



EUROPEAN  
COURT  
OF AUDITORS

## Data Protection – Privacy Statement

*Data processing in the event of preliminary assessments, administrative investigations, pre-disciplinary proceedings, disciplinary proceedings, and suspension proceedings*

# Contents

**Introduction**

**Who is responsible for handling your data?**

**Why do we collect your data?**

**What are the rules governing the use of your data?**

**What personal data do we process?**

**How long do we keep your data?**

**Who has access to your data, and to whom will your data be disclosed?**

**How do we safeguard against possible misuse of or unauthorised access to your data?**

**What are your rights?**

**Who should you contact if you have a query or complaint?**

## Introduction

This privacy statement concerns the processing by the European Court of Auditors (ECA) of personal data as part of preliminary assessments, administrative investigations, pre-disciplinary proceedings, disciplinary proceedings, and suspension proceedings.

Persons who might be subject to the processing of personal data are staff members and former staff members: officials in active employment, on secondment, on leave on personal grounds, on non-active status, on leave for military service, on parental or family leave; officials on invalidity and retired officials; temporary staff and former temporary staff; contract staff and former contract staff; national experts; trainees, and persons employed under private law contracts working on ECA premises.

The way the ECA processes and protects your personal data is described below.

Provision of your personal data is **mandatory** according to Article 86 of the Staff Regulations, Annex IX to the Staff Regulations, and Decision No 17-2024 of the European Court of Auditors laying down General Implementing Provisions for conducting administrative investigations and disciplinary proceedings.

## Who is responsible for handling your data?

Data processing operations come under the responsibility of the Secretary-General.

## Why do we collect your data?

The Appointing Authority (the Secretary-General or the Administrative Committee), the Legal Service, and if applicable, the investigator and the Disciplinary Board, will use your personal data to determine whether you have breached your obligations under the Staff Regulations and, if necessary, to issue a disciplinary penalty. For these purposes, they carry out preliminary assessments and administrative enquiries, and initiate pre-disciplinary, disciplinary, and suspension proceedings.

The personal data will not be processed for any purpose other than the one specified here, with the exception that, if a specific case falls within the mandate of the European Anti-Fraud Office (OLAF) and/or the European Public Prosecutor's Office (EPPO) and/or the Court of Justice of the European Union, your personal data will be transferred to and processed by these bodies.

## What are the rules governing the use of your data?

[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 (the **EUDPR**) is the legal framework for processing personal data at the Court.

The legal basis for processing your personal data is Article 86 of the Staff Regulations, Annex IX to the Staff Regulations, and ECA Decision No 17-2024 laying down General Implementing Provisions for conducting administrative investigations and disciplinary proceedings.

Considering that potentially sensitive and/or criminal data might be processed<sup>1</sup>, the legal bases for this processing are:

- Article 10(2)(b) of the EUDPR: “(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”;
- Article 11 of the EUDPR: “(...) processing is authorised by Union law providing for appropriate safeguards for the rights and freedoms of data subjects”. If criminal data are processed, the legal basis is the Staff Regulations and the ECA Decision mentioned above.

Your personal data will also be processed in accordance with ECA [Decision No 11-2024](#) and ECA [Decision No 42-2021](#) adopting internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the European Court of Auditors.

---

<sup>1</sup> Special categories of personal data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation; criminal data will be interpreted broadly in accordance with the case-law of the CJEU. This means that information about staff misconduct might fall into the category of offences, criminal convictions or security measures, and therefore trigger the applicability of Article 11 EUDPR.

## What personal data do we process?

The categories of personal data which can be processed may vary, depending on the specific circumstances of each case. The personal data that are usually processed are: staff number, name, corporate e-mail address and phone number, department or service, time recording data from SYSPER, physical access control data, IT logs, audio recordings of hearings (if the person has consented to a recording), data on recruitment and career, data on missions and travel, data on external activities, data on leave and absences, salary and allowances, and appraisal reports from COMPASS.

In some cases, the personal data processed may include other categories of data, such as data concerning family members, criminal records, bank statements, or medical expenses. This means that potentially sensitive and/or criminal data could be processed, such as health data, and e-mail exchanged with the EU Sickness Insurance Scheme.

Considering that an administrative investigation may concern all aspects of your administrative life and, insofar as it is relevant for the purpose of verifying compliance with the obligations under the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union (CEOS), even your private life, this list is not exhaustive.

