EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO THE PROCUREMENT WORKING GROUP IT PLATFORM BY THE EEAS

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 enable the Controller and/or Delegated Controllers to identify the users that have access to the Platform during a specific period of time, and for the users to be able to receive relevant email notifications. The IT Platform will be used to securely upload and distribute proposals for relevant transfers.

Upon designating users by the respective Ministry of Foreign Affairs of the Joint Comprehensive Plan of Action (JCPOA) Participating State, the personal data of the assigned PWGP user will be provided by the representative of the Ministry of Foreign Affairs of a JCPOA Participating State to the Delegated PWG Coordinator, and the IAEA. The Controller retains the overview of the users' personal data until the user requests their deletion. Individual users have the right to access and amend their own personal data only for as long as the Platform is in operation or until they inform the Controller, i.e. the EU Delegation that they wish their personal date to be removed.

3. DATA PROCESSED: What data do we process?

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

- Name (first name, last name)
- Contact information: email address, phone number (not mandatory)
- User name
- Participating Country
- Participating Organisation (IAEA)

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 organisational entity responsible for managing the personal data processing operation under the supervision of the Head of Delegation or the Delegated Controller acting on his/her behalf is

Delegation of the European Union to International Organisations in Vienna

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

The recipients of your data may be

- Assigned staff of the EU Delegation of the European Union to International Organisations in Vienna with purpose limitation
- Assigned staff of the EEAS with purpose limitation
- IT developers of the EEAS: 3 officially assigned staff from the IT Development team and 3 officially assigned staff from the IT Operations Team will have controlled access to the Production servers via a Token mechanism
- A limited number of assigned staff from DIGIT IT Infrastructure have access to production servers for maintenance purposes

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?

The Controller with the delegated controller(s) will grant users the right to access the Platform. 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:

PWG-COORDINATOR@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, i.e. EU Delegation to International Organisations in Vienna, 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.

The Procurement Channel was established by the Joint Comprehensive Plan of Action (JCPOA) and endorsed by the UN Security Council resolution 2231 (2015) to review proposals by States seeking to participate in or permit certain transfers of nuclear or dual-use goods, technology, and/or related services to Iran. Proposals should be submitted to the UN Security Council. The Security Council will forward proposals to the Procurement Working Group. The Procurement Working Group will review proposals within a specified timeline and submit a recommendation on behalf of the JCPOA Joint Commission to the Security Council for the latter's final review and decision. Given the high sensitivity of the information included in these proposals, the complexity of the distribution processes, the tight timeframes, and the need to ensure confidentiality, it was considered important to create an electronic platform for that supports all relevant operations.

- Good administrative practices in the framework of the Treaty of Lisbon and the Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) available on http://www.eeas.europa.eu/background/docs/eeas_decision_en.pdf

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 SECURITY: for what period and how securely do we process your data?

Storage period

Personal data is kept until the date of termination of the paltorfm or Platform or until the date of termination of the active service of the user (i.e. end of contract, removal from post). The user can inform the Controller, i.e. the Delegation of the European Union to International Organisations in Vienna, at any time if they wish their personal data to be removed. This may need to be prior agreed with the respective Ministry of Foreign Affairs of the Joint Comprehensive Plan of Action (JCPOA) Participating State. Once the Platform's operation has been terminated, the data at the central server level will also be destroyed by the EEAS, after one year.

- 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

Access to the Platform is only permitted to assigned staff from countries that are participating in the JCPOA Procurement Working Group, and the IAEA as an observer to the Procurement Working Group. Only assigned staff should be allowed to access and use the Platform which was created to help operationalise the process described in the UN Security Council Resolution 2231(2015) regarding the submission of proposals for the supply, sale or transfer on nuclear and dual use items, materials, equipment, goods and technology in Iran. The IT Platform will be used to securely upload and distribute proposals for relevant transfers. Assigned staff will have the possibility to access the proposals, and submit their recommendation and comment within a secure environment.

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.

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.