ZOOM Tutorial

Understanding & managing security and privacy issues

to ensure continuity of teaching

and working from home

zoom

UNIVERSITÉ DE GENÈVE

In this tutorial, you will learn:

- How to better understand and approach issues related to personal data on Zoom
- How to increase security when scheduling a meeting or class on Zoom
- How to guarantee safety during a course
- Some good practices about privacy

Management of personal data

Zoom is a US-based platform. It records and stores personal data and uses it once anonymized. A privacy policy applies.

Zoom is certified by the *Swiss-United States Personal Data Shield* (more information on this framework here).

Zoom does not have access to its users' Facebook data.

Zoom can be used without installing any application.

Principles for a secure meeting

- **Do not share confidential information/documents on Zoom;**
- **Do not share meeting links on social media** (when more people have the link, it is more likely that someone could use it for bad purposes);
- **Make sure that the computer/tablet/smartphone used is secure** (by updating regularly your OS, Zoom application, and antivirus software); and
- **Manage cookies:** only accept necessary cookies.

How to increase security when scheduling a meeting (1/2)

To protect meetings and webinars against trolls / hackers or unwanted content, you should set up **a password** (see next slide to learn how to do this)**.**

It is also possible to **exclude** non-UNIGE users, but this will prevent external contributors from participating.

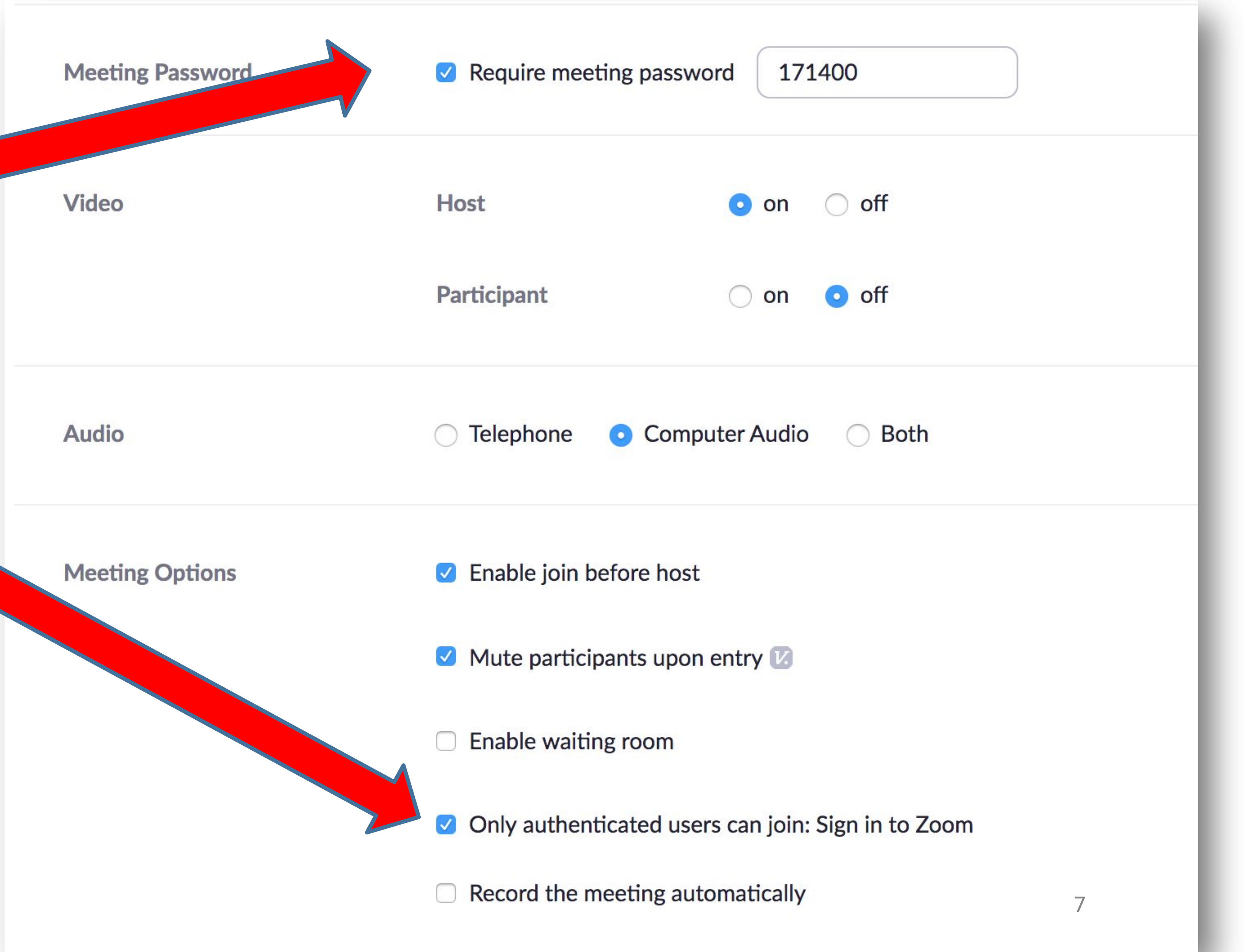
A key principle is to ask participants to **never** share the link or the password of a Zoom meeting in a public forum (e.g., social media).

