Privacy and security at Zoom

Version 021

In order to be able to continue teaching and providing teaching support, the UvA recently purchased online meeting and teaching software program Zoom. In response to media reports, a number of employees asked if Zoom is safe to use and sufficiently safeguards for the privacy of its users.

Zoom was purchased because a replacement for physical teaching had to be provided at short notice. There was no suitable alternative on this scale and within this term. Nonetheless, the UvA is aware of questions and concerns about privacy and security around Zoom. Consequently, we have set up Zoom while paying the greatest possible attention to these aspects. The UvA is currently carrying out more research, which may result in additional measures.

Zoom was purchased because the UvA had to offer online teaching and had no suitable alternative.

Faced with the coronavirus crisis, the UvA has had to replace physical teaching with online alternatives at extremely short notice. We had to make a quick decision about the purchase of suitable videoconferencing software. The Big Blue Button interface (in Canvas) was found to offer insufficient options; as a result, the UvA opted for an additional tool to support digital teaching: Zoom.

From a functional point of view, Zoom is a good solution: it enables online meetings and teaching in groups of up to 100 people. With regard to privacy and security, Zoom obtains reasonable, but not optimal scores. Given the pressure to enable activities to continue, it was decided to purchase Zoom early and to set it up with the greatest possible attention to privacy and security, while also looking more closely at, and tackling, any privacy and security risks.

We have set up Zoom for use within UvA while paying maximum attention to privacy and security.

Privacy and security have been essential principles in equipping Zoom for UvA use. We want to limit the privacy impact on users as much as possible; where we can, we work in accordance with ‘privacy by default’.

- Zoom has limited access to our data: the program does not store video sessions, while chats and documents shared between users are encrypted (and so cannot be viewed by Zoom) and are stored for a limited period only.
- Organisers of video sessions (hosts) cannot collect additional information about participants in the session (e.g., monitoring activities during the session).
- The UvA administrators of Zoom must access the service via two-step verification: an additional security measure, which makes it even harder for malicious parties to gain access.
- For most users, access is managed by SURFconext rather than by Zoom. This gives the UvA greater control over login details.

We advise users on how to use Zoom with maximum privacy and security awareness.

The most crucial settings are mandatory and cannot be changed. Users do have the option to toggle a number of other settings. As the default settings are the most privacy-friendly, we recommend that users do not change these settings. Guidance has been drawn up with regard to using Zoom in education, e.g. for oral examinations. (see appendix 1).

Until the UvA has carried out further research, it is recommended not to use Zoom for assessment interviews, for interviews between student psychologists and students, or for researching and interviewing vulnerable groups.

We are currently carrying out further research into the privacy and security aspects of Zoom, which may result in additional measures.

Upon the purchase of Zoom, the CISO (head of information security) and FG (head of privacy) carried out a limited privacy and security risk analysis. Zoom was found to score reasonably, while presenting privacy and security risks. We have also put questions about this to Zoom (appendix 2). Privacy and security specialists are currently carrying out a more in-depth privacy and security analysis, on the basis of which the UvA may introduce additional measures to address risks.

Bijlage 1: Handreikingen voor docenten

Recommendations For Teaching. In principle, the advice is data minimization. Teachers are advised to not record more than is necessary and to only share data which is essential for lessons. In all cases, students should not be portrayed. This, by default, implies the following practices:

- Only Share the audio file of any class recordings on Canvas (this can be made separately in Zoom).
- If a video is shown, only the teacher should be shown
- Consider what images you are showing and whether these images are necessary for recording
- Consider the retention period of storage on Canvas

If there are specific situations, other than official assessments, in which students' images must be shared - the teacher must write down why this is necessary, what s/he will do with the data, and the intended length of storage. This should then be submitted for the Examination Board.

Recommendations For Assessment. In view of current circumstances, there is a legitimate need to use a video conferencing system for *some* forms of assessment – limited to oral examinations- since there is no alternative. If an assessment requires recording, Zoom may be used for this assessment. Consult your OER, examination board, and/or your supervisor to determine if two teachers need to be present, and if the oral exam needs to be recorded. If the latter is the case, then make sure to inform the student in advance, but no consent is needed. The UvA Data Protection Officer (Functionaris gegevensbescherming) shared the following opinion.

