EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO THE "HIVE" COLLABORATIVE PLATFORM OF THE EEAS BASED ON OPENTEXT

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 The EEAS Information Management Strategy approved by the EEAS Secretary-General (Ref. ARES(2019)755822), identified several key objectives, namely: a strong culture of collaboration, the right information accessible to the right staff, preserving and securing information and knowledge, implement a wide-governance, commitment to information management and effective training and support. The roll-out of a collaborative platform constitutes a success-factor of such a strategy.

Description

- Set-up of a collaborative platform with document management capabilities to collaborate on, manage and share documents and discuss and share political information among their communities of interest.
- Need to adopt a solution that offers an "on premises" option due to the security constraints as indicated by the ICT Steering Committee.

3. DATA PROCESSED: What data do we process?

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

- Name, professional email address, professional phone, nationality.

*Content uploaded containing personal data is governed by the original processing operation under which the personal data in the document content were collected and are processed.

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 Division entrusted with managing the personal data processing under the supervision of the Head of Division is the following organisational entity

RM.SCS.1 – Information and Document Management

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

- Users of the system according to the access rights of each workgroup
- EEAS Technical staff
- Staff of the processor providing the software and support to the system with no access to the EEAS instances of the system

Recipients of the documents are defined according to the original processing acitivity under which the personal data in the document content were collected and are processed. Personal data in the dedicated collaboration spaces may be accessed by NATO, the United Nations, UN agencies and field offices as well as certain intergovernmental organisations including OECD, OSCE, INTERPOL, CARICOM and specific regional and continental bodies, such as the African Union, i.e. organisations with whom the EU cooperates based on common values and objectives. These international and intergovernmental organisations follow their own privacy policies. They may have access to dedicated spaces for cooperation with these international and intergovernmental organisations. Specifically, their access is limited to the identity of EEAS and Member States staff who are their interlocutors and to documents to which they have the right of access governed by the cooperation action or project under which the users are their interlocutors and the documents are shared, i.e. their access to the platform does not imply additional access and is justified under the original cooperation action or project.

Thus, their access to the HIVE system is necessary for an important reason of public interest, namely the enhancement of international cooperation of the European Union (Article 50 (1)(d) 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:

information-management@eeas.europa.eu

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

Lawfulness

- The processing of your personal data is necessary for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof.
- Processing of personal data in the content of the uploaded documents/files is necessary according to the legal bases of the original processing activity under which the personal data in the document content were collected and are processed.

Legal references

RECORDS management regulation (COUNCIL REGULATION No 354/83).

Decision of the Secretary General of the European External Action Service of 01/12/2022 on the EEAS records management and archives policy, ADMIN(2022) 61.

Regulation (EU) 1049/2001 on public access to documents.

Decision of the Secretary-General of the EEAS on the information sharing policy of the European External Action Service - ADMIN(2023) 32

Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS (2010/427/EU), OJ L201, 3/8/2010, p. 30.

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

Storage period

Personal data in access management and control data shall be retained for as long as the user is in the 'Active Directory' and has a HIVE account, active or inactive. The designation of a user as author of documents and the civility, department, city of service and office e-mail address of the author will be retained as long as other metadata of the document are retained (see below).

Personal data in document content shall be kept throughout the retention period, as defined in the common retention list, of the file in which the de facto controller has filed the document.

Personal data in mandatory metadata in relation to any document namely metadata about the author and addressee of a given document (typically name and surname of the respective individuals and the department/body to which they belong), metadata about the title or subject of a given document, metadata about the attachments (brief description) and metadata in relation to the title of the file in which it is filed shall be retained as long as the document is available. Documents stay in the recycle bin for 6 months after deletion.

Personal data in audit trail and workflow data shall be retained o ensure that the authors and participants in major records management actions at the level of metadata, documents, files or procedures can be identified.

Personal data may be kept for information and historical, statistical or scientific purposes for a longer period of time including the publication on the EEAS/EU Delegation website and on the EEAS Intranet with appropriate safeguards in place. 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 the EEAS records management and archives policy (Ref. Ares(2022)8313874), in its Art. 13, in addition to REGULATION (EU) 2018/1725, Art. 4 and 13.

In case of an incident, event, investigation or inquiry by authorities or by EEAS and EU institution services charged with a monitoring, inspection, control or audit task, 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, if longer than the usual storage period above, personal data will not be kept longer than 5 years after the judgment on the pending case is final.

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 collaborative platform is compliant with the Information Systems Security Requirements of the EEAS. Access rights will be set up on a need-to-know basis, according to the Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the security rules for the European External Action Service - ADMIN(2023) 18 and in line with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission C/2016/8998. Data is stored on premises secured by EEAS and DG Digit infrastructure; cloud use is not permitted.

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.