EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA BY THE EEAS RELATED TO ACCREDITATION AND NOTIFICATION OF THIRD COUNTRIES' DIPLOMATS AND OFFICIALS OF INTERNATIONAL ORGANISATIONS TO THE EUROPEAN UNION

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 to enable the accreditation of diplomatic agents to the European Union, including Heads of Diplomatic Missions of Third Countries and Heads of Representations of International Organisations. Personal data of heads and other members of the diplomatic missions accredited to the European Union, as well as the heads of the liaison offices of the international organisations accredited to the European Union and their deputies are collected for accreditation, notification and communication purposes including necessary verifications where applicable.

3. DATA PROCESSED: What data do we process?

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

- Name of the member of the diplomatic mission or international organisation office
- Name of the diplomatic mission or IO office
- Function, diplomatic title
- Date of the notification of arrival;
- Date of birth and patronym (where applicable)
- Name of the Spouse (where applicable)

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:

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

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

- Access to the data is provided to authorised EEAS staff of the Protocol Division (SG.3) according to the "need-to-know" principle. Such staff abide by statutory, and when required, additional confidentiality obligations.
- The Division responsible for HQ Security and EEAS Security Policy (EEAS.RM.SECRE.2) for the purpose of security related verifications where applicable
- The Diplomatic List including Heads and Members of the Diplomatic Missions accredited to the EU as well as Heads of Liaison Offices of international organisations accredited to the European Union is published on the website of the European External Action Service (EEAS)

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. The Diplomatic list is however published on the website of the European External Action Service (EEAS). 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:

PROTOCOL-ACCREDITATION@eeas.europa.eu

PROTOCOL-NOTIFICATION@eeas.europa.eu

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

Lawfulness: The processing is necessary for the accreditation and notification of diplomatic staff, a task performed by the EEAS within its public mandate and necessary for the management and functioning of the EEAS ~~lawful based on~~ (Article 5 (1) (a) of Regulation (EU) 2018/1725, of the European Parliament and of the Council of 23 October 2018).
Legal basis:
Article 04 and 10 of the Vienna Convention on Diplomatic Relations of 1961 and established diplomatic customs and practices followed by states and international organisations in international relations.
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 SECURITY: for what period and how securely do we process your data?

Storage period

Personal data is kept for as long as it is necessary to fulfil the purpose of collection and processing required for the accreditation and notification, for a maximum period of 10 years from the date of the communication by the diplomatic mission or liaison office, taking into account, among others, the purposes listed below. The electronic directory/database is continuously updated and obsolete data is deleted.

- 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 *e*-Domec policy.
- In case of an incident, event or enquiry by authorities, 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, personal data will not be kept longer than 5 years after the judgment on the pending case is final.
- When appropriate, personal data contained in supporting documents should be deleted where possible, if that data is not necessary for audit, inspection or other control purposes.

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: The data will be stored on the secured drive of the EEAS Protocol Division , hence meets EEAS' security standards or on EC DIGIT infrastructure that has been approved by EEAS Digital Solution and that meets their security requirements. Thereby, measures are in place to:

- aim for using privacy-enhancing technologies (PETs);
- ensure confidentiality, integrity availability and resilience of processing systems and services;
- restore availability and access to personal data in a timely manner in the event of physical or technical incident.

An information security policy is in place in specific areas and steps to make sure the policy is implemented and the controls to enforce them.

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.