 2018/1725. The data controller may do so where the exercise of those rights and obligations would jeopardise the purpose of the European Anti-Fraud Office's investigative activities, pursuant to Article 25(1)(b), (g) or (h) of Regulation 2018/1725.

Pursuant to Article 25(1)(b) and (g) of Regulation 2018/1725, the application of certain rights and obligations under that Regulation may be restricted if necessary in order to safeguard, respectively, the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties. This includes the safeguarding against, and the prevention of, threats to public security; or a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority for important objectives of general interest of the Union.

The European Anti-Fraud Office is required to protect the identity of informants, including whistleblowers, and witnesses, who should not suffer negative repercussions in relation to their cooperation with the Office. Consequently, the application of certain rights and obligations under Regulation (EU) 2018/1725 may also be restricted by data controller pursuant to Article 25(1)(h) of that Regulation in order to safeguard the protection of the rights and freedoms of others.

Article 10 of Regulation (EU, Euratom) No 883/2013 (‘Confidentiality and data protection’) specifies in this respect that information transmitted or obtained in the course of internal investigations, in whatever form, shall be subject to professional secrecy and shall enjoy the protection afforded by the rules applicable to the Union institutions. The institutions, bodies, offices or agencies concerned shall ensure that the confidentiality of the investigations conducted by the European Anti-Fraud Office is respected, together with the legitimate rights of the persons concerned, and, where judicial proceedings have been initiated, that all national rules applicable to such proceedings have been adhered to.

9. Contact information

The data controller:

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the data controller using the following contact information:

⁶ 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 (Official Journal L 315 of 12.12.2018, p. 41).

- Unit SG.C.2 (Ethics, Good Administration and Relations with the European Ombudsman) in the Secretariat-General, on behalf of the Secretariat-General:
 - Phone number + 32 2 2961393 or +32 2 2991111
 - Email: SG-UNITE-C2@ec.europa.eu

The Data Protection Officer (DPO) of the Commission:

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

The European Data Protection Supervisor (EDPS):

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

10. Where to find more detailed information?

The Commission Data Protection Officer publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You can access the register on the following link: <http://ec.europa.eu/dpo-register>.

This specific processing has been included in the public register with the following Record reference: Record DPR-EC-00829 'Implementation and follow-up, by the European Commission's Secretariat-General, of internal investigations conducted by the European Anti-Fraud Office (OLAF)'.

As regards the processing of your personal data by the European Anti-Fraud Office, please find the relevant privacy statements via the following link: https://ec.europa.eu/anti-fraud/olaf-and-you/data-protection/olaf-personal-data-processing-operations-and-privacy-statements_en.
