

Privacy Statement¹ – Cisco WebEx

1. Introduction

The Single Resolution Board (SRB) processes your personal data in accordance with the Regulation (EU) [2018/1725](#) (EUDPR). The privacy statement explains the reasons for processing your personal data, the way the SRB collects, handles and ensures protection of all personal data. It also specifies the contact details of the responsible SRB unit where you may exercise your rights, the SRB Data Protection Officer and the European Data Protection Supervisor (EDPS)

2. Who is responsible for processing your personal data?

The SRB is the data controller determining the purposes and means for the processing of your personal data.

The SRB's ICT Unit (Corporate-Services-ICT@srb.europa.eu) and each SRB Unit that organises the Webex meetings from or on behalf of which you receive the invitation are responsible for the processing.

Cisco is a cloud-based video conferencing solution utilized by the SRB for managing internal and external communication. Cisco, who provides the online teleconferencing platform (Webex), processes your personal data on behalf of the SRB. For further details on how your personal data are processed via Webex, you may also read Cisco's privacy policy [here](#).

3. Why do we process your personal data?

The purposes of processing your personal data are the following:

- To support the SRB's internal and external communication, as well as the organisation and management of meetings with the use of Webex. In particular, the management of meetings may include: using Webex for facilitating online meetings, handling participation requests, distributing preparatory materials and meeting reports, developing and exchanging knowledge, publishing information about the meeting on the SRB Intranet and/or its public website, etc.
- To record online meetings via Webex. The recording occurs only for specific and limited purposes such as: (a) to draft the minutes of a meeting with significant importance; (b) to use training presentations in other trainings for future reference in order to support EU staff's learning; (c) to share event presentations with participants who cannot participate in real time

4. What are the legal bases for processing your personal data?

The legal bases for processing your personal data are the following:

- Article 5(1a) and recital 22 EUDPR: The processing is necessary for the performance of a task carried out in the public interest by the SRB -which is to support the management and functioning of the SRB,

¹ Last update on 18/01/2023

by adjusting to the new technological environment- in conjunction with the Regulation (EU) 806/2014 establishing the organisation and functioning of the SRB.

- Articles 5(1d) and 7 EUDPR when the recording of Webex meetings is based on participants' consent. During the meeting registration/ invitation, information is provided to participants as to how consent to the recording can be provided. Consent can be withdrawn at any time. Participants who do not consent to be recorded are informed to: (a) indicate a pseudonym rather than their clear name when they connect to the session where possible, (b) switch their camera and microphone off, and (c) ask questions the chat function. Personal data will no longer be processed once consent has been withdrawn, but prior processing will remain lawful.

5. What categories of personal data are processed?

- Host registration information, e.g. name, business email address.
- Participants may be requested to indicate only their first name. 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.
- User generated information, e.g. meeting recordings, uploaded files exchanged via Webex.
- Analytics data, e.g. IP address, user agent identifier, hardware type, operation system type and version, client MAC address, meeting session information, call attendee information (including email address, IP address, username, phone number), etc.
- Information needed for technical support assistance provided by Cisco (TAC) and/or by dedicated SRB staff.

6. Who has access to your personal data?

When the SRB processes personal data for the above-mentioned purposes, the following persons may access your personal data on a strict need-to-know basis:

- Dedicated SRB staff members.
- Cisco's employees for the provision of the online teleconferencing platform and for technical support assistance.
- Staff of other EU institutions, if required.
- SRB staff and other SRB Intranet users (if data published on the SRB Intranet).
- General public (if data made public on the internet, the SRB website or social media platforms).
- Under certain conditions outlined in law, personal data may be disclosed 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.

7. In which third country personal data could be transferred?

Personal data (including User Information, Host & Usage Information, and User-Generated Information) processed by Webex Meetings is stored in the region located in Amsterdam.

Certain exceptions to Webex data residency rules exist and cross border transfers of personal data may still occur when a user:

- engages in collaboration with users outside of their region;
- requests technical support through Cisco TAC (in which case the information that a user provides within the initial TAC request may be transferred outside the region);

Besides, Cisco stores the following personal data in the United States of America (USA):

- Cisco Webex analytics platform data, which utilizes host and usage Information
- Billing information

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data outside the European Economic Area such as EU Binding Corporate [Rules](#) and EU Standard Contractual [Clauses](#). For further information, please also read the Cisco Webex [Privacy Statement](#)

8. How long will the SRB keep your personal data?

The SRB keeps your personal data for the time necessary to fulfil the purposes mentioned at part 3:

- After the event, personal data are kept as long as follow-up actions to the event are required. Any locally stored personal data will be deleted in five days by the meeting organiser in line with the event's privacy statement.`
- Host and usage information are kept for a maximum period of 3 years.
- If the meeting organiser records an online meeting, the records are saved in the Cisco data centers and the person who records the meeting is in charge of deleting the record or is there an automated routine that deletes the file after five days. At the end of the five days retention period (communicated in the meeting invitation), all the copies of the records are deleted in the Cisco data centers or moved to the SRB ICT infrastructure in accordance with the SRB security policies, guidelines and standards.
- Chat messages exchanged among participants during the meeting are deleted after it ends

9. What are your data protection rights?

You have the right to access your personal data and correct any data that is inaccurate or incomplete. You have also (with some limitations) the rights to delete your personal data or to restrict the processing of your personal data in line with the Regulation (EU) 2018/1725.

10. Who can you contact in case of queries or requests?

You can exercise your rights by emailing the SRB Unit that organises the online meeting (please find the contact details at the relevant meeting invitation) and/or the SRB's ICT department at Corporate-ServicesICT@srb.europa.eu.

You may contact the SRB's Data Protection Officer at SRB-DPO@srb.europa.eu for questions relating to the protection of your personal data..

11. Addressing the European Data Protection Supervisor

If you consider that your rights under Regulation (EU) 2018/1725 have been violated as a result of the processing of your personal data, you have the right to lodge a complaint with the [European Data Protection Supervisor](#) at any time.