

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF
PROCESSING PERSONAL DATA RELATED TO *EX POST* CONTROL ACTIVITY OF THE EEAS
VIA E-EPC

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS), including the Delegations of the European Union. You have the right under EU law to be informed when your personal data is processed [e.g. collected, used, stored] as well as about the purpose and details of that processing.

When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular Article 8 on data protection. Your personal data are processed in accordance with Regulation (EU) 2018/1725 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, aligned with Regulation (EU) 2016/679, the General Data Protection Regulation. In this privacy statement you find information about how the EEAS and EU Delegations process your personal data and what rights you have as a data subject.

2. PURPOSE OF DATA PROCESSING: Why do we process your data?

The purpose of the present processing activity is to ensure *ex post* controls over the financial transactions of the EEAS in accordance with Article 74(6) of Regulation (EU, Euratom) 2024/2509 ("the Financial Regulation"). This work is supporting the EEAS's Annual Activity Report and the Declaration of Assurance as required under Article 74(9) of the Financial Regulation.

Through its *ex post* controls, the EEAS has a yearly assessment of the level of legality and regularity of the transactions linked to the execution of the EEAS budget and establishes the financial and reputational errors which feed into the Declaration of Assurance. *Ex post* controls is performed on a number of transaction which are sampled over the budget year linked to the expenditure and revenue. Information about the analysis of the financial transactions are entered in the dedicated IT tool Electronic Ex-Post Control System (e-EPC).

In the course of their work, *ex post* controllers may be required to process personal data concerning the staff and their dependants or of contractors and other stakeholders with which the controlee has a relationship.

The data relating to natural persons and legal entities collected and controlled are any relevant data that may be requested by the EEAS with a view to verifying that the financial transactions relating to the execution of the administrative budget are justified. Such information should not be disclosed to the public without the permission of the natural person or legal entity concerned.

The processing operations are intended to allow for the identification, analysis, evaluation and recording of the information required to perform *ex post* controls and procedures. These serve as the basis for the findings and recommendations communicated to achieve the overall objectives of the *ex post* controls.

The processed personal data will be stored in IT systems which are accessible only to users within the EEAS.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed for that purpose are the following:

All necessary data to efficiently conduct a control relating to EEAS staff and external contractors to the EEAS and other stakeholders, in particular:

Data related to natural persons, mainly EEAS Staff:

- name
- function and position
- statutory link
- organisational entity
- grade
- activities
- salary and other reimbursements received, including deductions from these amounts
- email addresses
- information coming from EEAS, EC and local IT systems used to justify costs as eligible (e.g. family composition), mission declarations, supporting documents linked to travel costs, information concerning the dependents of the EEAS staff;

Data related to contact persons and other individuals linked to legal entities concerned by the financial transactions controlled:

- name
- professional address
- personal data in bank account details

- invoices with details of costs for services
- works and supplies - and other similar data depending of the nature of the financial transaction and the subject matter of the activity.

In the course of its activities, the *ex post* control of the EEAS may process special categories of personal data, pursuant to Article 10 of Regulation (EU) 2018/1725, or personal data related to criminal convictions and offences, pursuant to Article 11 of Regulation (EU) 2018/1725, only if necessary for the analysis of the sampled transaction. As such, the *ex post* control may process, for example, data required prior to recruitment such as data concerning health or criminal record.

Original documents

- Digital copies of original documents are supplied to justify financial transactions relating to the execution of the EU budget.
- Declarations of Assurance by Heads of Delegations are entered into a dedicated IT tool (with limited access).

4. DATA CONTROLLER: Who is entrusted with processing your data?

The data controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Division entrusted with managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

EEAS.GII.GOV.2 – Internal Audit

5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?

Personal data are processed by the EEAS *Ex post* controllers team (EEAS.GII.GOV.2).

Personal data may be shared, according to the "need to know" principle with

- the Head of service being controlled and persons appointed by the Head of service of the controlee as contact persons
- the data subject for validation purposes.
- other assigned EEAS staff to provide information related to the transactions controlled.

Ex post reports are shared with

- the entities controlled
- the Chief Governance Officer (EEAS.GII.GOV)
- the Director General for Resource Management (EEAS.DG.RM)
- the responsible Directors in EEAS.DG.RM,
- Head of Division in charge of Planning, Reporting and Compliance (GII.GOV.3)
- the Heads of the Division in charge of policy affected by the errors.

Transmission is possible to the bodies in charge of a monitoring or inspection task in accordance with Union law (OLAF, the European Court of Auditors, the European Ombudsman, EDPS, EPPO, IDOC and the Internal Audit Service (IAS) of the European Commission).

