EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO

SECURITY PORTAL BY THE EEAS (HQ AND EU DELEGATIONS)

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?

The purpose of the present processing operation is to ensure the EEAS fulfils its duty of care on staff working in Union Delegations around the world collecting the necessary information on staff posted or travelling to Delegations.

The data collected by the Security Portal will be used for the management of security and protection of the EEAS security interests, mostly to respond to incidents or emergencies/crises like evacuations or similar situations, natural or man-made disasters, civil unrests, criminal attacks or any other major threats.

In addition, some data of the Security Portal will be used also for day-to-day monitoring of compliance with security rules and instructions from HQ on continuity of operations (permanence of Head of Delegations, duty phones, list of professional visitors in the Union Delegation, security equipment and contracts, security of accommodations, etc.). The Security Portal includes modules to process personal data of EU staff and their dependents, delegation security assets as well as information on the Delegations' security providers.

3. DATA PROCESSED: What data do we process?

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

1) Data extracted from other databases (Sysper, HR Delegation, MIPS, Immogest, e-Tim):

- personal data of EU staff in Union Delegations, local agents and professional visitors (per ID, last name, first name, gender, birthdate, nationality, email, phones, status, begin/end date, job title/position, addresses, absences dates, mission dates and destination);
- personal data of dependents of EU staff in Union Delegations (EU staff per ID, last name, first name, gender, birthdate, nationality, begin/end date);
- contact persons of EU staff to be contacted in case of emergency (name, relationship, email, phones);

2) Data encoded directly in the Security Portal by the Data subject:

- additional personal data of expatriates (private emails, phone numbers, private vehicle details);
- diplomatic data (passports, laissez-passer and visa numbers);
- private visitors of expatriate staff (last name, first name, arrival/depart dates, address, telephone, comments, gender, birthdate)
- basic data including date of arrival and date of departure (to be used only in case of country evacuation);

3) Data encoded by the Titular expatriate in the Security Portal on behalf of the Data subjects in his/her household:

- dependents' absences details (dates, location)
- additional personal data of dependents (private emails, phone numbers, private vehicle details);
- diplomatic data of dependents (passports, laissez-passer and visa numbers);

4) Data encoded by a member of the Security Management Team on behalf of the Data subjects:

- personal data (Fist, Last name, Gender, birthdate, Institution, position, staff category, nationality, start and end date in Delegation) of Other Staff posted in the Union as co-locators
- personal data (Last, First name, Per ID, Position, Institution, Gender, Birthdate, Nationality, Mobile phone, Visit start and end dates, address during visit and purpose of the visit) of Professional visitors (not using MIPS) from other EU bodies/institutions under a Service Level Arrangement with the EEAS
- all different service phones available in each Union Delegation (duty phones, service mobile and satellite phones);
- radio network details ;
- contractors details (name and license number) in case they are armed.

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. The representative of the controller, the service – EEAS Division – responsible for managing the personal data processing under the supervision of the Head of Division is the following entity:

EEAS Field Security Division – SG.CRC.3

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

The recipients of your data may be

In Union Delegations:

- Titular Expatriate colleagues have access to their own personal information.
- The Security Management Team (SMT) members accesses will be limited to staff with a specific security tasks and officially designated as part of the SMT-team), including the Head of Delegation (HoD), the Delegation Security Coordinator (DSC), the Regional Security Officer (RSO), the Head of Administration (HoA), the Registry Control Officer (RCO) and other staff performing similar tasks or functions.

  The above-mentioned recipients have access to data of their own Union Delegations, except for RSOs who have access to the Union Delegations in their area of responsibility, but also have the possibility to access information on Delegations outside this area for business continuity reasons and on a strict need-to-know basis.
- Assigned staff of Member States embassies for support in case of country evacuations with the approval of the Head of Delegation/Chargé d'Affaires.

In EEAS Headquarters:

- Field Security Division colleagues will have different access rights and profile according to their 'need to know' and they responsibilities (Security Desk, Resources and Logistics or Strategy officers or assistants).
- EU Sitroom duty officers will have limited view access in order to be able to respond and contact colleagues in case of emergency.
- Auditors of the Internal Audit Division have viewer access .
- Inspectors of the Inspection Division have limited viewer access, for a pre-determined duration of one month, to the information on the Union Delegation they are mandated to inspect.

In all cases, the information in question will not be communicated to third parties, except where necessary for the purposes outlined above in case of absolute need.

Exceptionally, in case of a security incident or crisis requiring potentially a country evacuation, information concerning staff in a Union Delegation and/or professional visitors from HQ to this Union Delegation could be transmitted to another EU Member State Embassy in order to obtain assistance.

In countries where agreements have been reached in advance with another EU Member State Embassy for support in case of country evacuations, lists of EU staff in the Union Delegation concerned will be regularly extracted and sent to the partner Embassy to prepare necessary logistics. Only for such purposes, the information stored in the Security Portal could be communicated by the appropriate Security Officer to a Member State Embassy with the approval of the Head of Delegation or Chargé d'Affaires a.i.

Potential transfers of personal information may take place in the context of an emergency or an evacuation to International Organisations as the United Nations or to Third country authorities but will be limited to cases of vital interest for the security of concerned Data subjects. 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. 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:

SG-CRC-3@eeas.europa.eu

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

Lawfulness: The processing of your personal data is necessary for the performance of a task carried out by the EEAS in the public interest, in particular for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof and to comply with the legal obligation for the EEAS to fulfil its duty with regard to other institutions and member state embassies and in line with the Security Risk Management principles stated in EEAS Security Rules.

Legal references:

- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service - ADMIN(2017) 10.
    - Art. 3: duty of care obligation
    - Art 11 Security Risk Management principles
- The good administrative practices in the framework of the Treaty of Lisbon;
- Internal Instruction Note from Director General on Budget and Administration on the instructions for completion of Security Portal Ares(2020)4565848
- Agreements, including Service Level Agreements or Colocation agreements, with different EU Institutions, bodies and agencies (European Parliament, European Court of Auditors, European Investment Bank, etc.)
- Decision of the Secretary General of the European External Action Service on the EEAS Inspection Service ADMIN(2020) 5
- Internal Audit Charter, dated 1 March 2018
- Note to the attention of EEAS Management and EU Heads of Delegation on the updated Internal Audit Charter and Mutual Expectation Paper Ares(2018)1163393

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 STORING: For what period and how we process your data?

Data Storage: Personal data is kept for a maximum period of 5 years after the end date of assignment in a given Delegation unless the information has been flagged for a potential investigation or is required for a perusal of a security incident.

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. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. The data traffic between the servers and the client browsers is encrypted. Access to personal data is only possible to recipients with a UserID/Password. Data is processed by assigned staff members. The level of access to data within the Security Portal is controlled via assigned user roles. Physical copies of personal data are stored in a properly secured manner. The system makes usage of staff information from the internal staff management system Sysper. Certain information can be extracted from the system and saved in external files by authorized users. The Security Portal is accessible only from the internal network of the European Public Administrations.

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

In case 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 of recourse to the European Data Protection Supervisor at edps@edps.europa.eu.