Security when scheduling a meeting (2/2)

To activate **the password** when creating the meeting

To **exclude** non-UNIGE participants

See tutorial #1 to learn how to schedule meetings.



Meeting Password — ☑ Require meeting password 171400

Video — Host ● on ○ off

Participant ○ on ● off

Audio — ○ Telephone ● Computer Audio ○ Both

Meeting Options

☑ Enable join before host

☑ Mute participants upon entry

□ Enable waiting room

☑ Only authenticated users can join: Sign in to Zoom

□ Record the meeting automatically

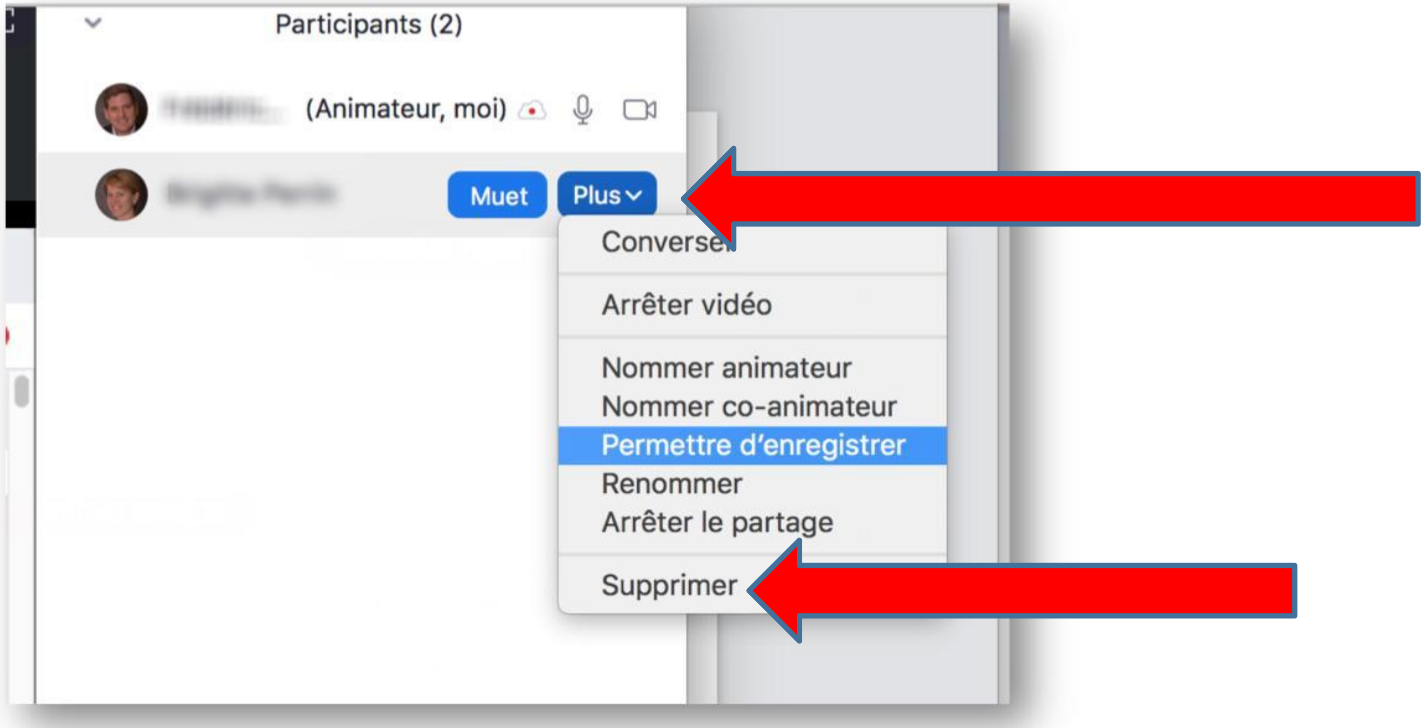
How to guarantee security during a meeting (1/2)

In case of inappropriate content appearing in a conversation, make sure that you immediately exclude those responsible (see next slide to learn how to do this).