Transmission of *ex post* reports by the Head of the entities controlled within her or his own service or its line managers and superiors is decided by the controlee. Personal data is not intended to be transferred to a third country or an international organisation, except where necessary for providing access to recipients as described above.

The only circumstances under which information arising from *Ex post* Controls could be transferred to authorities in third countries would be concerning a suspected fraud or financial irregularity or legal dispute concerning the fulfilment of contractual obligations. This would be managed by OLAF in the case of suspected fraud and irregularities and where appropriate by the EEAS Legal Department. The legal basis of this transfer is the important public interest of protection the finances and regular operations of the EEAS and of EU Delegations (Article 50 (d) of Regulation (EU) 2018/1725 and to establish, exercise or defend legal claims arising from the established irregularities or infringements (Article 50 (e) of Regulation (EU) 2018/1725).

The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

6. ACCESS, RECTIFICATION AND ERASURE OF DATA: What rights do you have?

You have the right of access to your personal data and the right to correct your inaccurate or incomplete personal data, taking into account the purpose of the processing. The right of rectification can only apply to factual data processed. Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. For more detailed legal references, you can find information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. If you wish to exercise your rights or have questions concerning the processing of your personal data, you may address them to the Data Controller via the functional mailbox:

EPC@eeas.europa.eu

7. LEGAL BASIS: On what grounds do we collect your data?

Lawfulness:

The processing of your personal data in the context of *ex post* controls is necessary for the performance of a task carried out by the EEAS in the public interest, in particular for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 1725/2018 as referred to in Recital 22 thereof].

The processing of your personal data is also necessary for compliance with the obligation as required by the Financial Regulation applicable to the General Budget of the Union (Article 74), and the Internal Rules (Article 37) [Article 5(1)(b) of Regulation (EU) 2018/1725].

Legal references:

- [Regulation \(EU, Euratom\) 2024/2509 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union \(recast\)](#)
 - Article 74(6): The authorising officer by delegation may put in place *ex post* controls to detect and correct errors and irregularities of operations after they have been authorised. Such controls may be organised on a sample basis according to risk and shall take account of the results of prior controls as well as cost-effectiveness and performance considerations.
The *ex post* controls shall be carried out by staff other than those responsible for the *ex ante* controls. The staff responsible for the *ex post* controls shall not be subordinate to the members of staff responsible for the *ex ante* controls.
- [Internal Rules on the implementation of the general budget of the European External Action Service \(ADMIN\(2018\)37 of 21/12/2019\)](#)
 - Article 37(4): *Ex post* controls may be carried out on the basis of documents and, where appropriate, on the spot. The outcomes of *ex post* controls shall be reviewed by the authorising officer by delegation at least annually to identify any potential systemic issues. The authorising officer by delegation shall take measures to address those issues.
- Further legal reference:
[Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS \(2010/427/EU\)](#) – OJ L 201, 3/8/2010, p. 30, in particular Article 4.3(b).

8. TIME LIMIT & DATA SECURITY: for what period and how securely do we process your data?

Storage period

Personal data such as data in control working papers is kept for a maximum period of 10 years after the budgetary authority gives discharge for the year of the control report. *Ex post* control reports are kept for information and historical, statistical or scientific purposes for an indefinite period of time. *Ex post* control results are considered to be a 'document of administrative value' as defined in Article 1 of Council Regulation 1700/2003 setting out the categories of documents which would be placed in the historical archives of the European Union.

- Archiving shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of individuals. Reports and other material containing personal data are archived according to e-Domec policy.
- In case of an incident, event or inquiry by authorities, data subjects or other concerned individuals' personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. In any case, personal data will not be kept longer than 5 years after the judgment on the pending case is final.
- When appropriate, personal data contained in supporting documents should be deleted where possible, if that data is not necessary for audit, inspection or other control purposes.

Security of data

Appropriate organisational and technical measures are ensured according to Article 33 of Regulation (EU) 2018/1725. The collected personal data are stored on servers that abide by pertinent security rules. Data is processed by assigned staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. General access to personal data is only possible to recipients with a UserID/Password. Physical copies of personal data are stored in a properly secured manner.

All *ex post* controllers have received appropriate instructions on the processing of personal data in the course of *ex post* controls and on the ethical use of the information made available to them. Whenever possible, they have been instructed to refrain from processing personal data for their *ex post* controls and procedures, by using 'desensitised' data instead, i.e. removing the information that enables linking the data with individual persons.

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

If you have enquiries you can also contact the EEAS Data Protection Officer at data-protection@eeas.europa.eu.

10. RECOURSE

You have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.