EEAS PRIVACY STATEMENT

for the purpose of the processing operation

'ESDAP (EEAS Security in Delegations Application)'

1. INTRODUCTION

THE PROTECTION OF YOUR PRIVACY INCLUDING YOUR PERSONAL DATA IS OF GREAT IMPORTANCE TO THE EUROPEAN EXTERNAL ACTION SERVICE (EEAS), THEREBY REFLECTING THE PROVISIONS OF THE CHARTER ON FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, AND IN PARTICULAR ITS ART. 8. THE PRESENT PRIVACY STATEMENT DESCRIBES WHICH MEASURES ARE TAKEN IN ORDER TO PROTECT YOUR PERSONAL DATA WITH REGARD TO THE ACTION INVOLVING THE PRESENT DATA PROCESSING OPERATION AND WHAT RIGHTS YOU HAVE AS A DATA SUBJECT. YOUR PERSONAL DATA ARE PROCESSED IN ACCORDANCE WITH REGULATION (EC) 45/2001 *ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA BY THE COMMUNITY INSTITUTIONS AND BODIES AND ON THE FREE MOVEMENT OF SUCH DATA*, AS IMPLEMENTED IN THE EEAS BY DECISION OF THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY OF 8 DECEMBER 2011. ALL DATA OF A PERSONAL NATURE - NAMELY DATA WHICH CAN IDENTIFY YOU DIRECTLY OR INDIRECTLY - WHICH YOU PROVIDE TO THE EEAS WILL BE HANDLED WITH THE NECESSARY CARE.

2. PURPOSE OF THE PROCESSING OPERATION

The purpose of the present processing operation is to help the EEAS fulfil its duty of care on staff working in EU Delegations around the world.

The data collected by ESDAP will be used for the protection of EEAS security interests[1], mostly to respond to emergencies or crisis like evacuations or similar situations, natural or man-made disasters, civil unrests, criminal attacks or any other major risk that could have a significant impact on the protection of EEAS security interests in Delegations.

In addition, some data of ESDAP could also be used for day-to-day monitoring of compliance with security rules and other instructions from HQ on continuity of operations (permanence of Head of Delegations, duty phones, list of visitors in the Delegation, security equipment and contracts, etc.).

Under no circumstance would this information be used for checking working times.

3. DATA PROCESSED

The data processed for that purpose are the following:

1- Data extracted from other Commission/EEAS databases (Sysper2, E-Del-HRM, MIPS, Syslog):

- personal data (per ID, last name, first name, gender, birthdate, nationality, status, begin/end date, job title/position) of EU staff in Union Delegations, local agents and professional visitors from HQ;
- personal data (EU staff per ID, last name, first name, gender, birthdate, nationality, begin/end date) of dependants of EU staff in Union Delegations;
- basic information of Personnel Security Clearance (if any) and status (to be extracted from e-Clearance - not yet implemented);
- contact persons in case of emergency (name, relationship, email, phones);
- Security trainings performed (name of training and dates)

2- Data encoded directly in ESDAP:

- additional personal data (private emails, car details);
- diplomatic data (passports, laissez-passer and visa numbers);
- private Visitors (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);
- all different service phones available in each Delegation (duty phones, service mobile and satellite phones);

ESDAP does not process data which reveal racial or ethnic origin, political opinion, religious belief trade union affiliation or sexual preference.

4. CONTROLLER OF THE PROCESSING OPERATION

The controller[2] responsible for the processing operation is the Head of MDR B.1 Field Security or his/her Deputy acting on his/her behalf.

---

[1] The Staff placed under the responsibility of the EEAS, EEAS premises, dependants (meaning the eligible dependants of the staff placed under the responsibility of the EEAS in Union Delegations forming part of their respective household as notified to the Ministry for Foreign Affairs of the receiving State), physical assets, including communication and information systems, information, and visitors.

[2] The controller is the organisational entity which determines the purpose and means of the processing of personal data.

5. RECIPIENTS OF THE DATA

With regard to the recipients of your data:

- In Delegations: the recipients of these data will be limited to staff with a specific security task and duly designated as part of the Security Management Team, including the Head of Delegation (HoD), the Delegation Security Coordinator (DSC), the Regional Security Officer (RSO), the Head of Administration (HoA) and other staff performing similar tasks or functions;

- In HQ: the recipients will be limited to relevant staff of MDR B Security Directorate (mainly MDR B1 Field Security), on a strict need-to-know basis, as well as Duty officers of the Managing Directorate for Crisis Response and Operational Coordination (EU SITROOM, Watch Keeper Capability and Consular Crisis Division). For security inspection purposes, also some inspectors in the Delegation Support and Evaluation Services of the EEAS could be granted access to ESDAP only after their need-to-know is adequately proven;

- In HQ and exclusively for the section "Permanence of HoD": "view only" access rights have been granted to middle and senior management in HQ (including the HR/VP Cabinet, Managing Directors and assistants of MDR and geographical Directorates, for the unique purpose of facilitating contacts between HQ and Delegations in case of absence or mission of Heads of Delegation, for the protection of EEAS security interests. In this module, only data of HoD and Chargés d'Affaires will be visible to users in HQ. The rest of staffs' personal information will not be visible to these users in HQ.
In all cases, the information in question will not be communicated to third parties, except where necessary for the purposes outlined above.
Exceptionally, in case of a country evacuation (or similar critical situations for staff), information concerning staff in a Union Delegation and professional visitors from HQ to this Delegation could be transmitted to another EU Member State Embassy in order to obtain assistance.
In some countries where agreements have been reached in advance with other EU Member State Embassy for such kind of support in case of country evacuations, lists of EU staff in the Union Delegation concerned are regularly sent to the partner Embassy to prepare necessary logistics. Only for such purposes, the information stored in ESDAP could be communicated by the appropriate Security Officer to a third party with the approval of the HoD or Chargé d'Affaire a.i.

- In HQ and exclusively for the section "Security Trainings":, View and Edit rights will be granted exclusively for this section to the appropriate member(s) of staff in EEAS MDR C4 Division, dealing with security trainings.

6. PROVISION, ACCESS AND RECTIFICATION OF THE DATA

You have the right to access your personal data and the right to correct any inaccurate or incomplete personal data, as well as to request the removal of personal data as follows. A request for blocking or erasure of data if deemed legitimate will be implemented within 10 working days In case you request to remove your data, they will be deleted from the system.

In case you are EU staff in Union Delegations, you have the following rights to your data:
- access rights only to your personal and your dependants data;
- right to correct or modify any inaccurate or incomplete personal data above;
- right to request the removal of personal data above stored in the application.

If you are a dependant, a local agent or a professional visitors to the Delegation (including staff from HQ on mission) you do not have access to the application, however you can request to modify the information through the appropriate EU staff, that is, respectively:
- the relative working in Delegation, for dependants;
- the Head of Administration of the Delegation, for Local agents and professional visitors to the Delegation.

If you have any queries concerning the processing of your personal data, you may address them to the data controller at the following functional mailbox: MDR-B1@eeas.europa.eu.

7. LEGAL BASIS FOR THE PROCESSING OPERATION

The legal basis of the processing operation at stake is:
Good administrative practices in the framework of the Treaty of Lisbon, 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, and the Decision HR DEC(2013) 006 of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service.

8. TIME LIMIT FOR STORING DATA

Your personal data of staff will be retained in principle for a period covering the duration of your assignment to a Union Delegation. However, for the purposes listed above, a backup of the data could be kept for a maximum period of 5 years. Data will be deleted at the end of this period.

9. CONTACT

In case you have questions related to the protection of your personal data, you can also contact the EEAS' Data Protection Office 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.