

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO ACCREDITATION AND NOTIFICATION OF DIPLOMATS BY UNION DELEGATIONS TO THE HOST COUNTRY AND TO INTERNATIONAL ORGANISATIONS

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS), including the Union Delegations. You have the right under EU law to be informed when your personal data is processed [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 processing activity i.e. the use and maintenance of personal data is the accreditation and notification of Delegation staff in Third Countries and at International Organisations (IOs) as laid down in the Vienna Convention on Diplomatic Relations (VCDR) of 1961.

Description

Processing at HQs: As laid down in Article 4 of the VCDR an "agrément" needs to be requested in order to accredit a Head of a Diplomatic Mission, for that reason personal data in a form of a CV are processed in order to launch the "agrément" request.

Processing at DELs: According to Article 10 of the VCDR staff members of a Diplomatic Mission needs to be notified to the local authorities, in order to do so the Delegation of the concerned country processes personal data according to the local requirements. The purpose of the notification is to have Delegation staff duly notified and accredited, enabling them to benefit from the privileges and immunities laid down in the Establishment Agreements and the VCDR.

3. DATA PROCESSED: What data do we process?

Data (category or type of data) processed are the following:

Headquarters: Personal data provided in a form of a Curriculum Vitae

EU Delegations: Personal data as per local requirements in order to launch a notification/accreditation request for the acquisition of local diplomatic ID documents.

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

Protocol Division of the EEAS (EEAS.SG.3)

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

The recipients, who may have access to the data are:

In Headquarters: designated staff of EEAS Protocol Division

In EU Delegations: designated staff from the relevant Delegation in the Third Country, including Administrative Section; Head of Delegation (HoD) and HoD Office; Regional Security Officer (RSO)

Heads of Diplomatic Missions receive this information when the Delegation collects the data for the purpose of local requirements before the notification/accreditation request.

Local authorities, including the Ministry of Foreign Affairs, or IOs, become recipients and may process personal data according to local requirements, as staff members of a Diplomatic Mission need to be notified to the local authorities pursuant to Article 10 of the VCDR. The purpose of processing and providing the data to local authorities, as described above, is to have Delegation staff duly notified and accredited, enabling them to benefit from the privileges and immunities laid down in the Establishment Agreements and the VCDR. Apart from the purpose defined above for accreditation personal data are 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 AND ERASURE OF DATA: What rights do you have?

You have the right of access to your personal data in particular at data collection 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. It is to be noted that requests for deletion of personal data may lead to the refusal or failure of the notification and accreditation process. 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 as well as to the relevant Delegations.

EEAS PROTOCOL DELEGATIONS < PROTOCOL-DELEGATIONS@eeas.europa.eu >

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

Legal bases at stake:

- Treaty on the Functioning of the European Union
- Protocol on Privileges and Immunities, in particular Article 7 thereof
- Delegations' Establishment Agreements
- The Vienna Convention on Diplomatic Relations 1961 (VCDR), in particular Art. 4 and 10 thereof

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 - DATA STORAGE: For what period and how we process your data?

Data will be retained for the duration of the posting and the following 5 years.

When appropriate – personal data contained in supporting documents is to be deleted where possible where the data is no longer necessary as per local requirements.

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.

In its electronic format the data will be stored by the Protocol Division in shared folders to which only designated staff members working have access. Security is also ensured by the safety measures built in IT applications used. 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.

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.