Then inform zoom@unige.ch.

If they are UNIGE users, write down their names so that awareness of good practices can be raised.

How to guarantee security during a meeting (2/2)



In the toolbar at the bottom of the screen, click on Participants.

A side window will appear. Next to the troublemaker, click More then Delete (Supprimer if in French).

Warning: excluded people are indefinitely banned: deleted participants cannot come back into the meeting.

Principles of privacy (1/2)

It is strictly forbidden to record meetings on Zoom without the prior and explicit consent of their participants, neither locally nor in the cloud.

You can assume consent during semi-public teaching events (course, seminar, etc.) when participants know that the video will be available after the meeting has ended.

See tutorials 1 and 3 (on the dedicated page the UNIGE website) for more details on how to record a Zoom meeting. See the following slides in this tutorial to learn how to use advanced settings about recording confidentiality.

Principles of privacy (2/2)

Host

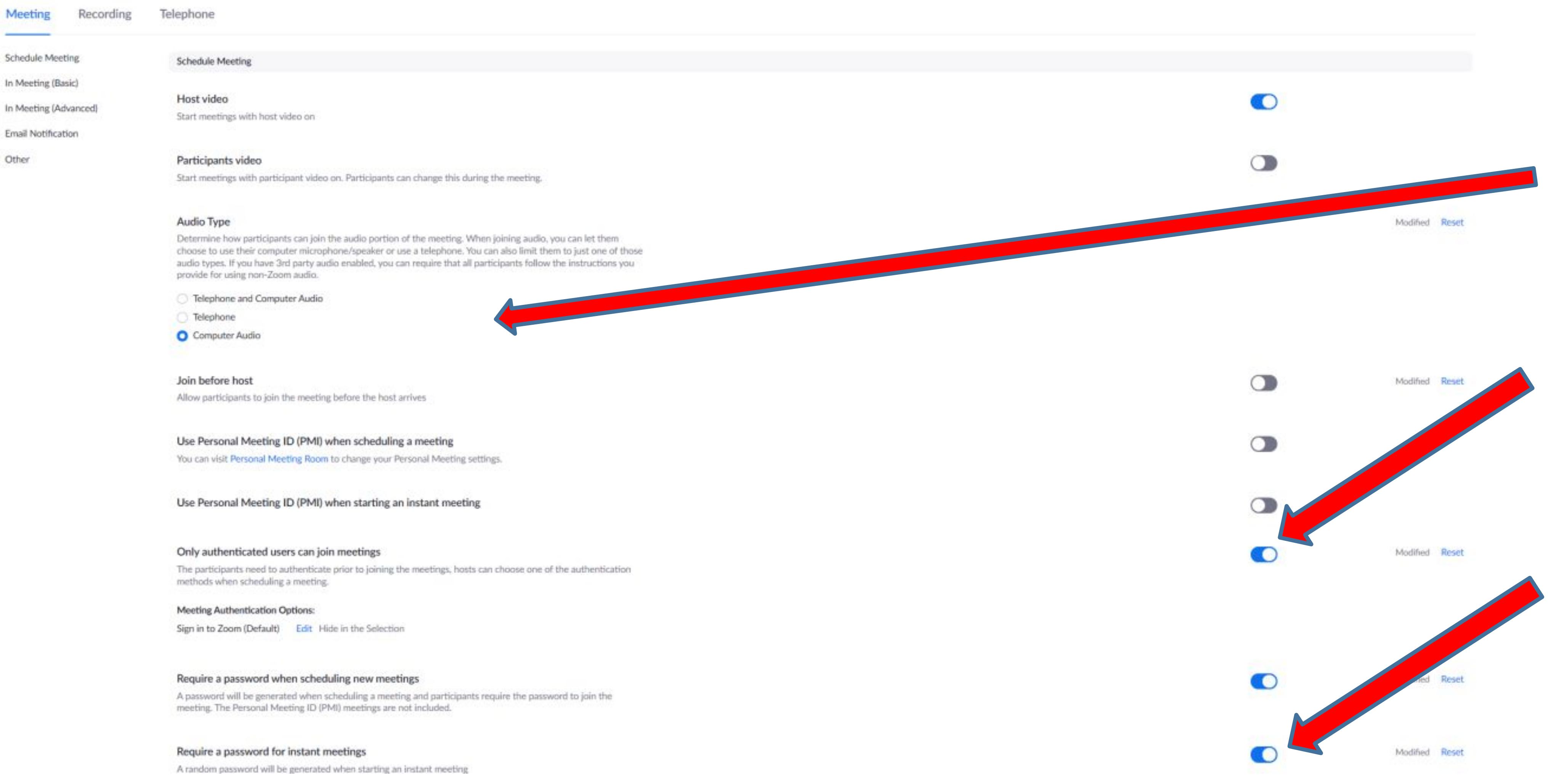
- When the host chooses to record the meeting, they must inform participants, and collect their consent as indicated by the privacy policy. A beep and a symbol appear when recording. The host must warn the participants and ask them to actively consent.

