EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA IN THE CONTEXT OF RECORDED

INTERVIEWS AND EXCHANGES

FOR PUBLICATIONS AND COMMUNICATION MATERIAL ORGANISED BY THE EEAS SERVICES

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the External Action Service (EEAS). 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 processes 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 is to ensure proper management of personal data collected through interviews or recorded exchanges with data subjects. Such data may be used for publication material, studies, research and social media content.
The collection of personal data during interviews will be carried out in a respectful and transparent manner. Participation in the interview is entirely voluntary, and individuals will be explicitly informed about the purpose of the interview and their rights as data subjects. They will have the option to decline or withdraw consent at any time without facing any negative consequences.
The data collection may happen though recorded exchanges, live streaming, written or verbal answers to interviews carried out in person or via video and tele-conferencing tools.

In case of virtual exchanges/interviews:

Use of Video and Tele-conferencing (VTC):

Video and Tele-Conferencing may be used in order to meet the objectives outlined above in various situations when personal presence at an interview is not feasible. The EEAS may therefore use a virtual platform (including, but not limited to Webex, MS Teams, Skype for Business) to host the interviews. If technically feasible, even if participants have a personal account for the respective platform they do not need to sign in to the platform to participate in the event, signing in is only necessary for the event organiser. Following the indications provided in the invitation may suffice (link or Meeting ID and password to join and the way of indicating their identity).

When video-conference tools are used, including but not limited to CISCO-Webex, Microsoft Teams, Microsoft Skype for Business service providers may become data processors. The aim to use these tools is to guarantee a feasible technical solution to participate at the interviews organised online. Further information on data that the IT tools (online platform providers) may process and details of the type of data they may obtain about you and your equipment, and what they use that data for as well as the Privacy Policy of these third party processors are available on their websites, as follows:

- WEBEX – CISCO Privacy Data Sheet
- Microsoft Teams Security compliance and privacy; MS TEAMS Privacy Statement
- Skype for Business Privacy

Recording or live-streaming:

It may be requested to record or live stream meetings with the iterviewees, in order to keep track of the answers and reuse them for publication material, studies or for other communications activities of the EEAS/EU Delegation.
In cases where an interview is live streamed or recorded, this will be indicated in the meeting invitation, or in any other way by means of a consent form.
Consent will be requested in advance, irrespective of the length of the recording/live streaming or if the interview takes place in person or thorugh VTC tool.
Consent culd be asked in different ways:

- The interviewee(s) and the participants will be asked to fill out and sign a consent form before the recording.
- Depending on the VTC platform used, a notification of the recording will appear:
    - Through a pop-up window that will be displayed automatically before the live streaming/recording feature is activated.
    - In case such consent collection is not envisaged by the VTC provider in use, the participant's consent will be obtained by asking for it formally in a written form through the chat-box of the VTC tool. The participants will provide it by sending an 'I AGREE TO THE LIVE STREAMING/RECORDING" text via the chat function. This part of the chat will be extracted and saved to document the informed consent.
    - Consent can be provided during registration or in reply to the invitation or at the beginning of the interview in a written form.

3. DATA PROCESSED: What data do we process?

Personal data will be collected during interviews, used and kept only to the extent necessary for the purposes above. Data, including personal data, that may be processed, are the following:

- Contact Information: To facilitate the interview process and maintain communication with the interviewee, we may collect basic contact details such as name, email address, and phone number. This information is only used for interview scheduling purposes and will not be used for any other purposes unrelated to the research.

- Demographic Information: In some cases, we may collect certain demographic information about the interviewee, such as age, gender, and nationality. This data is gathered solely for research purposes and, unless explicit consent by the individuals to use their data publicly, it will be treated with strict confidentiality and will be used in aggregate form, ensuring individuals' identities are protected.

- Opinions and Viewpoints: During the interview, the individual will have the opportunity to share their thoughts, beliefs, and perspectives on the topics discussed. These opinions will be recorded and analyzed to gain insights into broader trends or issues. Unless specific consent by the data subjects, this data will not be linked to the individual's demographic information.

The personal data collected during interviews will be used for research and analysis purposes, as described above, and they may appear in an anonymized way in publications. However, with the explicit consent of the interviewees, the interview material, including opinions and viewpoints, may be utilized in additional ways, such as publication in reports, and other publications, including social media platforms.
If interviewees provide consent for such extended usage, we may share videos or insights from the interviews with the public, including sharing selected interview excerpts.
We prioritize transparency throughout the process, and interviewees will be clearly informed about the potential for publication and social media usage during the consent process.

