Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Data Protection and Information Commissioner
FDPIC

Measures for the safe use of audio and video conferencing systems

The coronavirus pandemic is showing people all over Switzerland and, indeed, the world how a single event can completely change our surroundings and the way we do things. From one day to the next, it was no longer possible for us to meet friends and family in person, or exchange information with colleagues and hold meetings at our offices. In our work and in our private lives, we have abruptly switched to digital solutions such as audio or video conferencing systems. Despite the rush with which business meetings, children's 'visits' with their grandparents, or even parties have been moved online, we must not forget how important information security and data protection continue to be. This information sheet deals with exactly these issues, and is aimed at all user groups – both in business and in private life.

The first part of this information sheet lists measures we recommend you take to ensure that the audio or video conferencing system you are using during this crisis is safe. You should make sure to reassess your choice of service – either immediately or at a later point in time – by carrying out a risk analysis according to data protection criteria. If necessary, choose a different service more suitable to your needs. This information sheet also contains a list of points to observe when setting up and introducing an audio or video conferencing system, to ensure it complies with data protection guidelines.

Measures to take when using an audio or video conferencing system:

Do not share your meeting IDs publicly
A meeting ID (also called conference ID) is a unique number assigned to a specific conference call. Do not share your meeting IDs publicly online, for example on social media, as this makes it possible for uninvited people to join.

Lock your meetings and never use the same meeting ID twice
Never use the same meeting ID for two consecutive conference calls, and lock your current call as soon as everyone has joined. This prevents people from your next conference call from accidentally joining too early and listening in.

Use passwords wherever possible
You can further protect your conference call with a password. When inviting people to your meeting, it is best to send them the meeting ID and the password in two separate emails.

Always keep an eye on who is participating in your conference call
You should regularly check who is on your call. If an unfamiliar participant pops up, you should ask them to identify themselves.

Always let participants know in advance if you plan to record the conference call
Participants must be explicitly informed in advance that the conference call will be recorded

(e.g. sound, video). They must be given the chance to voice their concerns without fear of negative consequences, and to leave the call if they do not want to be recorded.

Beware of phishing
If you are sent a link to a video conference by email or through social media, you should contact the sender and verify their identity before you join their meeting. Never open links or attachments sent to you by someone you do not know!

Cover your camera when you are not using it and check what is visible in the background
We recommend you cover your camera when it is not in use to prevent others from spying on you. Before you start your video conference, check to see what will be visible to the other attendees (e.g. a bare wall, printouts, or a whiteboard with information on it). Some video conferencing systems also let you blur the space behind you.

Screen presentations / sharing your screen
Only show what is relevant to the conversation. Close all unnecessary windows, tabs and content. Wherever possible, avoid showing your desktop and only present the relevant program. You can also set up a separate desktop specifically for this purpose that does not show any files or links.

Check the service provider's privacy policy
Some providers pass on personal information or metadata to third parties, for example call duration, location, attendee identification or the number of attendees. If your audio or video conferencing provider wants to share your personal information with a third party, this needs to be stated in their privacy policy. Read the privacy policy and contact the service provider if anything is unclear.

You should consider the following points when choosing and preparing to use an audio or video conferencing system:

Check the service provider's reputation
Search online for information on user satisfaction, helpful features and known security issues. When in doubt, always choose an established provider.

Check the service provider's privacy policy
Check the provider's privacy policy for their guidelines on sharing personal information. If you are using a video conferencing system offered by a provider from outside Switzerland or the EU, or a provider who passes on information to 'third countries', you should check whether that country/provider offers a suitable level of protection (e.g. 'privacy shield certificates' in the case of US companies), or if the provider is offering any other guarantees (standard data protection clauses).

How the provider handles metadata
You should confirm that your provider does not collect, process for their own purposes, or pass on metadata to third parties. In addition to the already mentioned metadata on call duration, location, identities and number of meeting attendees, this may also concern email addresses in your contacts, your cell phone's brand and model, or the browser you are using.

Data encryption
Data should be protected at all times, both when 'in transit' between the sender and the

recipient, and when saved on either device. At the very least, data should be encrypted when it is being shared – ideally with end-to-end encryption.

Physical safety
Where are the service provider's data centres located, and do they meet your security requirements? In particular with services that store data centrally, it is important to make sure all of their data centres are secured round the clock, checked regularly and protected against physical breaches. Servers located in Switzerland or the EU are generally preferable.

Security controls
Some video conferencing systems offer advanced fraud protection to identify failed login attempts. This way, intrusion attempts such as someone repeatedly trying to guess your meeting ID can be identified and stopped.

If possible, conference call participants should be notified when a person joins or leaves the call with (distinctive) signals. Systems that let you see how many people are on your call, or that identify all attendees, should be preferred. Some systems allow you to delegate a meeting monitor or moderator.

Adjust your privacy settings
Adjust your default privacy settings to prevent your information from being used in ways you do not want. Provide users within your organisation with instructions on how to select privacy-friendly settings.

There are also important points to consider when introducing an audio or video conferencing system:

Do you need to register or sign in?
Browser-based systems that do not require you to install software, register or sign in can be very useful. However, this makes it much more difficult to identify participants and is therefore not suitable for communicating within a company.

Prevent unwanted app access
Many apps – especially those for mobile devices – access more of your personal information than they actually need. You should adjust your privacy settings to prevent your information from being used in ways you do not want, and configure, document and monitor app permissions in detail (limit permissions to those functions needed to perform the service).

Establish guidelines for your company
If there are no guidelines in place, employees will not know whether or not they can privately use an audio or video conferencing system while at work. Unless use is expressly restricted or prohibited, employees are entitled to assume that occasionally using such a system is allowed and will not be monitored by their company.

Information on monitoring and recording within your company
Unlike the guidelines mentioned above, which are not compulsory, employers are required to clearly communicate to their employees if they will be monitoring or recording audio or video conferences, as this is considered an invasion of privacy ('good faith principle', Art. 4 para. 2 Federal Act on Data Protection).

Bern, April 2020

Further information

A list of digital collaboration products, April 2020, Data Protection Commissioner of the Canton of Zurich (in German only)