- When the host activates the attention tracker (which checks whether the meeting window remains active on participants' computer), they are also required to inform participants (as per privacy policy).

- Make sure to manage settings in your Zoom user account.

UNIVERSITÉ DE GENÈVE

Privacy: Settings (1/4)



Schedule Meeting

Host video ☑
Start meetings with host video on

Participants video ☐
Start meetings with participant video on. Participants can change this during the meeting.

Audio Type
Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.

○ Telephone and Computer Audio
○ Telephone
● Computer Audio

Join before host ☐
Allow participants to join the meeting before the host arrives

Use Personal Meeting ID (PMI) when scheduling a meeting ☐
You can visit Personal Meeting Room to change your Personal Meeting settings.

Use Personal Meeting ID (PMI) when starting an instant meeting ☐

Only authenticated users can join meetings ☑
The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

Meeting Authentication Options:
Sign in to Zoom (Default) Edit Hide in the Selection

Require a password when scheduling new meetings ☑
A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a password for instant meetings ☑
A random password will be generated when starting an instant meeting

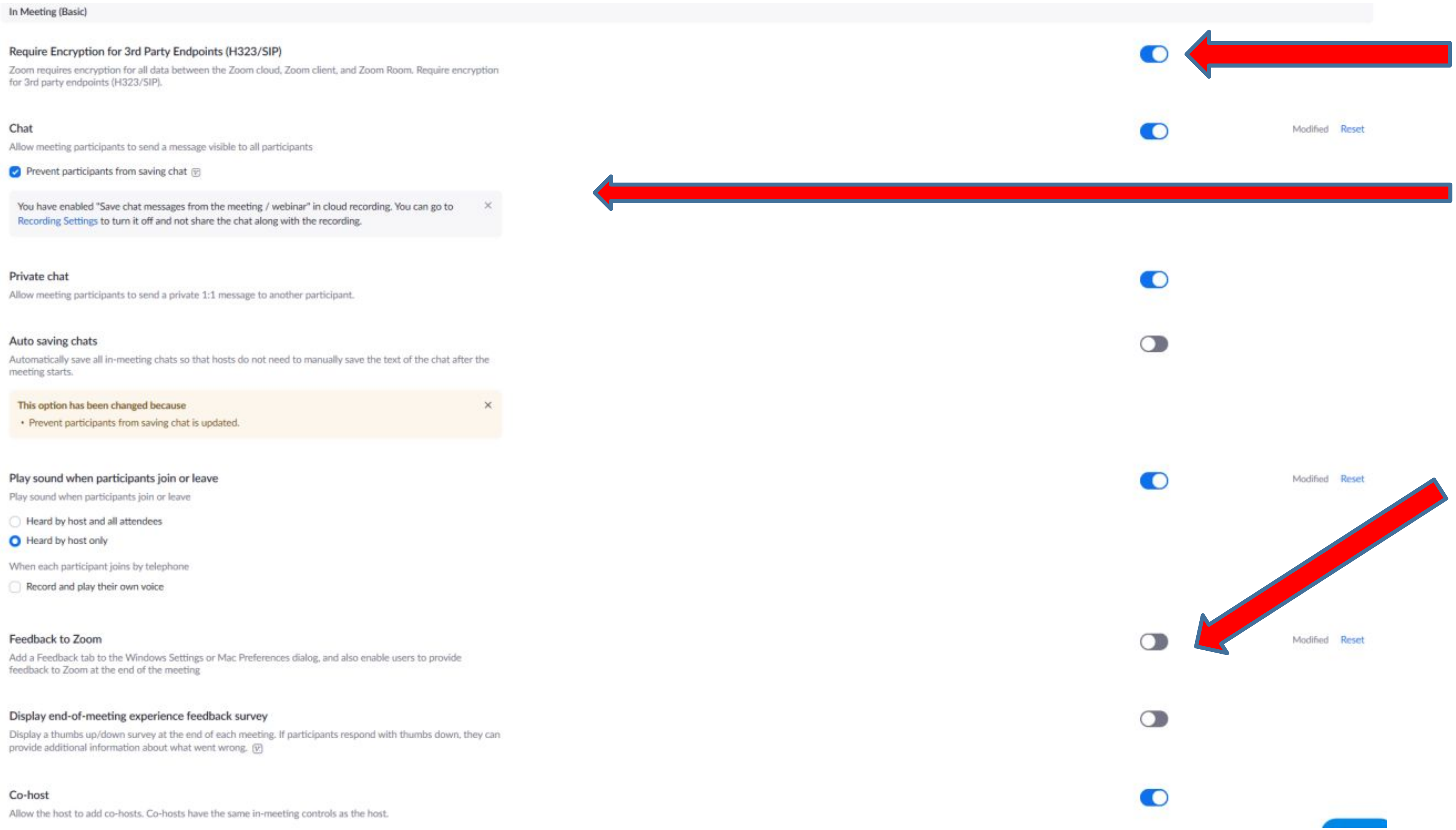
1. Restrict to “Computer Audio” if possible in order to avoid having an unencrypted conversion.

