EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO THE EEAS INTERNAL AUDIT DIVISION ACTIVITIES (HQ AND EU DELEGATIONS)

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 internal audit activities of the EEAS in accordance with articles 117 to 123 of Regulation 2018/1046 ("the Financial Regulation"), as well as article 3(4) and 4(3b) of Council Decision 2010/427/EU establishing the EEAS and the IAD Mission Charter (Ref. Ares(2023)177384 – 11/01/2023.). This work is supporting the EEAS' Annual Activity Report and the Declaration of Assurance as required under article 74(9) of the Financial Regulation 2018/1046.

The relevant part of the mission of the Internal Audit Division is to provide independent, objective assurance and consulting activity designed to add value and improve the operations of the EEAS. The Internal Audit Division helps the EEAS accomplish its objectives by bringing a systematic, disciplined approach in order to evaluate and improve the effectiveness of risk management, control, and governance processes.

The Internal Audit Division has unrestricted access to people, systems, documents and property within the EEAS it considers necessary for the proper fulfilment of its responsibilities. In accordance with the Internal Audit Mission Charter, all staff members are required to provide the information requested or cooperate otherwise to allow the auditors to carry out their work.

Auditors have the obligation to signal any findings to the EEAS senior management, including observations related to working relations and administrative management, spotted during the audit that might impact the proper functioning of the entity audited.

In the course of their work, internal auditors may be required to process personal data concerning the staff of the audited service or of contractors and other stakeholders with which the auditee has a relationship. Personal data may be obtained during our audit activities from documents we analyse in the course of our engagements (minutes of meetings, transactions in information systems, operational instructions given by or on behalf of the auditee / controlee or other types of data specific to the engagement, etc.) or from interviews.

The processing of such data will not constitute the major aim of the engagement, as the internal audit activities do not aim at investigating/inquiring particular individuals and/or conduct. In addition, the processing of the data falls within the reasonable expectations of data subjects, based on their relationship with the EEAS Internal Audit (a candidate participating in a recruitment procedure in the EEAS including the EU Delegations can expect that an internal audit on the recruitment process may involve the processing of his or her personal data). Furthermore, the risks to the fundamental rights and freedoms of data subjects, related to the processing of special categories personal data do not relate to the internal audit process, but to the activities for which they were initially collected (personal data available in recruitment files may be accessed by the internal audit, but the internal audit has no influence over the purpose and means of the initial processing).

The processing operations are intended to allow for the identification, analysis, evaluation and recording of the information required to perform audit tests and procedures. These serve as the basis for the observations and recommendations communicated to achieve the overall objectives of the Internal Audit process.

The processed personal data will be stored in audit working papers which will not be communicated to recipients outside the EU institutions.

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 audit tests relating to EEAS staff, 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:

- names
- professional address
- personal data in bank account details
- invoices with details of costs for services works and supplies
- other similar data depending of the nature of the financial transaction and the subject matter of the activity.

In the course of its audit activities, the Internal Audit 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 a task carried out in the public interest and to comply with the legal obligations to which the Internal Audit is subject under Regulation (EU, Euratom) 2018/1046. As such, the Internal Audit may process, for example, data required prior to recruitment such as data concerning health or criminal record in the context of an audit on recruitment by the EEAS, including for the EU Delegations.

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.SG.GOV.2 – Internal Audit

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

Personal data are processed by the EEAS Internal Audit team (EEAS.SG.GOV.2).

They may be shared according to the "need to know" principle with

- the Heads of the audited services and persons appointed by the Heads of audited services as contact persons
- the data subject for validation purposes
- other assigned EEAS staff to provide information related to the transactions controlled.

Recipients of the Audit reports, that usually do not contain personal data, aside from the names and positions of the recipients and the auditors, are

- the entities audited
- the Secretary General
- the Chief Governance Officer (EEAS.SG.GOV)
- the Director General for Resource Management (EEAS.DG.RM)
- the Managing Director and the Director of the audited services
- the Audit Progress Committee
- the Internal Audit Service of the European Commission
- the European Court of Auditors.

Transmission of audit reports by the Heads of audited services within her or his own service or its line managers and superiors is decided by the audited service itself.

Work papers documenting the audit work performed and supporting the audit conclusions may include personal data, particularly in checks of samples of transactions. Work papers are kept in the Internal Audit Division, and are in general not shared outside the Division.

These processes are without prejudice to a possible transmission of audit documents 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) and to bodies in charge of detection, investigation and prosecution of criminal offences in accordance with EU and Member State law.).

Personal data is not intended to be transferred to a third country or an international organisation.

The only circumstances under which information arising from audits 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 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?

As „data subject", 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:

INTERNAL-AUDIT@eeas.europa.eu

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

Lawfulness

The processing of your personal data in the context of internal audit activities 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) 2018/1725] 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 (Art. 74), and Article 5(1)(b) of Regulation (EU) 2018/1725.

Legal references

- Council Decision EEAS (2010/427/EU) of 26 July 2010 establishing the organisation and functioning of the European External Action Service, and in particular Art. 4.3(b)
- Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, articles 118 to 123:
  - Art. 118(1): The internal auditor shall advise his or her Union institution on dealing with risks, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management.
  The internal auditor shall in particular be responsible for:
  (a) assessing the suitability and effectiveness of internal management systems and the performance of departments in implementing policies, programmes and actions by reference to the risks associated with them;
  (b) assessing the efficiency and effectiveness of the internal control and audit systems applicable to each budget implementation operation.
  - Art. 118(2): The internal auditor shall perform his or her duties in relation to all the activities and departments of the Union institution concerned. He or she shall enjoy full and unlimited access to all information required to perform his or her duties, if necessary also on-the-spot access, including in Member States and in third countries.
- EEAS Internal Audit Charter – ref. Ares(2023)177834 - 11/1/2023

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

8. TIME LIMIT FOR DATA STORED & SECURITY MEASURES: For what period and how we process your data?

Storage period

Personal data such as data in audit working papers supporting the audit reports is kept for a maximum period of 10 years, in application by analogy of the 'Common Commission-level retention list for European Commission files – second revision' (Ref. Ares(2021)6574237 – 25/10/2021), section 12.9. Audit reports are kept for information and historical, statistical or scientific purposes for an indefinite period of time. Audit reports 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 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, documents containing sensitive personal data should be deleted where possible, if that data is not necessary for audit purposes.

Security of data

Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (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.

The internal audit team of the Internal Audit Division have received appropriate instructions on the processing of personal data in the course of internal audits and on the ethical use of the information made available to them. Furthermore, they are expected to respect the Code of Ethics of the Institute of Internal Auditors and abide by the applicable professional standards. In particular and whenever possible, they have been instructed to refrain from processing personal data for their audit tests 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.