European Union
EXTERNAL ACTION

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF
PROCESSING PERSONAL DATA RELATED TO

MEETINGS AND EVENTS RELATED TO THE FIMI-ISAC

ORGANISED BY THE EEAS

IN PERSON OR 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) as well as to the services of the European Commission. 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 data processing is to ensure you are aware of how your data are processed for the organization of events and meetings in relation to the **Foreign Information Manipulation (FIMI) Information Sharing and Analysis Centre (ISAC)**. The purpose of the data processing is to ensure proper organisation and management of the various online or in-person meetings, as well as possible events by the EEAS. This includes dissemination of information among participants to enhance cooperation, networking and facilitate exchange fora. It is also intended to further contact participants and to conduct EU Public Diplomacy engaging individuals in public diplomacy activities and other events.
You can find information on the legal basis in Point 7 of this Privacy Statement.

- The organisation of meetings and events in relation to the FIMI-ISAC 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, granting access to video-communications tools and publications to the participants.
- Possible publication and communication activity related to the above for dissemination purposes includes the publication of information about the cooperation between stakeholders on the EEAS Intranet and/or on the EEAS websites and social media accounts.

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

Video and Tele-conferencing (VTC)

Video and Tele-Conferencing will 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 to host events, workshops and webinars. Registration may be required through EU tools, such as 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 are requested to indicate 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.

In case of recording of event sessions:

To record events or meetings, in particular when provided via videoconference, may be necessary to use the presentations or to share it with participants who cannot participate in real time. The presentations can be made available:

- for future reference used by participants
- for interested individuals who were unable to attend.

In cases where a 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:

- Consent can be provided during registration or in reply to the event invitation or at the beginning of the event in a written form, e.g. on the presence list.

- Through a pop-up window that will be displayed automatically before the recording feature is activated. 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.

If the VTC tool used enables to limit the recording to the speaker/presenter/moderator only, this option will be chosen in case not all participants agree to the recording.
If possible, participants 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 full 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.

The video-conference tool Microsoft Teams used for interaction between participants may become a data processors. The aim to use this tool is to guarantee a feasible technical solution to participate at meetings organised online. Further information on data that the IT tool (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 website, as follows:
- Microsoft Teams Security compliance and privacy; MS TEAMS Privacy Statement

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. Prior consent to process certain types of data will be explicitely requested. Data, including personal data, that may be processed, could be the following:

Participants:
- Personal details: name, surname, including work position, division, e-mail address
- Contact data (e-mail, phone, address – as necessary)
- Identification name (or a pseudonym chosen by the user for online training), login credentials in case of online registrations or where required by the VTC tool
- For in-person events, nationality, passport or identity card number and its date of issue and expiry date may be collected, so that the data subjects may obtain access to the premises where the meeting/event is held
- For in-person events, financial information (such as a payment card number or bank account) may be collected for the payment of fees of the meeting/event or for possible reimbursements in the case of participation in person
- Dietary requests (if any) or specific access requirements in the case of participation in person
- Data processed by service providers – like logs (please see last paragraph of point 2)
- Pictures, videos
- Data submitted by the participants when connecting to the training session using the registration or VTC tool (if you do not consent to recording, you can provide a pseudonym, providing an e-mail address is optional)
- Your contribution during the training session (recording of the session), if the you consent to the recording, including the extract of the chat providing proof of the consent given by the nominal text of "I agree to the recording"
- Your VTC conversation history in the group chat

Speakers/Moderators:
- Data categories detailed above
- Material shared and contribution during the training session (presentation, handout, etc.)
- Data submitted by the trainers during registration for the VTC tool (name and other data (e.g. email address) as required by the tool (data are kept to the necessary minimum)
-

Please note that in case of 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 case of in-person events, data may be also collected in the form of 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. Prior consent will be requested.

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 you as a user. 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.

The EEAS SG.STRAT.2 - Strategic Communication, Task Forces and Information Analysis as Data Controller is responsible for managing the personal data processing under the supervision of the Head of Division and is the controller entity engaging with Data Processors such as EC DG DIGIT, being the manager of the online conferencing platform (point 2), and the service provider ICF Next (Belgium) which will manage external communications with participants and stakeholders related to FIMI-ISAC

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

In general, access to your personal data is provided to the EEAS staff responsible for carrying out this data processing activity and to authorised staff of EC DG DIGIT and ICF Next according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.
The recipients of your data may be:

- Designated organising staff of the EEAS
- European Commission assigned staff members designated for the tasks to be implemented (EC DG DIGIT)
- 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 organizer (ICF Next Belgium - Avenue Marnix 17, 1000 Brussels, Belgium: consultancy enterprise for the organisation of the FIMI-ISAC events)
- Participants, interpreters, technical staff if relevant
- Microsoft Teams tool is used for meeting management purposes, the service provider operating the tool and its processors will be also recipient(s) of your personal data.

Personal data is not intended to be transferred to a third country or an international organisation.

Data will not be communicated to third parties, except where necessary for the purposes outlined above and will not be used for direct marketing. Under certain conditions outlined in law, we may disclose your 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 abide by contractual clauses for the protection of your data and will process data on documented instructions and on behalf of the EEAS/EU Delegation in accordance with Article 29 of Regulation (EU) 2018/1725.

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
STRAT-DATA-ANALYSIS@eeas.europa.eu

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

Lawfulness of the data processing
The processing of personal data related to FIMI-ISAC meetings and events organised by the EEAS is necessary for the performance of a task carried out in the public interest [Article 5(1)(a) of Regulation (EU) 2018/1725], as mandated by the Treaties, in particular by articles 5, 11, 20, 21-40, 42, 43 of the of the Treaty on European Union (TEU) and 2 (4) and (5), 205, 220-221, 326 – 334 of the Treaty on the Functioning of the European Union (TFEU).
The processing is also necessary for archiving purposes. 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 the data subject.
Further 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) and Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy of June 2016 and 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 is based on your consent requested separately [Article 5(1)(d) of Regulation (EU) 2018/1725]. Your consent is required for:

- photos, video recordings and web streaming related to events which may be shared in EU communications (*see details in paragraph "Recording of events given via videoconference" of point 2*)
- the processing of your personal data relating to your dietary requirements and/or access requirements
- sharing the attendance list containing your name, affiliation and contact details among participants and with the host/presenter of the event
- 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, you also have the option not to provide consent to any of the above or to give consent only to one or more data processing activities. You can withdraw your consent at any time.

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

Personal data will be deleted two years after the last action in relation to the event/meeting. 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. Possible 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 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 with appropriate safeguards in place.

Security of data

The EEAS 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 and the EEAS. 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 the data MS Teams can be verified at the relevant websites.

- MS Teams Security Compliance Overview; Microsoft cloud recording

As MS Teams 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.