2. Restrict to authenticated users if possible, in order to decrease the risk of bots / trolls and hackers

3. Organize meetings with passwords whenever possible

UNIVERSITÉ
DE GENÈVE

Privacy: Settings (2/4)



In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

☑ Prevent participants from saving chat

You have enabled "Save chat messages from the meeting / webinar" in cloud recording. You can go to Recording Settings to turn it off and not share the chat along with the recording. ×

Private chat

Allow meeting participants to send a private 1:1 message to another participant.

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

This option has been changed because ×

- Prevent participants from saving chat is updated.

Play sound when participants join or leave

Play sound when participants join or leave

○ Heard by host and all attendees

● Heard by host only

When each participant joins by telephone

□ Record and play their own voice

Feedback to Zoom

Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting

Display end-of-meeting experience feedback survey

Display a thumbs up/down survey at the end of each meeting. If participants respond with thumbs down, they can provide additional information about what went wrong.

Co-host

Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.

1. Force encryption of third-party audio methods if possible

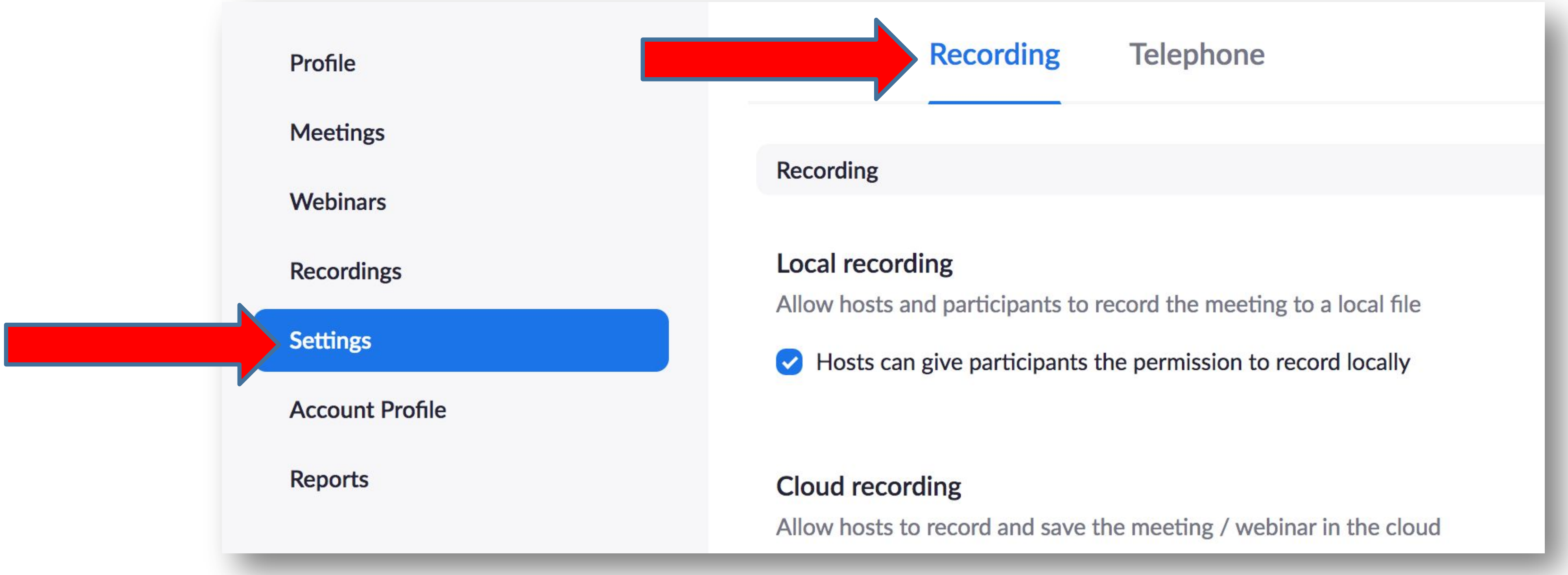
2. Block chat backups if necessary for better privacy