> Original NL Opinion: *Gezien de (uitzonderlijke) omstandigheden is er op dit moment voor online toetsing sprake van gerechtvaardigd belang. Op dit moment is, alles afwegende, deze vorm van toetsing de meest geschikte variant. Daarbij worden vanzelfsprekend maatregelen genomen om de privacy te waarborgen. Als de toetsing moet worden opgenomen, hoeft er op dit moment ook geen toestemming te worden gevraagd aan de studenten. Als de student het zo niet wil dan zal hij/zij moeten wachten tot alles weer is genormaliseerd, aangezien er op dit moment geen alternatieve mogelijkheid kan worden geboden. Voor vragen over privacy kan contact worden opgenomen met avg@uva.nl. Voor zorgen of klachten over privacy kan contact worden opgenomen met de Functionaris gegevensbescherming, Miek Krol, fg@uva.nl*
>
> EN Translation: *In view of the (exceptional) circumstances, there is currently a legitimate interest for online assessment. At the moment, all things considered, this form of assessment is the most suitable variant. Naturally, measures are taken to guarantee privacy. If the assessment has to be recorded, no permission needs to be requested from students at this time. If a student does not wish to partake in an online exam, s/he will have to wait until everything has returned to normal as there is currently no alternative available. For questions about privacy, please contact avg@uva.nl. For privacy concerns or complaints, please contact the Data Protection Officer, Miek Krol, fg@uva.nl.*

Recommendations for Communication About Zoom Use to Students. We recommend that every faculty determine their best manner of communicating about the use and privacy policies of Zoom to their students in a manner and form which best fits their student body. FNWI has prepared a letter (in EN / in NL) that they will share with their students which may be an appropriate model for your own faculty.

Bijlage 2: Correspondentie UvA — Zoom over privacy en security

In onderstaande correspondentie staan de vragen die de UvA heeft gesteld over de privacy en security van Zoom, en de antwoorden die Zoom daarop heeft gegeven.

UvA: What are the details of Zoom's privacy policy? Is it true that Zoom can collect users' physical address, phone, job title, credit and debit information, Facebook account IP address, OS and device details?
Zoom: Zoom only collects user data to the extent necessary to provide technical and operational support, and to improve our services. Zoom must collect technical information like users' IP address, OS details and device details in order for our service to function properly. When user data is used for service improvement, it is completely anonymized and aggregated immediately upon collection in order to protect users' identities and privacy.

Does Zoom sell user data to third party companies?
No. Zoom does not sell user data of any kind to anyone.

Does Zoom share data with Facebook or have access to a user's Facebook content?
Zoom does not share user data with Facebook, and Facebook cannot access any personal data. Zoom does not have access to any user's Facebook content.

Do users own their data? Does Zoom have rights to data if it passes through the platform?
Customers and end users retain all ownership of any files, documents, recordings, chat logs, meeting subject and attendees, transcripts, and any other information they may upload to Zoom's service in connection with use of the service. Zoom collects and processes this only at the direction of the customer and end user for no other purposes than the provision of Zoom's services.

Can you define "user-generated information"? It's referred to in Zoom's privacy policy, but there is no definition for the term.
"Customer Content" (how Zoom refers to "user-generated information" in contract documents) is any data or content originated by a customer or an end user, and stored or transmitted using Zoom's services. Customer Content includes files, documents, recordings, chat logs, meeting subject and attendees, transcripts, and any other information customers or end users may upload to Zoom's service in connection with their use of the service. Zoom collects and processes Customer Content only at the direction of the customer and end user for no other purposes than the provision of Zoom's services. Customers and end users retain all ownership of their Content.

Is it true person-to-person in meeting chat messages could be later sent to a user's boss after a call is recorded to the cloud?
No. Private chats are not made available to the meeting host. (Note: Chats to Everyone may be stored by the meeting host.)

Is Zoom compliant with privacy laws in other jurisdictions like the GDPR?
Yes. Zoom complies with all applicable privacy laws, rules, and regulations in the jurisdictions within which it operates, including the GDPR. Zoom's official statement can be found here.

Does Zoom have the ability to "break in" or monitor conversations, whether in real time or record a copy? Or, if a customer is recording, keep a copy? Or, in transit to storage?

Zoom does not break-in or monitor conversations in real time and places the highest priority in the operations of its suite of products and services. By default, Zoom employs in-transit and at-rest encryption for in-meeting and in-webinar presentation content. End-to-end encryption for chat is enable. If customers employ local storage of meeting recordings, Zoom does not have access to or store these local meeting recordings. Only customers can access their local meeting recordings. Zoom is legally required to work with law enforcement when there is a violation of Zoom's online Terms of Service. Zoom provides customers with a robust set of security features. Customers can learn more at https://zoom.us/security.