Ref. Ares(2023)7952348 - 22/11/2023

European Union
EXTERNAL ACTION

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO VISITORS TO EU DELEGATIONS VIA THE E-VISITOR SYSTEM

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 this data processing operation is to register all visitors (non EU Delegation staff) who access the premises of an EU Delegation and to monitor and have control over the visits.

- The EEAS' EU Delegations visitors' management system aims at managing all processes related to the organisation of a visit for non-EEAS staff, except co-located staff working on the premises, to the EU Delegations premises. It facilitates a smooth check-in process, provides a high level of security and reliable information on the number of visitors inside the EU Delegations buildings as well as increases the safety of visitors.
- It also ensures the protection of EU Delegations security and safety interests, including staff under the responsibility of the EEAS, EU Delegations premises, physical assets, information and visitors.

Description

I. Registration of visitors via the "e-Visitor@EUDELs" system

EU Delegations shall manage visits to their premises under the responsibility of the management of the delegation and in accordance with the procedures defined centrally by the HQ Security and EEAS Security Policy Division and the CRC Field Security Division.

Before allowing any visitor (including a family member of Delegation staff) to enter the Delegation premises the receptionist/security guard* will check either on the printed list received or, if the visitor is not on the list, with the person receiving the visit and, if the visit is confirmed, will allow the visitor to proceed to the reception. The receptionist/security guard will deliver a numbered "Visitor" access card upon showing a valid picture ID card. Unless an equivalent procedure is in place, the receptionist/security guard will retain the ID card until the "Visitor" card is returned. The printed list of the daily visits will be collected and destroyed at the end of the day by a designated staff member of the EU Delegation.

*except:

- staff members of EU institutions, in particular based in Brussels,
- ambassadors who may not be provided with a visitors' badge depending on the reciprocity of the Protocol of each Delegation.

Registration of the visit will be implemented using the "e-Visitor@EUDELs" available on @HelloAdmin where all EU Delegations staff (HOST) will be able to pre-register their visitors. During the pre-registration, the HOST records following visitor personal information: "first name", "last name" and "nationality". Optionally, the passport/ID number, email address, phone number(s), representing entity (private company, public organisation, institution, etc ...). The HOST can modify the data at all times.

Authorization to access is managed within the visitor management system. Authentication to the system is managed through EU Login.

Once this is completed, and when the visitor presents him/herself at the main entrance reception desk or in one of EU Delegation buildings he/she will be able to proceed with the check-in. The receptionist encodes the passport/ID number or the number of another personal document recognised by the delegation, if not provided during pre-registration.

The first name, last name, nationality and passport/ ID number will be scrambled automatically after 2 years following the last visit registration. It will be kept for this period of 2 years for the purpose of security reasoned investigations.

II. Use of registry/logbooks [In case the e-Visitor system is not operational]

Delegations may use registry/logbook in case the application is not available for any technical and logistic reason. The receptionist/ security guard records personal data from the visitor and the entry and exit times in the visitors' registry/logbook.

3. DATA PROCESSED: What data do we process?

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

Identification and contact data EEAS/EU Delegation staff ["Host"]

- First name, last name, EEAS e-mail and EU login user ID (moniker), professional phone(s), department, office

Identification and contact data of a VISITOR ["Invited participant, guest"]

- First name, Last name, Title
- Nationality
- Passport or ID number
- E-mail or Phone number
- Company

Visit related information

- Time and date of check in, break and check out
- Person visited (HOST)
- Approval of the visit
- Visits registered by an EU Delegation staff member or where the EU Delegation staff member is the visited person.

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 Directorate / Division / EU Delegation entrusted with managing the personal data processing under the supervision of the Director / Head of Division / Head of Delegation is the following organisational entity:

HQ Security and EEAS Security Policy Division, RM. SCS.3

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

The recipients of your data may be

- EU Delegations staff of the organisational entity acting as meeting organiser or registering the visit (HOST)
- EEAS staff who act as administrators/host of the system
- In HQ: dedicated staff members of "HQ Security and EEAS Security Policy Division" and 'Field Security' Division that would need this data for audit or inspection of the visitor's registry. The Division 'Inspection' for evaluation, ex-post control or inspection and the Security Directorate of EC upon an official request to HQ Security and EEAS Security Policy Division" and 'Field Security' Division for justified purposes.
- Contractors and employees of external security companies in charge of EU Delegations accreditation services, who for the performance of their duties need access to the IT system (subject to their "need to know") and to follow the instructions of the members of EU Delegations Security Management Teams in application of the EEAS access policy
- Contractor of the Digital Solution division for technical application support and troubleshooting purposes of the system
- ServiceNow technical support for issues with the underlying SAAS platform
- The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

Even though not considered as recipients under Regulation (EU) 2018/1725, investigating entities of the EEAS, the EU and Police forces in the exercise of their official authorities may be granted access to personal data processed by the e-Visitor@EUDELs system. This is subject to the authorisation by the relevant EEAS Authority.

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?

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:

EEAS-Security-Accreditation@eeas.europa.eu

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

Lawfulness

The processing of personal data is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the EEAS, in particular for the management and functioning of the European External Action Service in order to protect EEAS security interests, including premises, staff, equipment and information, [Article 5(1)(a) of Regulation (EU) 1725/2018 as referred to in Recital 22 thereof].

Legal references

- Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community(OJ 45, 14.6.1962, p. 1385)
- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19/06/2023 on the security rules for the European External Action Service ADMIN(2023) 18

Further legal reference:

- Vienna Convention on Diplomatic Relations and Optional Protocols of 18 April 1961
- Establishment agreements concluded by the EEAS with the third countries
- 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 FOR DATA STORED & SECURITY MEASURES: For what period and how we process your data?

Personal data is kept as follows:

- For EU Delegations HOST:

Identification and contact data is kept until the host staff member is employed by the EU Delegations as it is part of the user provisioning and access rights to the system and for subsequent 5 years until the exhaustion of all claims related to a possible disciplinary action.

- For EU Delegations VISITOR:

Personal data (first name, last name, email, company, passport/ID) is kept for a maximum period of 2 years after the last visit. After that period all data subjects' relevant records will be anonymised.

- For visit-related data:

Data is kept as long as the system is in use.

Only badges not containing personal data (i.e. those for visitors) may be re-used

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.

Data is stored in the cloud in the ServiceNow databases, it is encrypted at rest Data in the application is protected by access control lists based on roles defined in the system. Data shall not be stored by the sub-contracted enterprise employing the security guards.

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.