## How long do we keep your data?

Your data will be stored in accordance with the time limits that are set by the relevant legal provisions, in particular Decision No 26-2024. The time limits vary, depending both on the file concerned (e.g. a personal or disciplinary file) and on the final result of the administrative investigation and/or disciplinary procedure. Specifically:

- **Pre-inquiry file:** Documents are kept for two years after adoption of the decision that no enquiry will be launched.
- **Personal file:** When a written warning or reprimand is issued, all the related data placed in the official's personal file may be removed and destroyed after three years at the request of the person concerned. For all other disciplinary penalties, the period is six years. However, the data are kept indefinitely in the official's personal file if the disciplinary sanction was removal from post.
- **Disciplinary file:** The disciplinary file is kept for three years after adoption of the decision, if the decision results in a written warning or a reprimand, or no disciplinary penalty is imposed, or no case can be made against the official. The retention period is six years after adoption of the decision if one of the penalties envisaged by Article 9(c) to (h) of Annex IX to the Staff Regulations is imposed. However, the disciplinary files are kept beyond this period if they need to be consulted for the purposes of judicial or administrative proceedings which are still pending after the period has expired.

## Who has access to your data, and to whom will your data be disclosed?

The Secretary-General, acting as the Appointing Authority, and their designated staff, the designated investigator, the Legal Service, and possibly the Disciplinary Board have access to your personal data processed as part of administrative investigations or disciplinary proceedings.

Your personal data may be transferred to other recipients (both internal and external to the ECA) on a need-to-know basis; for example, to staff of the Human Resources Directorate or, if translation is required, to the ECA Language and Editorial Directorate, or, if a question arises with regard to information security or data protection, to the ECA's Information Security Officer and or Data Protection Officer.

Furthermore, your line manager may be informed where necessary for the proper functioning of the service or, at the end of the procedure, for the purpose of assessing your conduct in accordance with Article 43 of the Staff Regulations. If data are shared, your line manager only receives information about the outcome of the investigation, but would not receive any personal data collected during it.

If you lodge a complaint, your personal data will be transferred to the European Ombudsman and/or the European Data Protection Supervisor and/or the ECA Data Protection Officer (DPO).

If the specific case falls within the mandate of the European Anti-Fraud Office (OLAF) and/or the European Public Prosecutor's Office (EPPO), your personal data will be transferred to the competent office(s). Files may also be transferred to the Court of Justice of the European Union in the event of legal proceedings concerning staff members, and/or to the competent national authorities.

## How do we safeguard against possible misuse of or unauthorised access to your data?

Data sets are stored securely in our data centre in Luxembourg, and are therefore covered by the many measures taken to protect the availability, integrity, and confidentiality of the institution's electronic assets. Given the sensitivity of processing activities, the information and personal data processed as part of preliminary assessments, administrative investigations, pre-disciplinary proceedings, disciplinary proceedings, and suspension proceedings are protected using encryption, and other appropriate tools used at the ECA to handle sensitive data/information (such as ZoneCentral), and encrypted email.

Furthermore, for each case, those handling administrative investigations and disciplinary measures will carry out a case-by-case assessment and limit the collection of personal information to what is strictly relevant and necessary for the purpose of their enquiry or disciplinary proceeding.

Further processing/sharing of cases with OLAF/EPPO/CJEU occur using ECAfiles, with documents being encrypted and password-protected.

Access to personal data is restricted to a specific user group. Access rights are granted on a “need-to-know” basis, taking account of the role, post and responsibilities of the user concerned.

## What are your rights?

Your personal data rights are set out in Articles 17 to 24 of Regulation (EU) 2018/1725. Those rights may be restricted in accordance with Article 2(1)(b) of ECA [Decision No 42-2021](#). This [document](#) contains further details about your rights. In short:

- You have the right to access your personal data, or have them rectified without undue delay if they are inaccurate or incomplete, and to withdraw your consent at any time.
- Subject to certain conditions, you have the right to ask us to erase your personal data or restrict their use. Where applicable, you have the right to object at any time to your personal data being processed, on grounds relating to your specific situation, and the right to data portability.
- Where the processing of your personal data is based on your consent, you may withdraw that consent at any time, following which your personal data will be irrevocably removed from our records without undue delay and you will be informed thereof, unless such deletion is prevented by a legal/contractual obligation.
- We will consider your request, take a decision, and notify you of the outcome without undue delay, within one month of receiving your request. This period may be extended by two further months where necessary.
- You are not subject to automated decisions (i.e. made solely by machines), including profiling.
- You can exercise your rights by contacting the data controller, using the contact information provided below.

## Who should you contact if you have a query or complaint?

The first point of contact is the data controller. Therefore, please write to the Secretary-General or the President.

You may contact the ECA's Data Protection Officer ([ECA-Data-Protection@eca.europa.eu](mailto:ECA-Data-Protection@eca.europa.eu)) at any time if you have any concerns/complaints about the processing of your personal data:

Data Protection Officer
European Court of Auditors 12, rue Alcide de Gasperi 1615 Luxembourg LUXEMBOURG

You may lodge a complaint, at any time, with the European Data Protection Supervisor ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) about the processing of your personal data.