Ref. Ares(2022)4870569 - 04/07/2022

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

EU SITUATION ROOM DATA COLLECTION AND MAINTENANCE FOR PROVIDING CRISIS-RELATED INFORMATION VIA THE GCT SYSTEM BY THE EEAS

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 processing of the data such as telephone numbers, conference call identifiers, e-mails of addressees of alerts and Duty Officer (DO) contact data is to allow for the EU Situation Room to provide crisis-related information for relevant parties in the form of receiving SMS/e-mail alerts.

Description:

The EU Situation Room is collecting and maintaining data in a database including both office GSM and private GSM telephone numbers as well as office e-mails of officials who have to receive alerts and Duty Officers' contact data protected by passwords on various contact lists. Data used for conference calls are also kept for further reference in case of technical problems.

Further communication by the EU Situation Room takes place in the specific context of the EU Integrated Political Crisis Response (IPCR) using the IPCR database of the Council.. Arrangements for alerting, spreading and exchanging information, including information about monitoring of the crisis situation and contacting the relevant persons about crises are the cases where the IPCR and its tools are being used.

The EU SITROOM acts as contact point to IPCR for the EEAS, receives the request from EEAS staff who want to be part of IPCR fills in a form which is forwarded to the Council. It contains the EEAS e-mail address.

The IPCR record and privacy statement can be found here.

3. DATA PROCESSED: What data do we process?

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

- Name, surname
- Function
- Title/post held
- Telephone numbers, office GSM or private GSM numbers
- Professional e-mail address, certain specific private e-mail addresses
- Duty Officers contact data (password protected)

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:

EEAS EU SITUATION ROOM, MD CSDP-CR.SITROOM

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

The recipients of your data may be

- EU Situation room staff
- Relevant services of the EEAS (EEAS management and Watchkeepers)
- In respect of IPCR: staff of the General Secretariat of the Council (GSC).
- Users entitled to access the IPCR application will be able to see the list of contact details of central IPCR contact persons and of Member States' points of contact at a national level accessible via the system.
- Member States' core users as well as the core users from EU institutions can furthermore access the whole list of users of the system and have editing rights for their own core user group.
- Information on IPCR webpage: data of contact persons may be disclosed to the originators of any IPCR system on a-related request received by the EU Situation Room.

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:

EUSITROOM@eeas.europa.eu

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

Lawfulness: The processing of your personal data is necessary for the performance of a task carried out by the European External Action Service 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.

Legal reference:

- 2732nd Council meeting (Justice and Home Affairs): conclusions of 1-2 June 2006;
- 9687/06 List of A Items;
- 9552/2/2006 Second revised I/A Item Note;
- Article 240 of the Treaty of the European Union

Further legal references:

- 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.
- Good administrative practices in the framework of the Treaty of Lisbon

8. TIME LIMIT & DATA SECURITY: for what period and how securely do we process your data?

Storage period

- Your data are kept for the period during which the person is entitled to receive SMS/e-mail alerts. It will be erased when the EU Situation Room is informed about the change of status.
- IPCR (Council website): Your data are erased from the applicable list when you request to be removed. IPCR manages its users. As office e-mails are contained in IPCR, when your EEAS e-mail address is discontinued, notifications are not received any more and the mechanism of IPCR tracking inactivity will remove the person according to IPCR policies.
- Data updates are done as needed on information received or collected and systematically once a year. For being able to trace back information and for backup purposes, the immediately preceding versions of contact lists are kept for another year.
- Once information is provided to the EU Situation Room to do so – blocking or erasure is made within 3-5 days both for IPCR and GCT.
- Personal data may be kept for information and historical, statistical or scientific purposes for a longer period of time with appropriate safeguards in place. Archiving shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of individuals. Reports and other material containing personal data are archived according to *e*-Domec policy.
- In case of an incident, event or enquiry by authorities, data subjects or other concerned individuals' personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. In any case, personal data will not be kept longer than 5 years after the judgment on the pending case is final.

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.

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.