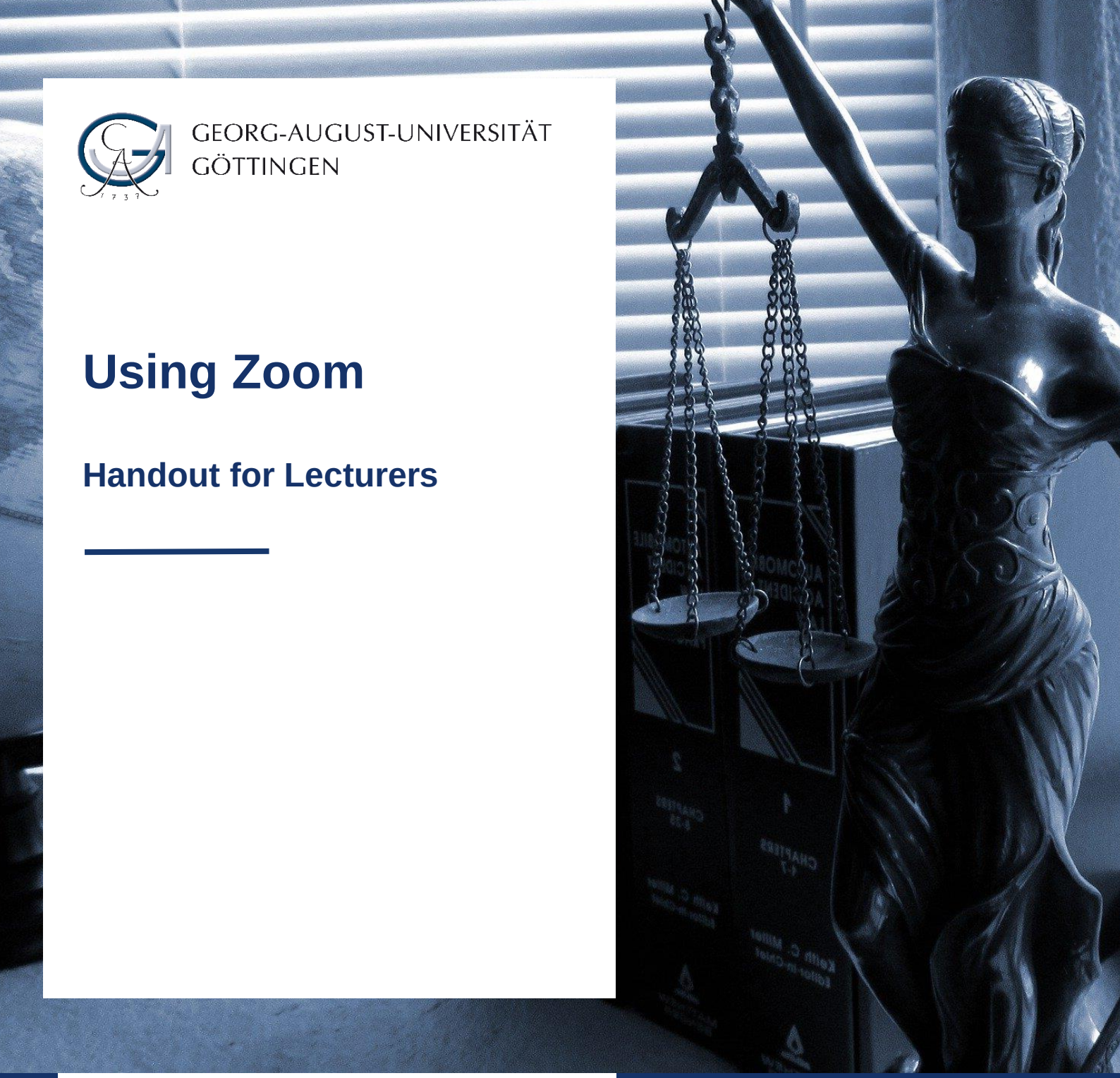

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Using Zoom

Handout for Lecturers

HANDOUT

Georg-August-University Göttingen

Team Digital Learning and Teaching

April 2020

Digitales
Lernen und Lehren

elearning.uni-goettingen.de

elearning@uni-goettingen.de

Handout for lecturers: Using Zoom

Dear lecturers,

In times of Corona, new forms of teaching and learning provide opportunities to offer courses during the current summer semester and beyond. In particular, the use of the video conferencing software "**Big Blue Button**" and "**Zoom**" for synchronous teaching scenarios as a live stream is an innovation that has rarely been used to date.