3. Disable feedback to Zoom in order to limit the amount of shared data

UNIVERSITÉ DE GENÈVE

Privacy: Settings (3/4)

To ask participants for their consent, or to manage who will have access to the recordings, go to Settings then Recording. See next slide.



Recording

Local recording

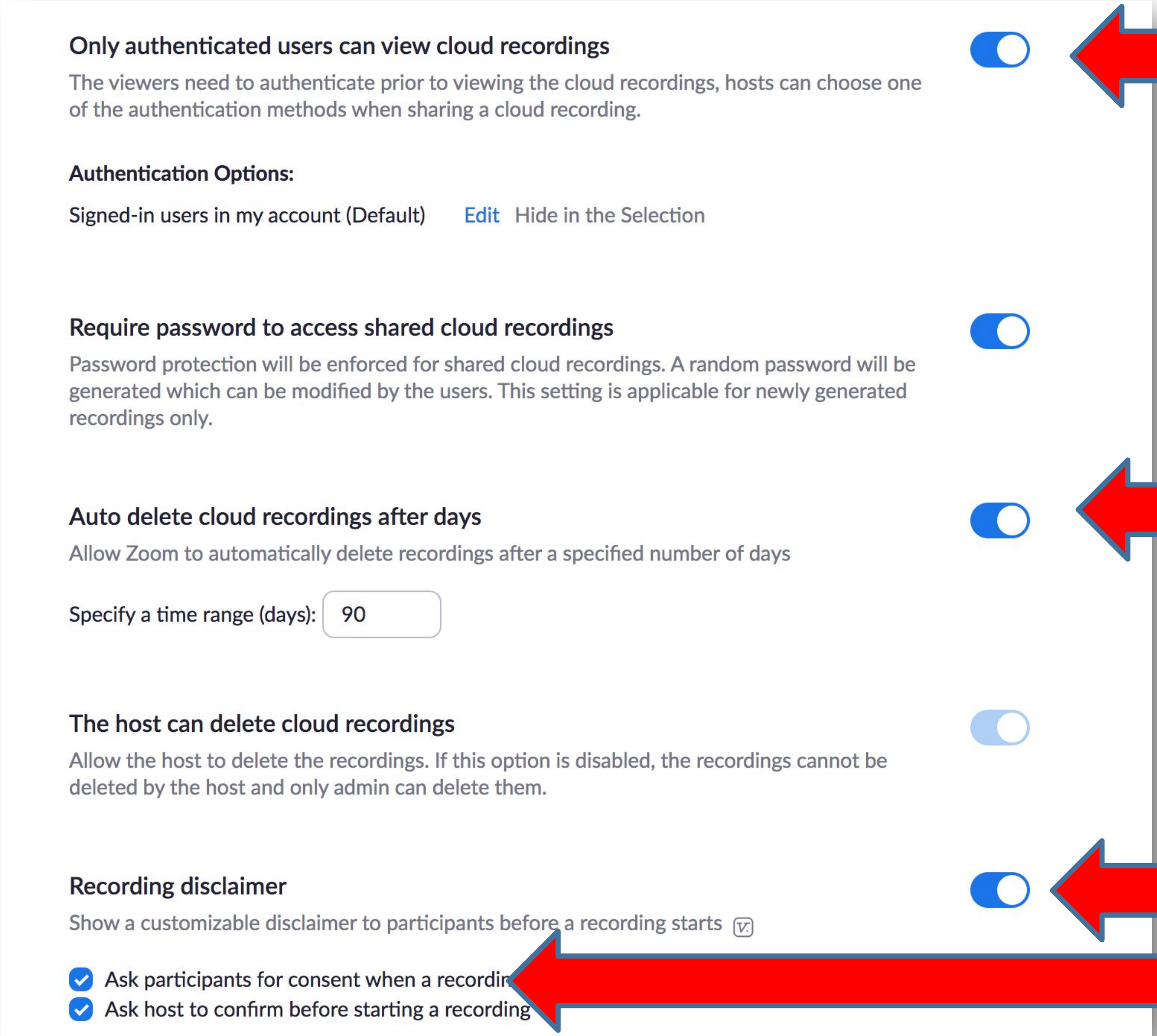
Allow hosts and participants to record the meeting to a local file

