

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO AI-GENERATED BRIEFINGS VIA THE EEAS AI BRIEFING TOOL

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?

Purpose(s)

The purpose of this processing operation is to provide accurate information on topics relating to EU Foreign Affairs and the state of play of EU policies to the EEAS hierarchy (Corporate Board and HR/VP) as well as both Presidents (EU Council and EU Commission) and Commissioners via the EEAS AI Briefing tool.

Description

The EEAS department, division or delegation responsible for producing AI-augmented briefings draws its information from two main data sources: curated repositories in HIVE and previous briefings stored in the e-Brief application. The AI briefing tool generates a first draft by reformulating existing text prepared by the desk officers. These briefings are circulated up the hierarchy in advance of a specific meeting or decision-making process. Once finalised, they are uploaded to and retained in either e-Brief.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed for the following data subjects:

A. Public figures related to external relations issues that may appear in the briefing material

The personal data, including CVs collected, are all data deemed relevant to understand the public action of a public figure concerned.

The data are collected from various sources, including public sources. A limited number of data might be received directly from the public figures concerned or their representatives.

B. Assigned staff participating in the briefing process within the various departments of EEAS (including officials, temporary agents, contract agents, SNEs and other relevant staff members)

The data are the name(s) and surname(s), function, professional contact details. The data are also covered by the Notification on the Use of Basic Personal Data for Professional Purposes and its Privacy Statement.

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 Information and Document Division (RM.SCS.1)

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

The recipients of your data may be

- The EEAS hierarchy/Corporate Board (at HQ and/or in Delegations), the HR/VP, both Presidents and Commissioners in preparation of a particular meeting or decision making.
- The staff of the department/division/Delegation concerned and of its counterpart at HQ / in Delegations.

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. In case of international transfers appropriate safeguards are ensured in accordance with Chapter V 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:

ai-tools@eeas.europa.eu

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

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

Legal references: Article 27.3/TEU

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?

Documents produced using the EEAS-specific IT application for creating AI-augmented briefings can be downloaded for up to 72 hours. After this time, they are automatically deleted, even if they have not been downloaded. Users may also choose the 'delete' option, which erases the text instantly. No data is shared with third parties.

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.

Specific security measures : Access to the tool is provided via the EEAS Connect authentication system.

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.