EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO

E-VISITOR – THE EEAS VISITORS' MANAGEMENT SYSTEM

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS) and to the Delegations of the European Union. 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 the 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 EEAS visitors' management system aims at managing all processes related to the organisation of a visit to the EEAS premises. It facilitates a smooth check-in process, provides a high level of security and reliable information on the number of visitors inside the building as well as increases the safety of visitors.
- It also ensures the protection of EEAS security and safety interests, including staff under the responsibility of the EEAS, EEAS premises, physical assets, information and visitors.
- The purpose of processing data required in the context of the COVID-19 pandemic prevention measures is to ensure fulfilling the necessary public health measures and to protect EEAS/EU Delegations' staff and third parties, including external visitors by containing and preventing the spread of the Coronavirus (COVID-19) in the current emergency context.

3. DATA PROCESSED: What data do we process?

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

- For EEAS HOST / FPI HOST/ EUSR HOST (Staff of the EU Special Representatives) - ["meeting organiser"]:

  First name, Last name, EEAS, EUSR (professional) email address or Commission (professional) email address, Office address, office telephone number, user mobile number (optional)

- For EEAS VISITOR / FPI VISITOR/ EUSR VISITOR ["invited participant, guest"]:

  First name, Last name, Nationality, Passport or ID number, E-mail (optional), Phone number (optional), company (optional), validity of the Security Clearance if EU Classified meeting is organised in KO building, time and date of check in and check out.

  In the context of the COVID-19 pandemic prevention measures additional information is processed:

  - Data on whether you have been in contact with anyone who tested positive with Covid-19 in the last 14 days
  - Data on whether you have any of symptoms of fever, tiredness, dry cough, loss of smell/taste

  Answer options are 'yes' or 'no'. If the answer to any of the questions is 'yes', you will be requested to reconsider the form of your visit and make arrangements for an alternative solution, including a video-conference with your host.

As of 15/10/2021 external visitors are requested to exhibit either a proof of vaccination, a certificate of recovery or a negative Nucleic Acid Amplification Test (NAAT) of less than 72h or a Rapid Antigen Test (RAT) of less than 48h to be checked at entry with no further data storage.

4. DATA CONTROLLER: Who is entrusted with processing your data?

The Controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Division responsible for managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

HQ Security and EEAS Security Policy Division RM.SECRE.2

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

The recipients of your data may be

- EEAS staff of the organisational entity acting as meeting organiser (HOST); In respect of data required in the context of the COVID-19 pandemic prevention measures the meeting organiser will be notified in an e-mail only about the fact that at least one of your answers was "Yes"
- Staff of the Service for Foreign Policy Instruments (FPI) of the European Commission, when FPI acts as the meeting organiser, has access to the same data as the meeting organiser in the EEAS.
- EEAS staff who act as administrators/host of the system
- Assigned staff of HQ Security and EEAS Security Policy (RM.SECRE.2) with access to Yes/No replies on screen
- Contractors of external security companies in charge of EEAS 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 EEAS Internal Security in application of the EEAS access policy
- Contractor of external company "Proxyclick" which is the service provider of the system and acts as Cloud Customer has only access if absolutely required for troubleshooting purposes, under the binding clauses of the Data Processing Agreement (DPA).

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 eVisitor 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. 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 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. Efforts will be made that if deemed legitimate rectification or deletion requests would be implemented in general in 10 working days. Special attention is drawn to the consequences of a request for erasure, in which case any trace to be able to contact an individual, e.g. a visitor to notify for example about contact with a contaminated person, will be lost. 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. The EEAS may restrict the right of access, rectification or erasure as well as the right to know about a data breach for the grounds of protecting EEAS internal security laid down in Article 25(1)(d). 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 FMB:

EEAS SECURITY ACCREDITATION

<EEAS-SECURITY-ACCREDITATION@eeas.europa.eu>

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

- 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, namely to preserve the security of its buildings. The processing is lawful under Article 5(1)(a) of Regulation (EU) 2018/1725.
- Data, including health-related information is processed based on Article 10.2 (i): public interest in the area of public health, in addition to Art. 5.1 (a): necessary for the public interest in the exercise of duty of care and Art. 5.1 (e) vital interest of individuals.
- 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.
- 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 19/09/2017 on the security rules for the European External Action Service (ADMIN(2017)10).
- ADMIN(2021)251 Decision of the Secretary General of the European External Action Service of 12/10/2021 on Health and Safety Measures for visitors to the EEAS premises in Brussels (Ref. Ares(2021)6208970 - 12/10/2021).

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

- For EEAS HOST:

  Data is kept until the host staff member is employed by the EEAS 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 EEAS VISITOR:

  Automatic deletion of data after 2 years.

Data concerning risk factors in the context of the COVID-19 pandemic prevention measures are to be kept for 30 days taking into account the general incubation and quarantine period of fourteen days plus one day prior to the visit (for testing and feedback of results) equalling fifteen days doubled for the purposes of staff safety, contact tracing and duty of care (timeframe to be adjusted according to updated information issued by ECDC or WHO for the incubation period, as needed).

Data will be automatically deleted after 30 days. For the Covid questionnaire data will not be retained further for an audit trail than the 30 days defined in the system, except for the scenario described below.

In case it is required to keep data longer exclusively for reasons of protection of public health, including when a positive case being detected or traced back to a particular meeting makes it necessary to ensure the possibility to warn individuals who are at risk of contamination, data may be furthermore needed and therefore specific information on particular days/visits will be retained for the time period required to be informed about eventual positive test of any participant of the meeting as well as for the time-period technically needed for subsequent manual deletion of the selected data.

Data of visitors related to proof of vaccination, certificates of recovery or results of a NAAT/RAT tests are not kept by the EEAS.

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. 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. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. Security is also ensured by EU Login account authentication through unique password, associated with only one email address with double authentication. The eVisitor system is cloud-based to which the EEAS has administrator rights. The cloud provider selected for the tool provides sufficient assurance to act on behalf of EU Institutions and to implement the necessary technical, organisational and data protection measures as well as to verify the effectiveness of those measures (effective security strength in data traffic encryption, copies of audit certificates) based on legally binding contract clauses including the protection of personal data. Responses to the questions asked in the context of the COVID-19 pandemic prevention measures are only visible to persons on a need-to-know basis.

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.