

# EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

## FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO EVENTS AND MEETINGS ORGANISED BY EEAS SERVICES & EU DELEGATIONS BY MEANS OF VIDEO AND TELECONFERENCING (VTC) TOOLS

### 1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the External Action Service (EEAS) including the Delegations to the European Union. 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 and the 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 is to ensure proper organisation and management of events and meetings by an EEAS service in Headquarters and/or EU Delegations in order to disseminate information among participants and to the public, enhance cooperation, networking, facilitate exchange fora, often web-based. It is also intended to further contact participants and to promote EU Public Diplomacy permitting to engage individuals in public diplomacy activities and other events. You can find information on the legal basis in Point 7 of this Privacy Statement.

Description: Coordination, organisation and management of meetings and events, incl. workshops, info days, seminars, etc.

- 'Events and meetings' include in-house and external location workshops, information days, conferences, seminars, expert meetings, visits and other events or meetings related to the functioning of and the tasks entrusted to the EEAS.
- The organisation of 'events and meetings' includes the management of contact and mailings lists for invitations, handling of participation requests and feedbacks, the preparation and distribution of preparatory materials, meeting reports, news items and publications to the participants as well as travel arrangements, accommodation and the entry to the premises with access control as well as using VTC platform for facilitating online events and meetings. In the framework of organising meetings and events the following processing may take place:
  - to send e-mails, invitation letters; collect names, postal/e-mail addresses, phone/fax numbers, by electronic/manual means; publish participants lists and distribute it to participants and organisers;
  - to collect and manage lists and mailing-lists for meetings, news and publications;
  - if relevant, to follow up reimbursement of travel expenses and payment of daily allowances
- Publication and communication activity related to 'events and meetings' for dissemination purposes includes the publication of information about the event/meeting on the EEAS Intranet and/or on the EEAS website and the facilitation of photos and videos, web streaming, audio or video recording during the event/meeting.

Different ways to manage the meetings include the following:

- Meetings and events organised by EEAS staff internally
- Meeting and events organised by EEAS staff by using the SCIC services;
- Meetings and events organised by EEAS staff with third parties, either from the public or from the private sectors. In case the meeting or event is organised with the support of an external company (contractor) processing personal data, including the provision of an online platform, a data protection clause should be inserted in the service contract.

The meetings of Council instances chaired by the EEAS are out of the scope of this processing activity.

The publication of images concerning internal events on the intranet of the EEAS is also out of scope of this processing activity.

#### 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 a meeting is not feasible. The EEAS may therefore use a virtual platform (including, but not limited to Webex, Zoom, MS Teams, Skype for Business) to host events, workshops and webinars. Registration may be required through EU tools like EU Learn or through an Outlook invitation from the event manager or the VTC platform. 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).

Participants can be requested to indicate only their first name and, if relevant, their organisational entity or – for external participants – their organisation, Member State or international organisation and the initial of their last name. Participants may opt to provide their full name.

Your personal data will not be used for automated decision-making including profiling.

## Recording of event sessions

**To record events, in particular when given via videoconference, may be necessary to use the event presentations in other events or to share it with participants who cannot participate in real time.** The presentations can be made available by different means.

- for future reference used by participants and course organisers and for communications activities of the EEAS/EU Delegation;
- for interested individuals who were unable to attend.
- In cases where an event is recorded, this will be indicated in the invitation, or in any other way at registration. Information will be provided as to how and when consent to the recording can be provided.
- **Consent will be requested in advance, irrespective of the length of the recording.** Depending on the VTC platform used, consent may be asked in various ways:
- Through a pop-up window that will be displayed automatically before the recording feature is activated (e.g. Zoom). The consent will be saved automatically in the reports available to the licence manager in the professional account/web portal of the VTC tool. The report on consent will be exported to document the consent.
- 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 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 training invitation or at the beginning of the training in a written form, e.g. on the presence list.

If the VTC tool used enables to limit the recording to the trainer only, this option will be chosen in case not all participants agree to the recording.

If possible, you, as a participant, will have the opportunity to choose a non-recorded alternative. At an event via VTC, where no alternative session is feasible, participants who do not consent to be recorded should indicate a pseudonym rather than their clear name when they connect to the session and switch their camera and microphone off as well as refrain from asking questions through their microphone. Questions can be put using the chat function. That part of the chat will not be stored, whereas the part of the chat indicating the consent from participants who agreed to the recording is extracted and saved.

When video-conference tools are used, including but not limited to CISCO-Webex, Microsoft Teams, Zoom, 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 meetings 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](#)
- [ZOOM Privacy](#)
- [Microsoft Teams Security compliance and privacy; MS TEAMS Privacy Statement](#)
- [Skype for Business Privacy](#)

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

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

- Identification and contact data, including name, title, profession, function, postal/e-mail address, phone numbers and any other administrative information and contact details
- Identity/passport number and validity, nationality, country of residence, gender, date of birth or any data necessary for access control purposes to the EEAS/EU Delegation premises (under EEAS Security Directorate/ EU Delegation responsibility) or to external premises including EU venues
- Biography or CV if needed
- Information about transport and accommodation if foreseen; financial information and banking details for the purpose of reimbursement of travel expenses/allowances together with supporting documents (e.g. tickets)
- Dietary requirements and special assistance when applicable, processed in a secured manner for the sole purpose of accommodating special needs or dietary requests
- Login credentials in case of online registrations

**Please note that due to recording of parts or all of the training, workshop or webinar, even if you do not share either your audio or your video, your screen name may appear in recordings.**

II. In addition, data are also collected during the event and processed for documenting the event and the purpose of informing the public, promoting EU public diplomacy in communications and publications:

- Photos, audio or video filming and web streaming of speakers, participants or organisers as well as feedbacks, surveys, reports and other information about the event/meeting

Disclaimer:

The organisers waive responsibility of videos/photos taken, shared, published by participants or other individuals, including journalists and other members of the press not contracted by the EEAS/EU Delegations.