☑ Hosts can give participants the permission to record locally

Cloud recording

Allow hosts to record and save the meeting / webinar in the cloud

Privacy (4/4)



Only authenticated users can view cloud recordings

The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.

Authentication Options:

Signed-in users in my account (Default) Edit Hide in the Selection

Require password to access shared cloud recordings

Password protection will be enforced for shared cloud recordings. A random password will be generated which can be modified by the users. This setting is applicable for newly generated recordings only.

Auto delete cloud recordings after days

Allow Zoom to automatically delete recordings after a specified number of days

Specify a time range (days): 90

The host can delete cloud recordings

Allow the host to delete the recordings. If this option is disabled, the recordings cannot be deleted by the host and only admin can delete them.

Recording disclaimer

Show a customizable disclaimer to participants before a recording starts

☑ Ask participants for consent when a recordi

☑ Ask host to confirm before starting a recording

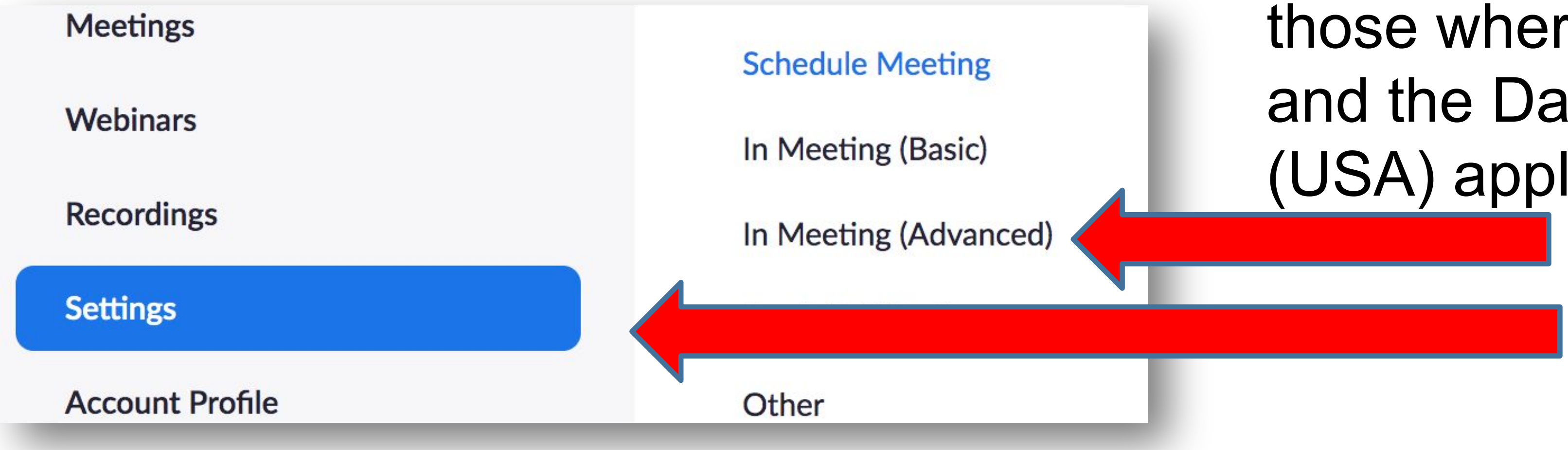
Limits access to recording to UNIGE users

