

Stand 6. April 2021

Datenschutzkonforme Zoomeinstellungen

Um Zoom datenschutzkonform nutzen zu können, müssen die Grundsätze der Datenschutzgrundverordnung (DSGVO) wie Datensparsamkeit und datenschutzfreundliche Voreinstellungen so weit wie möglich umgesetzt werden. Dazu gehört auch, dass die Einstellungen für die Nutzung von Zoom entsprechend gewählt werden. In dieser Handreichung wird gezeigt, wie Sie Zoom einstellen sollten, um den Dienst den datenschutzrechtlichen Prinzipien entsprechend einsetzen zu können.

Ausführliche Anleitungen und Hinweise zur Nutzung von Zoom finden Sie unter

<https://www.leuphana.de/universitaet/entwicklung/lehre/support-tools/digitale-plattformen-und-tools/videoconferencing/zoom.html>

Die hier dargestellten Einstellungen erreichen Sie über <https://zoom.us/profile?from=client> und nachdem Sie sich mit Ihrem Account angemeldet haben.

Sollten Sie bestimmte Funktionen unbedingt benötigen, aktivieren Sie diese Optionen nur für den Zeitraum der Nutzung der Funktion. Bitte überlegen Sie vor dem Einsatz, ob Sie die Funktion tatsächlich benötigen, oder ob Sie ggf. hauseigene Tools der Leuphana nutzen können. Nach der zwingenden Nutzung stellen Sie bitte die hier empfohlenen Einstellungen wieder her. Einige Einstellungen wurde bereits von der Leuphana voreingestellt und können von Ihnen nicht verändert werden.

Sollten Sie konkrete datenschutzrechtliche Fragen zum Einsatz von Zoom haben, können Sie sich gerne an das Datenschutzmanagement (datenschutz@leuphana.de) wenden.

Ihr Team des Datenschutzmanagements



Beim Anberaumen neuer Meetings Kenncode verlangen

Bei der Planung eines Meetings wird ein Kenncode erzeugt, den die Teilnehmer zum Beitritt benötigen. Meetings mit Personal-Meeting-ID (PMI) sind nicht betroffen.



Vom Administrator gesperrt

Das sind vom Administrator gegebene Voreinstellungen, die mit Ihrer Lizenz nicht verändert werden können.

Kenncode für Sofort-Meetings verlangen

Beim Start eines Sofort-Meetings wird ein Zufallskenncode erzeugt



Vom Administrator gesperrt

Bei Personal-Meeting-ID (PMI) Kenncode verlangen



Vom Administrator gesperrt

Nur Meetings, bei denen Teilnahme vor dem Host möglich ist

Alle Meetings mit PMI

Kenncode 000000

Einbetten des Kenncodes in den Einladungslink für die Teilnahme mit einem Klick

Meeting-Kenncode wird verschlüsselt und in den Einladungslink eingefügt, so dass die Teilnehmer mit nur einem Klick teilnehmen können, ohne den Kenncode eingeben zu müssen.



Aktivieren, um Einladungslinks zu verschlüsseln.
Einladungslinks dürfen generell aber nicht verwendet werden, da mit einem Klick auf den Link auf der Zoom-Website automatisch und nicht unterbindbar Cookies gesetzt werden.

Nur berechtigte Benutzer können vom Web-Client aus an Meetings teilnehmen

Die Teilnehmer müssen sich ausweisen, bevor sie vom Web-Client aus an Meetings teilnehmen



Aktivieren, um Zugriffe durch ungewollte Teilnehmer mit Webclient zu verhindern.

Genehmigen oder sperren Sie Einträge für Benutzer aus bestimmten Bereichen/Ländern

Sie können festlegen, ob Benutzer aus bestimmten Bereichen oder Ländern an Meetings/Webinaren auf Ihrem Konto teilnehmen können, indem Sie sie auf die Freigabe- oder Sperrliste setzen. Das Sperren von Bereichen kann die Optionen "CRC", "Einwahl", "Mich anrufen" und "Per Telefon einladen" für Teilnehmer sperren, die aus diesen Bereichen beitreten.



Aktivieren, um Zugriffe von Teilnehmern aus anderen Ländern zu verhindern.



End-to-End-Verschlüsselung nutzen

Beim Anmelden oder Starten eines Meetings wählen Sie zwischen der erweiterten und der End-to-End-Verschlüsselung. Im letzteren Fall sind einige Funktionen (z. B. Cloud-Aufzeichnung, Telefon/SIP/H.323-Einwahl) stillgelegt. [Mehr erfahren](#)



Aktivieren, um Meetings datenschutztechnisch am sichersten abzuhalten. Bitte beachten Sie, dass gewisse Funktionen technisch bedingt nicht mehr funktionieren. Überprüfen Sie vorher, ob Sie diese Funktionen wirklich benötigen und aktivieren, falls nicht.

Vorgegebene Lizenzart

Wenn der Administrator diese Einstellung sperrt, können die Benutzer den Verschlüsselungstyp für Meetings nicht ändern (d. h. geplant, sofort, PMI).

- Erweiterte Verschlüsselung ?
- End-to-End-Verschlüsselung ?

Aktivieren Sie hier die End-zu-End-Verschlüsselung erneut.

Dateiübertragung

Hosts und Teilnehmer können Dateien in einem Chat im Meeting senden. [?](#)



Um die Möglichkeiten der Übertragung von Schadsoftware zu verringern, geben Sie bitte an, welche Datentypen übertragen werden dürfen. Schließen Sie z.B. nur Office-Dokumente, PDF, oder Bilddateien ein.

- Nur bestimmte Dateitypen zulassen [?](#)
- Höchste Dateigröße [?](#)

Meetingumfrage

Host darf 'Umfragen' in Meetings einsetzen. Hosts können vor oder während eines Meetings Umfragen aufnehmen. [?](#)



Bitte verwenden Sie für Umfragen eine von der Leuphana gehostete Umfrage-Software wie Limesurvey.

Disable desktop screen sharing for meetings you host

When this option is on, users can only share selected applications and files. [?](#)



Aktivieren, um keine ungewollten Fenster oder die Desktopansicht zu präsentieren.

An Zoom melden

Man kann Meetingteilnehmer wegen unangemessenen Verhaltens dem Vertrauens- und Sicherheitsteam von Zoom zur Überprüfung melden. Diese Einstellung ist auf dem Sicherheitssymbol in der Symbolleiste der Meetingleitung festgelegt. [?](#)



Deaktivieren, da diese Funktion ein gesonderter Verarbeitungsvorgang bei Zoom in den USA ausgelöst wird.