4. DATA CONTROLLER: Who is entrusted with processing your data?

The data controller determining the purpose and means of the processing is the European External Action Service (EEAS).

The data controller for each individual meeting/event/interview is the organising entity from or on behalf of which you received the invitation.

Strategic Communication, Task Forces and Information Analysis - SG.STRAT.2

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

The recipients of your data may be:
- Designated organising and interviewing staff of the EEAS/EU Delegation
- Contractors performing their duties under a contract with the EEAS
- Assigned staff of other EU institutions and other assigned organiser team members, if required
- Security and other partners, contractors, service providers on behalf of the organiser
- Participants, Interpreters, Technical staff if relevant
- EEAS staff and other EEAS Intranet users (if data published on the EEAS intranet)
- General public (if data made public on the internet, the EEAS or EUvsDisinfo website or social media platform).

The specific recipients of your data will be listed in the consent form outlining the purpose of the activity to which the data subjects are taking part.

In case of publication on Social Media:
The EEAS and the EU Delegations use social media to promote and inform about their communication priorities through widely used and contemporary channels. Videos or pictures may appear on the EEAS/EU Delegation webpage and social media channels, or the EUvsDisinfo website and social media channels (Facebook/Meta, Instagram, LinkedIn, X [ex Twitter] and YouTube). Consent for publication on social media will be asked prior to the interview. The use of social media does not in any way imply endorsement of them or their privacy policies. We recommend that users read the Facebook/Meta, Instagram, LinkedIn, X [ex Twitter], and YouTube privacy policies which explain their data processing policy, use of data, users' rights and the way how users can protect their privacy when using these services.

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 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 consented to recording a session, you have the right

to withdraw your consent to its use by notifying the data controller. In this case, the EEAS will make every effort to remove your contribution from the recording.

The withdrawal of your consent will not affect the lawfulness of the processing carried out before you have withdrawn the consent. 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:

To contact the data controller please use the mail address you received the invitation from or the Strategic Communication, Task Forces and Information Analysis at SG-STRAT-2@eeas.europa.eu

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

Lawfulness of the data processing

Participation in the interviews is based on your consent [Article 5(1)d of Regulation (EU) 2018/1725] and you can deny your consent, withdraw your consent at any time or deny to respond to any question.
Data processing for EU communication activities, inclusing publication of videos, insights or excerpts from the interviews shared with the public, is based on your consent. If you do not wish for some personal data, including photos or videos, to be published on the web, you also have the option to deny and withdraw your consent at any time.

General 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)
Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy of June 2016.

8. TIME LIMIT - DATA STORING: For what period and how we process your data?

Our aim is to keep your personal data not longer than necessary for the purposes we collect them. After the interview or exchange in question, your data are kept as long as follow-up actions to the event are required.
Personal data will be deleted five years after the last action in relation to the interview. Personal data may be kept for information and historical, statistical or scientific purposes for a longer period of time including the publication on the EU Delegation webpage and EEAS Intranet or EEAS website with appropriate safeguards in place and prior explicit consent of the data subjects.

Security of data
The EEAS, the EU Delegation and FPI strive to ensure a high level of security for your personal 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. In case a service provider is contracted, as a processor, the collected data may be stored electronically by the external contractor, who has to guarantee data protection and confidentiality required by the Reg. (EU) 2018/1725. These measures also provide a high level of assurance for the confidentiality and integrity of the communication between you [your browser] and the EEAS/EU Delegation. Nevertheless, a residual risk always exists for communication over the internet, including email exchange. The EEAS relies on services provided by other EU institutions, primarily the European Commission, to support the security and performance of the EEAS website.

Security of the online platforms used for video-conferencing is assured by the service providers. The security policy of data processors, such as CISCO-Webex, Skype, MS Teams can be verified at the relevant websites: WEBEX – CISCO Privacy Data Sheet , Microsoft Teams Security compliance and privacy; MS TEAMS Privacy Statement , Skype for Business Privacy

As CISCO-Webex, MS Teams and Skype for Business and other online platform providers enhance their security and privacy features, the EEAS keeps under constant review the technical measures it takes to protect your personal data.

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.