GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

EINSATZ VON VIDEOCONFERENCING IN DER LEHRE UND BEI GREMIEN

1 Zusammenfassung

Es stellt sich durch die Coronakrise die Herausforderung, Lehre und Gremienarbeit im größeren Umfang online durchzuführen. Dafür stehen verschiedene Lösungen zur Verfügung und es stellen sich Fragen, unter welchen datenschutzrechtlichen Voraussetzungen eine der Lösungen eingesetzt werden darf und wofür empfohlen werden.

Von der GWDG werden aktuell mehrere Lösungen für die Universität angeboten. Dies ist zum einen BigBlueButton (BBB) verfügbar als meet.gwdg.de und als integrierter Teil von StudIP. Es handelt sich um lokal von der GWDG betriebene Software-Lösung. Daneben gibt es Zoom als externe Cloud Lösung, wofür eine Lizenz für die Universität und Universitätsmedizin erworben wurde. Daneben gibt es weitere Angebote, wie DFNConf, Jitsi Meet, Cisco WebEx, MS Teams, WebToGo etc.

Vom Grundsatz her lautet die Empfehlung aus datenschutzrechtlicher Betrachtung die Nutzung von BigBlueButton zu bevorzugen, wo immer dies sinnvoll möglich. Zoom als kommerzielle Plattform kann benutzt werden, wenn die Inhalte des Meetings keine besonders schützenswerten Informationen enthält und die Teilnehmer keine Informationen gegen ihren Willen auf einer externen Plattform bereitstellen müssen bzw. dazu indirekt genötigt werden. Im Folgenden finden sich hierzu Empfehlungen für einzelne Nutzungsszenarien.

Einsatz in der Lehre:
Die empfohlene Lösung für Videoconferencing in der Lehre ist daher BigBlueButton, welches von der GWDG lokal betrieben. Damit ist die Lösung aus Sicht des Datenschutzes zu bevorzugen. Diese Lösung ist technisch für bis ca. 25 Personen mit gleichzeitigen Videos oder ca. 50 Teilnehmer mit Audio-Teilnahme geeignet.

Im Vergleich erlaubt Zoom darüber hinaus Veranstaltungen auch für größere Nutzergruppen mit Videos. Aus Sicht des Datenschutzes ist eine Nutzung von Zoom für die Lehre für solche Szenarien, wo BBB nicht geeignet ist, vertretbar, sofern Randbedingungen eingehalten werden:

- Studierende sind nicht gezwungen, an der Veranstaltung teilzunehmen.
- Die Teilnahme in Zoom ist anonym und im Web-Browser ohne Einsatz der Zoom-App möglich.
- Es wird keine Klarnamen-Pflicht für Studierenden eingefordert.

Einsatz in Gremienarbeit, z.B. Berufungskommissionen:
Bei Verarbeitung von Daten mit besonderem Schutzbedarf ist die empfohlene Lösung für Videoconferencing BigBlueButton. Diese Lösung ist technisch für bis ca. 25 Personen mit gleichzeitigen Videos oder ca. 50 Teilnehmer mit Audio-Teilnahme geeignet. Dies sollte für die typischen Gremien, wie z.B. Senat, Fakultätsrat, Dekanekonzil, Professorien, Prüfungsausschüsse ausreichend sein.

Gerade bei Gremien mit stärkerem Anteil vertraulicher und personenbezogener Kommunikation, Berufungskommissionen, Prüfungsausschüsse und persönlicher Beratung sollte unbedingt der Vorrang von BigBlueButton als einzusetzendes System beachtet werden. Zoom kann nur dann herangezogen werden, wenn sich bei Gruppen über 25 Teilnehmern ein sinnvoller Einsatz von BBB als nicht durchführbar erweist.

2 Zusammenfassung des Datenschutzes bei Zoom

Zoom ist ein US-amerikanisches Unternehmen ist und unterliegt damit nicht der Datenschutzgrundverordnung (DSG-VO), wie wir dies als Universität bevorzugen würden. Stattdessen unterliegt der Datenschutz bei Zoom dem EU-US Privacy Shield registriert. Damit ist auch für die Fa. Zoom die Nutzung von Daten reglementiert. Die GWDG hat hierzu einen Vertrag zur Auftragsdatenverarbeitung (ADV) mit der Fa. Zoom geschlossen, die auch vom Datenschutzbeauftragten der Universität geprüft wurde. Im Vergleich zur DSG-VO gibt es mit dem EU-US Privacy Shield ein theoretischer Zugriff auf die Daten durch staatliche Stellen in den USA. In Abwägung kommt daher die Empfehlung zustande, keine sensiblen Daten zu kommunizieren. Dies gilt allerdings auch unabhängig von der Situation mit Zoom/den USA auch für andere hochschulöffentliche Kanäle.

Es ist jedoch anzuerkennen, dass nicht in allen Szenarien eine geeignete lokal betrieben Alternative angeboten werden kann. BBB hat bekannte Limitationen, an denen zwar gearbeitet wird, die jedoch letztlich nicht immer in allen Bereichen mit kommerziellen Lösungen mithalten werden kann. Auch gibt es aktuell keine offensichtlich besseren Alternativen sowohl für den lokalen Betrieb als auch bei kommerziellen Cloud-Angeboten. Entsprechend müssen pragmatisch die Konsequenzen abgewogen werden, wenn eine Veranstaltung oder Termin aufgrund der technischen Randbedingungen nicht stattfinden kann im Vergleich zu einer Nutzung von Zoom. Hier kann Zoom auf Basis der existierenden Auftragsdatenverarbeitungsvereinbarung und der EU-US Privacy Shield aus Sicht des Datenschutzbeauftragten zulässig sein, sollte dabei jedoch auf ein Minimum reduziert bleiben.

