EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO THE "CONSULAR ON-LINE" PLATFORM (CoOL-EXONAUT)

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 personal 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?

Purpose

The purpose of the present processing operation is to provide and share information on consular protection matters and, in particular in the case of a consular crisis affecting EU citizens.

Description

The Consular Online (CoOL-EXONAUT) platform provides travel advice and information on consular representation of the EU and its Member States in third countries based on data provided by Member States' Ministries of Foreign Affairs. It also features a discussion forum to share information on consular issues, including threads on specific topics. As a reference, the platform provides links to the websites of Member States' Ministries of Foreign Affairs, where further details on travel advice can be found. In addition, a restricted area accessible to a limited number of users gives access to consular crisis preparedness' documentation, such as Joint EU Consular Crisis Preparedness Frameworks, exercises (incl. contact lists of embassies and consulates, honorary consuls and local authorities), children and family issues, including a secured forum. CoOL also contains a contact list of EU Member States' Ministries of Foreign Affairs Crisis Centres and Consular Services. The platform is also used to generate lists of users to exchange information between the EEAS, EU Member States and like-minded third countries, as well as to exchange information regarding crisis contingency (EEAS/EU MS) and crisis response.

3. DATA PROCESSED: What data do we process?

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

- First name
- Last name
- Email address
- Entity/Country (Member States capitals and diplomatic representations as well as honorary consuls, EC/ECHO, DEVCO, HOME, JUST, EU Delegations, EEAS, Australia, Canada, Iceland, New Zealand, Norway, Switzerland, the United Kingdom and the United States, third countries' local authorities)
- Place of posting (EU Delegations)
- Title (optional)
- Description (optional)
- Address (optional)
- Telephone (optional)
- Mobile phone (optional)
- Information exchanged in the discussion forum (optional)

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 Consular Affairs Division (EEAS.ISP.4)

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

I. Administrators

- Assigned staff members of the EEAS ISP 4 Consular Affairs Division

II. Processor (4 C Strategies)

- Assigned staff members of 4C Strategies

The service provider processing data on behalf of the data controller is 4C Strategies (Vattugatan 17, 11152 Stockholm, Sweden)

III. Other Users (According to their respective rights)

- Member States' representatives (designated by the Ministry for Foreign Affairs both in central administration and some diplomatic representations abroad);
- Relevant representatives of like-minded third countries (Australia, Canada, Iceland, New Zealand, Norway, Switzerland, the United Kingdom, and the United States);
- Other EU colleagues (EU Delegations/EEAS/ECHO/DEVCO/HOME/JUST/General Secretariat of the Council) nominated by their hierarchy.
- Exceptionally, for technical support and troubleshooting the EEAS RM.BS.3 (IT) Division.

The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

CoOL users have access to the crisis management contact lists of EU Members States' Ministries for Foreign Affairs (Crisis Centres and Consular Services) as well as the personal information in documents stored in CoOL provided they have the necessary rights. Access to the Consular Online tool is granted to ministry and government representatives, including like-minded third countries such as Australia, Canada, Iceland (EEA), New Zealand, Norway (EEA), Switzerland, the United Kingdom and the United States of America on the basis of mutual understanding. Transfer of personal data to the aforementioned countries is necessary for important reasons of public interest (Art.50(1)(d) of Regulation (EU) 2018/1725), namely to improve consular assistance provided for EU citizens, recognised in the legal references below.

Legal references with regard to the data transfer

- GUIDELINES ON CONSULAR PROTECTION OF EU CITIZENS IN THIRD COUNTRIES, 10109/2/06 of 26.10.2010 in particular Point 7.3 and 12.5 thereof
- EU-US Summit 2021 statement 'Towards a renewed Transatlantic partnership' https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf
- Article 39 of the Framework Agreement between the European Union and its Member States, of the one part, and Australia, of the other part (to enter into force in October 2022)
- Article 24 of the Strategic Partnership Agreement between the European Union and Its Member States, of the one part, and Canada, of the other part
- 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance.)
- 2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) Text with EEA relevance

Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021)4800) (Text with EEA relevance)

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 any inaccurate or incomplete personal data. 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 have questions concerning the processing of your personal data, you may address them to the Data Controller via the functional mailbox:

COOL@eeas.europa.eu

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

Lawfulness

The processing of 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].

Legal references

- Article 35 TEU, Article 20 (2) (c), Article 23 and Article 221 TFEU
- Article 11, Article 12, Article 13 of the Council Directive (EU) 2015/637 of 20 April 2015 on the coordination and cooperation measures to facilitate consular protection for unrepresented citizens of the Union in third countries and repealing Decision 95/553/EC

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., in particular Articles 3(1), 4(3), 5 (9) and (10) and Article 10.

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 10 working days after the deletion of a user account was requested either by the users themselves or the CoOL user administrators from EU Member States. Hard deletion of data (deleted users' access) is performed simultaneously each time a user access is deleted in CoOL.

Security measures

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.

Specific security mesures

The application is hosted by 4C Strategies, the processor, within secured hosting environment located in Sweden. Unauthorised reading, copying is addressed by 4C Strategies infrastructure architecture and back-up procedures. Preventing any unauthorised memory inputs as well as unauthorised disclosure, alteration or erasure of stored personal data is addressed at the application level using appropriate authentication and authorisation. The application uses 'https' standard protocol for secure systems. The application has auditing and logging procedures implemented, allowing to track user actions. The application level authentication and authorisation ensures that

- personal data being processed on behalf of third parties can be processed only in the manner specified by the controller
- during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation and that
- authorised users of the data-processing system can access no personal data other than those to which their access right refers.

The processor, 4C Strategies selected for the tool provides sufficient assurance to act on behalf of EU Institutions pursuant to Article 29 of Regulation (EU) 2018/1725 and to implement the necessary technical, organisational and data protection measures as well as to verify the effectiveness of those measures.

Users and recipients of data, when granted access to the Consular Online (CoOL) portal are requested to handle data with due care and are informed that by using the portal their names, functions and contact details will be accessible by other users, including Member States and abovementioned like-minded third country representatives in order to fulfil the objective to provide and disseminate information on consular situation matters, and in particular in the case of a consular crisis affecting EU citizens.

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.