EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO LESSONS AND GOOD PRACTICES FROM THE AREA OF CONFLICT PREVENTION AND CRISIS RESPONSE (CPCR) USING THE CPCR LESSONS DATABASE BY THE EEAS (HQ AND/OR 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?

Purpose:
The purpose of the present processing activity is to ensure collection, storing and dissemination of lessons and good practices from the area of Conflict Prevention and Crisis Response.

Description:
Personal data stored within the system relates to access rights management. The access to the system will be managed first via EULogin application, with the administrator granting specific individual rights to view or edit the content.

3. DATA PROCESSED: What data do we process?

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

- Name
- E-mail address
- Access rights

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:

ISP.1.SEC1 - Methodology of Integrated Approach

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

The recipients of your data may be

- Assigned staff of
  - EEAS RM.BS.3, Digital Solutions Division – project development team
  - EEAS organisational entities dealing with missions (mainly Civilian Planning and Conduct Capability, the Security and Defence Policy Directorate, EU Military Staff, Military Planning and Conduct Capability and the Integrated Approach for Security and Peace Directorate)
  - European Commission (mainly the Directorate General of Foreign Policy Instrument).
  - CSDP missions and operations
- Member States representatives

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

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:

ISP-1@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 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.

Conflict Prevention and Crisis Response is within the mandate of the EEAS.

The database enables EEAS staff to exchange lessons/good practices and inform management about them and to improve the operations of the EEAS.

Legal reference:
Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service OJ L 201, 3.8.2010, p. 30.

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

Storage period
User data are stored as long as the user is active in the system. Data of users inactive for more than two years are removed unless they need access due to their job function. The lessons under the removed person (Author) will be moved under 'Anonymous' user. Data are only kept longer, until the expiry of legal claims, if necessary for investigations or if legal proceedings are in progress.

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: CMP is hosted by DIGIT, which ensures that security updates are applied on a regular basis. The TTSO office in the Digital Solutions division BA.BS.3 produces Security Vulnerability reports for all EEAS applications on a regular basis, and the domain teams address all of the findings. Only authorised individuals have access to the data. EU LOGIN authentication is required to access the database.

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.