# EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

**FOR THE PURPOSE OF**

**PROCESSING PERSONAL DATA RELATED TO**

**THE RECORDING OF THE EMERGENCY PHONE CALLS AT THE EEAS SECURITY CONTROL ROOM**

## 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 ensure safety and security of individuals, EEAS staff, third parties, premises, goods and information by recording the incoming emergency phone calls to the security numbers of the EEAS Security Control Room for security-related reasons and possible subsequent investigations. The phone calls are analysed for potential threats to take action and for an eventual investigation of the incidents or any risks to the EEAS. The recordings are also used for the purpose of controlling the quality of handling the calls, by retrieving the data, if and when needed, with the aim of verifying the content of the information exchanged with the caller and to improve the service, if necessary.
The analysis of the phone calls allows avoiding and mitigating potential threats and taking action for subsequent investigations of the incidents or any risks to the EEAS.
Pre-announced automated recording of the incoming emergency calls takes place and selected calls are listened to by security personnel in order to identify any potential threat to be analysed further by investigators to reconstruct the events, in case necessary, as appropriate.

## 3. DATA PROCESSED: What data do we process?

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

- Phone calls with the conversations
- Phone numbers
- All categories of data may be recorded depending on the content of the phone call, including the name and any other personal data of the caller.

## 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 Division responsible for managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

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

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

The recipients of your data may be

- authorised EEAS Security Officers, Heads of Sector, Operations Team, Security Investigations Sector (RM.SECRE.2)
- call centre personnel
- Director General for Budget and Administration
- EEAS Security and Infrastructure Director (RM.SECRE)
- EEAS Head of Security Division (RM.SECRE.2)
- EEAS Horizontal Division in case of necessity of a fraud or disciplinary investigation (RM.01)

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. 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-HQ-SECURITY-COORDINATION@eeas.europa.eu**
**Please indicate in the Subject of your e-mail:**
**'Request in relation to the emergency phone call to the Security Control Room'**

**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) 1725/2018] as referred to in Recital 22 thereof. In case you contact the EEAS Security Control Room related to an emergency situation, the processing of your personal data may be necessary to protect the vital interest of any individual concerned [Article 5(1)(e) of Regulation (EU) 2018/1725].

Legal reference

- EEAS Security Rules, HR/VP decision ADMIN(2017) 10 of 19/09/2017
- Art 3 (Duty of care); Art 7 (Security incidents and emergencies); Art 10 (Investigations of security incidents, breaches and/or compromises and corrective actions); Art 13 (Organisation of security in the EEAS)

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?**

Personal data is kept for the following periods:
- For quality control and security-related purposes calls are kept for 360 days.
- Data necessary for an on-going investigation are kept till the legal claims from the investigation expire.

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. Files have authorised access. 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.