The use of web conferences is subject to Art. 13 EU-GDPR. The privacy policy of University of Göttingen can be found at https://studip.uni-goettingen.de/dispatch.php/siteinfo/show/5 (in German)
While Big Blue Button is hosted on the GWDG servers, Zoom is a commercial platform of Zoom Video Communications, Inc. in the United States. Therefore, special requirements apply here.

In consultation with the data protection officer of the University of Göttingen, we have prepared this document to inform you about aspects of data protection and data security when organizing online meetings with "Zoom". The aim is to ensure that the privacy and personal data of all those concerned at our university is protected as well as possible when using the zoom.

The legal requirements of data protection obviously limit the use of external platforms outside the university so that not everything that is desirable can also be implemented. In any case, students should be able to decide which of their data they want to make available on the platform.

Please consider the following information on data protection when designing your meetings with Zoom.

When should Zoom be used

Big Blue Button (BBB) is a conference system provided by the university. BBB is installed on the GWDG servers and offers the possibility to host meetings designed for 20-25 participants using video or approx. 50 participants using audio only. BBB also offers access that is restricted to participants who are registered for your course in Stud.IP. From the data protection point of view, the need to use Zoom is therefore only relevant if BBB is not suitable.

It is important that you do not use Zoom for meetings in which sensitive content and data are in use. For example, Zoom is not suitable for exams, personal advice, teaching with confidential content, confidential committees, etc.

How can Zoom be used

The students have the right to decide about the data that they grant access for in the Zoom system. Therefore, when using Zoom, it must be ensured that students who wish to do so can participate in the meetings without making themselves directly identifiable to the system.

Students must be given the opportunity:

- to join the conference with an alias, i.e. without registering at Zoom and without typing their real name.
- to participate without sharing their own video and/or microphone.

Our tip: If an attendance check is necessary, please clarify **aliases** with your students in advance. The alias names of your students can be collected in a list in your Stud-IP course to be used for attendance control in meetings with Zoom

Please keep in mind that the students cannot be forced to identify themselves with their real name.

Always offer students an alternative way to communicate with you

- It is important to offer an alternative channel for students where they can ask questions, if they do not willing to actively participate in the Zoom meeting with video, sound, chat, etc.In this case, you can grasp asynchronous communication channels (Stud.IP, e-mail) in order to answer the questions of those students. However, this communication path will be time-independent and not ad-hoc, like in a live seminar or lecture in Zoom.
- The exchange of course relevant information such as dates or literature lists as well as lecture notes should always be accessible via Stud.IP.

For the security of your conference room

It has been repeatedly reported that strangers dial into conferences and interfere. Usually it happens if the access data of the meeting room is made public or passed on in an uncontrolled manner.

It is therefore recommended:

- to secure your conference room with a password
- to send invitations only with the room URL, including the Meeting ID but not the password. The password can be separately communicated at participants before the beginning of the meeting
- to run the organization of your Zoom meetings from your Stud.IP course This includes informing the students about the scheduling of the meetings and the confidential access data to the zoom meeting room.
- to advise your students that they must ensure that the access data for the meeting is not disseminated elsewhere.
- to ensure that you allowed your students to use a pseudonym if they wish.

- Zoom offers you further options for securing your room (e.g. blocking a meeting, deactivating the option to join a meeting before the host does, and activating a waiting room). For more information about your Zoom meeting room security, see https://blog.Zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/

Recordings in Zoom

Zoom enables the recording of meetings. As with all forms of video recordings, this is only allowed, even in Zoom, with the consent of all identifiable persons. We have created a general handout about what should be considered when recording meetings. Zoom offers two options for recording of meetings. Therefore, **please make sure that you save recordings only locally** and not in the cloud.

Student information and personal data

According to the law, the participants should be informed about their rights under **Art. 13 EU-GDPR** before using the video conference software. We have made a declaration available (in German) at https://studip.uni-goettingen.de/dispatch.php/siteinfo/show/5
In addition, we have created a handout for students on using Zoom (link to PDF) For the summer semester 2020, we will inform students via email.

Photo credits

Picture „Justiz“ on the cover, by jessica45 in Pixabay
Icon „Homepage“ on the cover by Freepik in www.flaticon.com
Icon „E-Mail“ on the cover by Freepik in www.flaticon.com