EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO EEAS BUSINESS CONTINUITY BY THE EEAS (HEADQUARTERS 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 Union Delegations. You have the right under EU law to be informed when your personal data is processed 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 business continuity (BC) in Headquarters and Union Delegations in case of unforeseen disruptions of service by establishing the appropriate plans and procedures in order to maintain critical and essential functions. This includes the collection and storage of personal data that enable the EEAS to identify and contact EEAS staff members where necessary to allow exercising duty of care.

3. DATA PROCESSED: What data do we process?

The following categories of personal data may be processed in the context of business continuity:
In Headquarters (HQ):

- Name and surname
- Function
- Professional contact details (phone number, office number)
- Private contact details (phone number, address)
- If required, additional details for the specific emergency situation
  - Data in BC documents
  - Staff members may be asked to self-identity in case of vulnerability (medical condition yes or no – but no actual processing of medical details in the course of BCP processing activities) in order to allow the employer to exercise duty of care

In Delegations:

- Name and surname
- Function
- Professional contact details (phone number, office number)
- Private contact details (phone number, address)
- Nationality
- Family situation
- If required, additional details for the specific emergency situation
  - Location data
  - Data in BC documents and in EEAS Security IT application for Delegations (ESDAP / EEAS Security Portal)
  - Staff members may be asked to self-identity in case of vulnerability (medical condition yes or no – but no actual processing of medical details in the course of BCP processing activities) in order to allow the employer to exercise duty of care

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). Delegated data controllers are:

- For general BCP coordination in HQ:
  Head of Division and the BCP contact person in the Horizontal Coordination and Protocol Division (EEAS.BA.01)
- For HQ staff: BC related personal data processing in the Division is under the responsibility of the respective Head of Division
- For Delegation staff : BC related personal data processing in the Division is under the responsibility of the respective Head of Delegation

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

The recipients of your data may be EEAS assigned staff and line managers in your Division/Delegation to collect and store required data for the purpose of a BCP locally.

In order to handle an emergency situation dedicated staff of the follwing centralised HQ entities may also have access to your data:

- EEAS Business Continuity Team (BCT) is the body in charge of managing business continuity at HQ level. It is composed of the DG BA management, a representative of the SG Office and services in charge of security, IT, HR and budget. In specific situations it may need to call on other HQ services.
- Delegation Security Management Team (SMT): The SMT may have access in order to ensure Business Continuity and security and safety of staff.
- Departmental Security Coordinators are in charge of maintaining and updating BCP process data (phone numbers, evacuation procedures, identification of staff in need of special assistance) and defining a Business Impact Analysis, with attention given to political events (such as major conferences) or organisational changes.
- BA.SI.1 (Field Security): The Field Security Division is in charge of providing security risk management advice and solutions, leadership of the RSO network, physical security of Delegations and staff accommodation.
- EEAS Medical Cell in cases where medical advice is needed.

Personal data is not intended to be transferred to a third country or an international organisation. The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

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

You have the right of access to your personal data and the right to correct any inaccurate or incomplete personal data. 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 information, please see 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 have questions concerning the processing of your personal data, you may address them to your respective Division or Delegation administration (as the delegated controller) or to HQ BCT via the mailbox:

HQ-BUSINESS-CONTINUITY-PLAN@eeas.europa.eu

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

- 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.
- Article 18 of Decision of the High Representative on EEAS Security Rules dated 19/09/2017 - ADMIN(2017) 10;
- EEAS Headquarters BUSINESS CONTINUITY PLAN (Ref. Ares(2019)6539106 - 23/10/2019)
- Further reference: EEAS Business Continuity Operations Manual

8. TIME LIMIT - DATA STORING: For what period and how we process your data?

It is essential to maintain data in business continuity documents up-to-date and only as long as needed for BC purposes. Personal data is kept for the period of employment of the individual staff member or until the next update of contact lists. BCP overview and contact lists are updated regularly, at least once a year.

In the IT application - used for facilitation of day-to-day security in the Delegation as well as for providing crucial information for Delegation staff and assets in case of crises, the EEAS Security in Delegations Application (ESDAP) and its upgrade, the EEAS Security Portal, an all-in-one online portal bringing together security relevant information for Union Delegations - a backup of the data could be kept, in general, for a maximum period of 5 years after the end date of assignment in a Delegation. The specific Privacy Statement is available on the intranet under 'Security in Del'.

Security of data: Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725. Access to data processed for the purpose of BC is given only to dedicated staff members on a need-to-know basis. The collected personal data are stored on servers that abide by pertinent security rules. Access to specific files is provided based on 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. Entities may need to keep physical copies which are stored in a properly secured manner.

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