Determines when records will be deleted

Enables collecting consent of participants

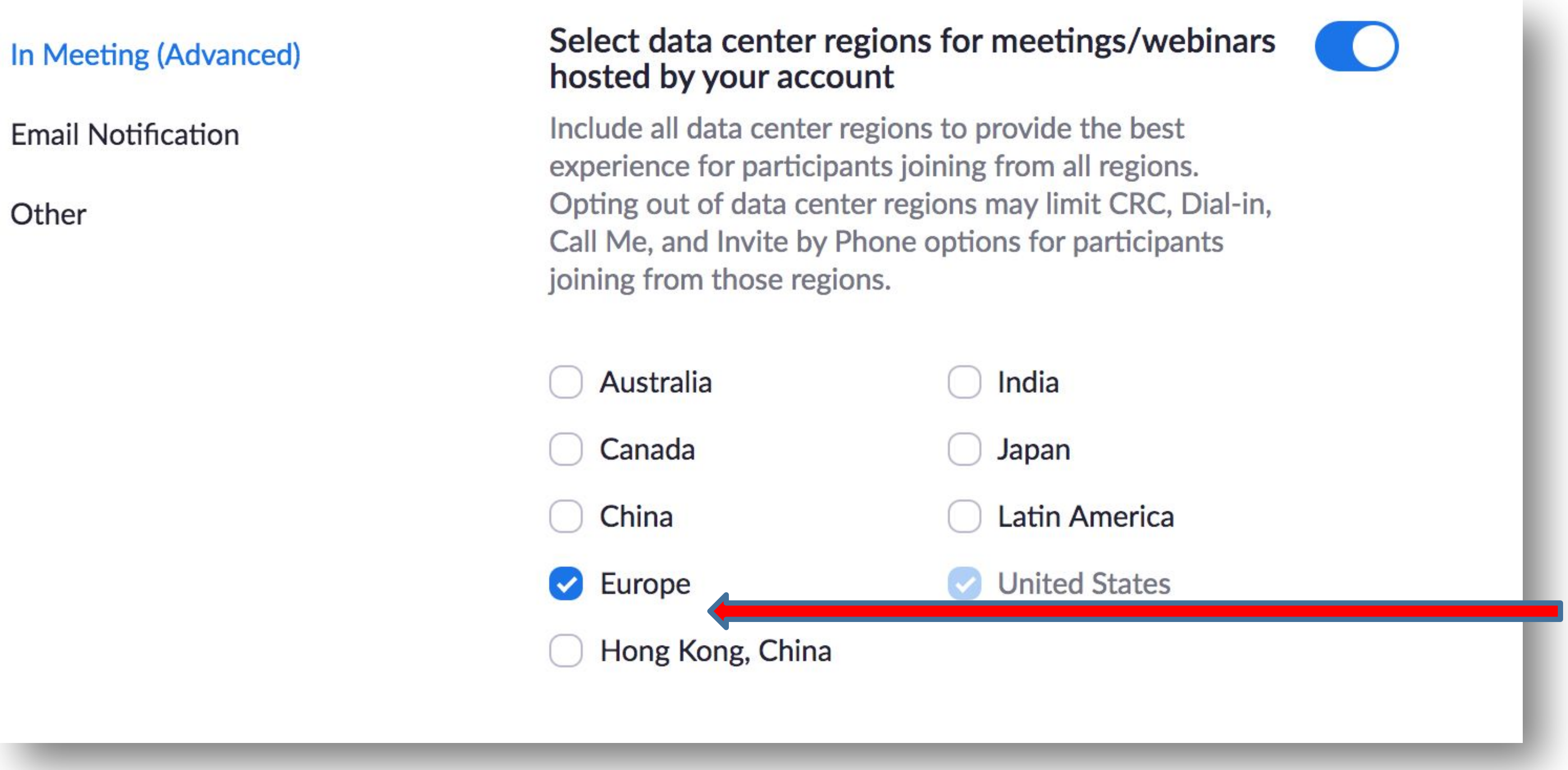
Privacy and GDPR (1/2)

Zoom allows you to limit the geographical area where the data is processed. It is therefore possible to limit these areas to those where the GDPR (Europe) and the Data Protection Shield (USA) apply.



To modify these geographical settings, click Settings, then in Meeting (advanced)

Privacy and GDPR (2/2)



In Meeting (Advanced)

Email Notification

Other

Select data center regions for meetings/webinars hosted by your account

Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

□ Australia	□ India
□ Canada	□ Japan
□ China	□ Latin America
☑ Europe	☑ United States
□ Hong Kong, China	

Restrict data processing to Europe (in addition to Zoom servers in the United States)

When in doubt

Contact zoom@unige.ch

You have learned the basics of security and privacy on Zoom!

Other tutorials are available on our dedicated page.