

 Passend zu diesem Thema enthält das Thema [Zoom](#) eine Auswahl interessanter Seiten.

Datenschutzkonforme Einstellungen


Sie haben die Möglichkeit ein Zoom-Meeting aufzuzeichnen und als Video zu speichern. Im Folgenden werden die Einstellungen beschrieben, die aus Datenschutz- und Sicherheitsgründen für die Studierenden und Sie, nötig sind.

Um die Sicherheitsmaßnahmen zu aktivieren, melden Sie sich zunächst im Browser auf Ihrem [Zoom-Konto](#) an. Klicken Sie dann in der linken Spalte auf *Einstellungen*.

Meeting

Unter *Sicherheit* stellen Sie den Schalter *Wartezimmer* auf *Aktiv*. Auf diese Weise können Sie entscheiden, wer Zutritt zum Meeting hat. 

Scrollen Sie nach unten. Unter *Bei Personal-Meeting-ID (PMI) Kenncode verlangen* klicken Sie in der Zeile *Kenncode* rechts auf das Stift-Symbol. Vergeben Sie ein Kennwort für Ihr Meeting und bestätigen Sie mit *Speichern*.

Unter *Meeting* stellen Sie unter *Besprechung planen* die Schalter *Moderatorenvideo* auf *Inaktiv*. Der Status *Inaktiv* wird immer durch einen grauen Schalter angezeigt. 

Stellen Sie den Schalter *Teilnehmern Beitritt vor dem Host gestatten* auf *Inaktiv* und stellen Sie auch den Schalter bei *Zu Beginn eines Meetings die persönliche Meeting-ID (PMI) verwenden* auf *Inaktiv*. Auf diese Weise wird ein zufälliger Link zum Meeting generiert, der nicht beliebig oft kopiert werden kann. Scrollen Sie weiter nach unten.

Stellen Sie den Schalter *Alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten* auf *Aktiv*.

Unter *In Meeting (Grundlagen)* finden Sie den Schalter *Verschlüsselung für Endpunkte*. Für noch mehr Sicherheit stellen diesen auf *Aktiv*. 

Auch die Chat-Funktionalität kann individuell konfiguriert werden. Um mit den Teilnehmenden zu chatten, stellen Sie den Schalter *Chat* auf *Aktiv*. Aus Datenschutzgründen *Verhindern* Sie aber, dass *Teilnehmer den Chat speichern* durch ein Häkchen und Klick auf *Speichern*. Damit auch Studierende ohne Datenschutz-Einwilligung Fragen stellen können, sollte der Schalter *Privater Chat* auf *Aktiv* sein.

Um Störungen zu vermeiden, sollte *Ton abspielen, wenn jemand einsteigt oder geht* auf *Inaktiv* gestellt werden.

Mithilfe der *Bildschirmübertragung* können Sie Anwendungen auf Ihrem Bildschirm den Teilnehmenden zeigen. Der Schalter sollte auf *Aktiv* stehen.

Auch Teilnehmende können mit Ihrer Erlaubnis ihren Bildschirm allen anderen zeigen, wenn Sie bei *Wer kann freigeben?* die Option *Alle Teilnehmer* und bei *Wer kann die Freigabe starten, wenn eine andere Person die Freigabe verwendet?* die Option *Nur Host* wählen.

Scrollen Sie weiter nach unten und nehmen Sie im Abschnitt *In Meeting (Erweitert)* erweiterte Einstellungen vor. Ein *Breakout Session* ist sehr gut für Gruppenarbeiten geeignet.

Alle wichtigen Einstellungen im Reiter *Meeting* sind damit erfolgt. Weitere Einstellungen können Sie optional vornehmen.

Aufzeichnung

Scrollen Sie nun ganz nach oben und klicken auf den Reiter *Aufzeichnung*.

Stellen Sie den ersten Schalter *Lokale Aufzeichnung* auf *Aktiv*, aber deaktivieren Sie das Häkchen vor *Die Hosts können den Meetingteilnehmern die Erlaubnis erteilen, lokal aufzuzeichnen*. Damit entziehen Sie den Teilnehmenden das Recht zur Videoaufnahme.

Nun sind alle Einstellungen für ein sicheres und datenschutzkonformes Zoom-Meeting vorgenommen. Die Teilnehmenden können jetzt selber entscheiden, ob sie bei der Aufzeichnung gesehen (Video einschalten) und/oder gehört (Mikrofon einschalten) werden wollen.

Ende-zu-Ende-Verschlüsselung

Das Videokonferenzsystem Zoom bietet seit Kurzem eine Ende-zu-Ende-Verschlüsselung an (E2EE – end-to-end encryption). Diese ist dann sinnvoll, wenn Sie sicher gehen wollen, dass das Gespräch nicht abgehört werden kann (z. B. bei Forschungsprojekten oder Vorstellungsgesprächen).

Diese E2EE sollte nicht als Default eingestellt werden, da dadurch weitere Optionen deaktiviert werden:

- Beitritt vor Host
- Cloud-Recording
- Streaming

- Breakout Rooms
- Umfragen
- Private Chats
- Reaktionen

Außerdem sind manche Telefonanlagen mit der Technik nicht kompatibel.

Es empfiehlt sich daher die E2EE nur zu nutzen, wenn diese wirklich nötig ist.

E2EE aktivieren

Um die E2EE zu aktivieren müssen Sie folgendermaßen vorgehen:

- Klicken Sie auf *Meeting*
- Im Bereich *Sicherheit* aktivieren Sie die Option *End-to-End-Verschlüsselung nutzen*.
- Unter *Vorgegebene Lizenzart* wählen Sie *End-to-End-Verschlüsselung* aus.
- Benutzer mit der Basis-Lizenz benötigen ggf. eine Verifikation über eine SMS.



- Speichern Sie die Einstellung.

Sobald Sie jetzt ein Zoom-Meeting hosten, ist dies E2EE verschlüsselt. Dies erkenne Sie auch an dem Symbol in der linken oberen Ecke.



Um die Verschlüsselung zu überprüfen klicken Sie auf „Verifizieren“ und vergleichen Sie mit den Teilnehmenden den Code, der dort angezeigt wird.



From:

<https://wiki.zil.haw-landshut.de/> -

Permanent link:

https://wiki.zil.haw-landshut.de/doku.php?id=zoom:datenschutzkonforme_einstellungen

Last update: **21042026, 10:24**