III. Data collection by websites: when using online applications, websites may apply dynamic tools such as cookies for technical functioning, gathering statistics and providing a personalised experience for them as users. More information about cookies can be found on the specific websites.

#### 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 event under the supervision of the Director/Head of Division/Head of Delegation is the organising entity [event/meeting organiser] from or on behalf of which you received the invitation.

EEAS.SG.STRAT – Directorate responsible for Strategic Communication and Foresight

Contact entity: SG.STRAT.1 - Strategic Communications 1

Division in charge of Communications Policy & Public Diplomacy

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

The recipients of your data may be:

- Designated organising staff of the EEAS/EU Delegation
- 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 website or social media platforms)

Data will not be shared with third parties for direct marketing. Under certain conditions outlined in law, we may disclose their information to third parties, (such as the European Anti-Fraud Office, the Court of Auditors, or law enforcement authorities) if it is necessary and proportionate for lawful, specific purposes. Service providers will process data on documented instructions and on behalf of the EEAS/EU Delegation in accordance with Article 29 of Regulation (EU) 2018/1725. More information on how the provider processes personal data on the website of the contracted organisation. Data will not be communicated to third parties, except where necessary for the purposes outlined above.

##### **Social Media**

The EEAS and the EU Delegations use social media to promote and inform about events and meetings through widely used and contemporary channels. In addition to the [EEAS Webpage](#) or [FPI webpage](#), videos may be uploaded to the [EEAS YouTube](#) channel and links from our website can appear on [Twitter](#), [Instagram](#), [Flickr](#), [LinkedIn](#) and [Facebook](#). The use of social media does not in any way imply endorsement of them or their privacy policies. We recommend that users read the [Twitter](#), [Flickr](#), [Facebook](#), [Instagram](#), [LinkedIn](#) 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 functional mailbox of the event  
[the mail address you received the invitation from]**

SG.STRAT – Directorate responsible for Strategic Communication and Foresight

Contact entity SG.STRAT.1 - Strategic Communications 1 Communications Policy & Public Diplomacy

[\(STRATEGIC-COMMUNICATIONS@eeas.europa.eu\)](mailto:STRATEGIC-COMMUNICATIONS@eeas.europa.eu)

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

##### Lawfulness of the data processing

The processing of your personal data related to events/meetings organised by the EEAS or EU Delegations, as mandated by the Treaties, specifically by articles 5, 11, 20, 21-40, 42, 43 of the of the Treaty on European Union (TEU) and 2 (4) and (5), 15, 205, 220-221, 326 – 334 of the Treaty on the Functioning of the European Union (TFEU), 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.

Further 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) and Shared Vision, Common Action: A Stronger Europe - [A Global Strategy for the European Union's Foreign and Security Policy](#) of June 2016 as well as Council Conclusions of October 2016 where the Council of the European Union emphasises "the need of joining up efforts in the field of public diplomacy including strategic communication, inside and outside the EU, to speak with one voice and ultimately promote its core values".

At the same time, data processing for EU communication activities and publications, if applicable, is based on your consent requested separately [Article 5(1)(d) of Regulation (EU) 2018/1725] for the following:

- o photos, video recordings and web streaming related to events/meetings which may be shared in EU communications (see point 3)
- o the processing of the personal data relating to the dietary requirements and/or access requirements
- o attendance list containing their name, affiliation and contact details which may be shared among participants
- o permanent contact list created and shared internally among EEAS services for the purpose of promoting EU activities/events and disseminating information.

If you do not wish for some personal data, including photos, to be published on the web, you also have the option not to provide consent. Participants that choose this option, depending on the type of event and available resources, may take a seat in non-photographed areas, may follow the event/meeting by web streaming or wear an identifier including a colour code on stickers or badges. You can withdraw your consent at any time and you also have the option to give consent only to one or more data processing activities.

#### **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 event, your data are kept as long as follow-up actions to the event are required. Reports and other material containing personal data are archived according to e-Domec policy.

Personal data will be deleted five years after the last action in relation to the event. Personal data may, however, be part of a contact list shared internally among EEAS services for the purpose of promoting future EU activities and disseminating information. The privacy statement on public diplomacy initiatives is also available on the EEAS website. Financial data related to the event will be kept for a maximum period of 10 years after the end of the event or meeting for auditing purposes. Sensitive personal data relating to dietary and/or access requirements will be deleted as soon as they are no longer necessary for the purpose for which they have been collected in the framework of the meeting or event, but no later than within 1 month after the end of the meeting or event. 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.

##### 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. Physical copies are stored in a secured manner. 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, Zoom, can be verified at the relevant websites.

- [WEBEX – CISCO Security and Privacy](#); [CISCO – WEBEX meeting Privacy Data Sheet](#); [CISCO Privacy Data Map](#)
- [MS Teams Security Compliance Overview](#); [Microsoft cloud recording](#)
- [Microsoft Privacy Supplement](#); [MS Security Guide for Skype for Business online](#)
- [Zoom security](#); <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>

As CISCO-Webex, Zoom, 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](mailto: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](mailto:edps@edps.europa.eu).