



EUROPEAN
COURT
OF AUDITORS

Data protection statement

The processing of visitors' personal data at the European Court of Auditors

This data protection statement concerns the processing of visitors' personal data at the European Court of Auditors (ECA).

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

Your host provides your personal data using a specific form on the ECA's internal ticketing system to request authorisation for you to access the ECA's premises.

When you arrive, you must be able to present a valid identity document (ID card, passport, residence card) so that the ECA can check your identity and allow you to enter the premises.

On-site checks may be carried out to comply with internal safety rules.

Who is responsible for handling your data?

Data processing operations fall under the responsibility of the ECA's Security and Safety Service (SSS).

Why do we collect your data?

The SSS will process your personal data to plan your arrival, facilitate the access procedure (for example, carry out ID checks and security checks), monitor and keep track of visitors at all times.

The SSS may also contact you, or produce statements and reports including your personal data in the event of an incident. Examples of an incident include suspicious behaviour, lost and found items, thefts, badge incidents, accidents, and damage to property or persons.

What rules govern 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 EU institutions, bodies, offices and agencies and on the free movement of such data (the “EUDPR”) is the legal framework for processing personal data within the ECA.

The legal basis for processing your personal data is:

- Article 5.1(a) of the EUDPR: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the ECA, namely, the management of the internal security of the ECA; and
- Article 5.1(b) of the EUDPR: processing is necessary for compliance with a legal obligation laid down in Article 1(e)(2) [Staff Regulations](#), Staff Notice 02/2007 (K1) – Control of access to building K1, and Staff Notice 036/2007 – Control of access to building K1 lifts and staircases.
- Article 5.1(d) of the EUDPR: the data subject consents to the processing of his or her personal data for one or more specific purposes. You provide consent either when your ECA host fills out a visitor’s form on your behalf, or when you complete the form (or provide your data to the security guard) at the entrance to the ECA.

What personal data do we process?

We process the following categories of personal data:

- data relating to your identity (name, nationality, address, date of birth, ID number and the expiry date of your identity document);
- email address;
- visitor badge identification number;
- information on access to ECA premises (date and times of entry and exit, private or professional visit, parking requests, disability or access requests, etc.);
- the name of your ECA host;
- any particular needs (for example, assistance for a disability, parking, access to specific rooms or areas);
- video surveillance footage that may feature you (please refer to our [video surveillance policy](#));
- in the event of an incident, written statements and reports that may include your personal data;
- vehicle information (if we allocate you a parking space), including brand of car, model, colour and numberplate; and

- for groups of visitors, the name of your organisation (for example, the company or the service provider).

How long do we keep your data?

Your personal data is retained in the visitors' register for 13 months.

The visitor forms filled in by your host at the ECA and transferred to the SSS's calendar are also retained for 13 months.

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

Your personal data will be processed by the SSS on a need-to-know basis.

For an official or group visit or event, the Events, Visits and Protocol Service (EVP) may also process your personal data to organise the events they manage effectively. Please refer to the EVP team's specific privacy statement, which applies in addition to this privacy statement.

SOCOM (the external maintainer and service provider responsible for technical support, maintenance and system development) has technical access to the ECA's badging system. SOCOM only has access to the database to carry out system maintenance and any access is strictly in accordance with standard security measures (for example, access on a need-to-know basis, confidentiality requirements and other safeguards).

The ECA's ticketing system is built on the ServiceNow platform. Internal administrators in the Directorate for Information, Workplace and Innovation (DIWI) have limited access to the platform for technical, maintenance and development purposes only. While this may allow them to see tickets and their content, they do not access or process the personal data in the tickets unless it is strictly necessary for the system to function properly.

If the processing activity is audited by the ECA's Internal Audit Service (IAS) at a later stage, please note that your personal data will only be shared with the IAS if necessary to fulfil the obligations of the IAS and in full compliance with the principle of necessity and proportionality.

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

Local police may be given access to your data if they need to investigate or prosecute criminal offences. Under exceptional circumstances, access may also be granted to the European Anti-Fraud Office (OLAF) in the framework of an investigation carried out by OLAF, or to investigators carrying out a formal internal investigation or a disciplinary procedure within the ECA, provided that it can be reasonably expected that such transfers of data may help the investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence. No requests for data mining are accommodated.

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

Data sets are stored securely in the ECA's data centre in Luxembourg and are therefore covered by the numerous measures taken to protect the availability, integrity and confidentiality of our electronic assets.

We use ServiceNow Inc. to process and manage the visitor access request form and allow visitors to enter the ECA's premises. Appropriate data processing terms exist between the ECA, as data controller, and the data processor. These guarantee the adequate protection of the personal data that is processed. ServiceNow is certified ISO27001.

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 person concerned. These rights are continually updated as staff assignments change.

The ECA's Secretary-General has overall responsibility for implementing the rules on access rights and compliance with the rules on data protection, and has delegated responsibility in these areas to different internal entities.

The ECA has an information security policy and an Information Security Officer (ISO) who ensures that the policy is implemented correctly and that any related checks are tested for efficiency.

What are your rights?

Your rights regarding your personal data are set out in Articles 17 to 24 of Regulation (EU) 2018/1725. Further details about your rights are included in this [document](#).

- You have the right to access your personal data, and to have it rectified without undue delay if it is inaccurate or incomplete.

- You have the right to ask us to delete your personal data or to restrict its use under certain conditions. Where applicable, you have the right to object to the processing of your personal data at any time, on grounds relating to your particular circumstances, 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 duly informed, unless deletion is prevented by a legal or contractual obligation.

- When you visit the ECA, you will not be subject to any decision based solely on automated processing, including profiling.

You can exercise your rights by contacting the data controller using the contact information below.

We will consider your request, take a decision, and notify you of it without undue delay, no more than one month after we have received your request. This period may be extended by two further months if necessary.

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

Your first point of contact is the data controller: ECA-security@eca.europa.eu.

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

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

You have the right to lodge a complaint with the European Data Protection Supervisor (edps@edps.europa.eu) at any time concerning the processing of your personal data.