Die Firma Zoom tauchte in den letzten Wochen mit diversen kritischen Berichten in der Presse auf. Diese Informationen werden von CIO, Datenschutzbeauftragten und GWDG verfolgt und laufend bewertet. Auf dieser Basis wurden beispielsweise Empfehlungen auf den Webseiten der GWDG und der Universität zur Einstellungen bei Videokonferenzen für Moderatoren bereitgestellt, die für einen wesentlichen Teil der öffentlich genannten Probleme Abhilfe leisten. Diese Empfehlungen sollten daher beim Einsatz von Zoom auch gefolgt werden. Weiterhin ist festzustellen, dass die Fa. Zoom aktiv daran arbeitet, Abhilfe zu bekanntgewordenen Problemen zu liefern. Hierzu wurden Apps aktualisiert und Einstellungen für Optionen verändert. Daher gilt bisher weiterhin die Einschätzung, dass Zoom kein grundsätzliches oder untragbares Problem bzgl. Informationssicherheit und Datenschutz darstellt.

3 Datenschutzrechtlichen Rahmenbedingungen für den Einsatz von Videokonferenzen in der digitalen Lehre

3.1 Grundsätzliches

Die Universität Göttingen als Verantwortlicher für die digitale Lehre folgt einem gemischten Ansatz, der für kleinere Veranstaltung eine Nutzung des eigenen Systems „BigBlueButton“ vorsieht und für größere Veranstaltungen die Software „Zoom“. Für Gremiensitzungen soll grundsätzlich nur „BigBlueButton“ zum Einsatz kommen.

Zoom hat aufgrund der weltweit geführten intensiven Diskussion in vielen Punkten nachgebessert. Insbesondere werden keine Inhaltsdaten mehr weiterverwendet, wie dies die alte Datenschutzerklärung theoretisch ermöglicht hätte. Einige kritische Punkte können über Voreinstellungen geregelt werden, die vom Dozenten oder Teilnehmer erfolgen können. Beispielsweise müssen aufgezeichnete Inhalte nicht in der Cloud gespeichert werden.

Da Zoom ein US-amerikanisches Unternehmen ist, bleiben aber wegen der Datenübermittlung in die USA einige grundsätzliche Bedenken, die dazu führen, dass die rechtliche Situation (Registrierung unter den EU-US Privacy Shield einerseits) mit der faktischen Lage (theoretischer Zugriff auf die Daten durch staatliche Stellen in den USA) abzuwägen ist. So kommt die Empfehlung zustande, keine sensiblen Daten zu kommunizieren. Dies gilt allerdings auch unabhängig von der Situation mit Zoom/den USA auch für andere hochschulöffentliche Kanäle.

3.2 Rechtsgrundlagen der Verarbeitung

Als Rechtsgrundlage kommt vor allem Art. 6 Abs. 1 lit. e) DSGVO i.V.m. § 3 NHG i.V.m. §§ 28, 29 PersDatO, die bis zu einer notwendigen Änderung bzw. Ergänzung erweiternd ausgelegt werden können, um auch die breite Nutzung externer Systeme zu erfassen, solange dies aus Gründen des Gesundheitsschutzes erforderlich ist.

Für den Fall einer Aufzeichnung der Videokonferenz erscheint die dann mögliche Erfassung von Bild und Ton von teilnehmenden Studierenden nicht mehr im Rahmen der Erforderlichkeit abgedeckt. In diesem Fall wäre eine Aufzeichnung zu unterlassen oder die Konferenz technisch so einzustellen, dass Beiträge der Studierenden nicht möglich sind. Alternativ kann die Aufzeichnung erfolgen, wenn alle Teilnehmer eine datenschutzrechtlich wirksame Einwilligung nach Art. 6 Abs. 1 UAbs 1 lit. a) DSGVO erklärt haben.

Problematisch ist allerdings die Datenweitergabe an Dritte (Google Ads, Google Analytics, Werbepartnern und weitere Dienstleistungsunternehmen). **Nach der Datenschutzerklärung von Zoom werden Daten für Werbezwecke nur bei Marketing-Websites und nicht für Zoom-Dienste erfasst. Die Dienste enthalten danach keine Werbe-Cookies oder Tracking-Technologie. Allerdings zählt Zoom Analyse-Tools auch von Dritten zu den funktionellen Cookies. Daher erscheint eine Deaktivierung dieser Tools im Browser des Nutzers erforderlich. Google hält dafür folgenden Link vor: https://www.aboutcookies.org/how-to-control-cookies/. Ein entsprechender Hinweis wird den Studierenden gegeben.**

Hinsichtlich des Datentransfers in die U.S.A. (Cloud) ist ist Zoom dem Privacy Shield beigetreten.

3.3 Zugangssicherung

Der Konferenzraum soll mit einem Passwort gesichert werden. Für Einladungen zu einem Konferenzraum sind immer Link und Passwort getrennt mitzuteilen. Die Möglichkeiten von Stud.IP können genutzt werden, um die Studierenden über die Termine und die vertraulichen Zugangsdaten zu informieren. Zoom bietet Ihnen weitere Möglichkeiten, den Raum zu sichern (z.B. Meeting sperren, Beitritt vor Moderator zu deaktivieren, Aktivierung eines Warteraums).

3.4 Keine Klarnamenspflicht/Bereitstellung anonymer Nutzungsmöglichkeit

Für die Teilnahme an Lehrveranstaltungen über „Zoom“ müssen die Teilnehmer keinen Account auf der Herstellerwebseite (https://zoom.us) registrieren oder sich anzumelden. Die Teilnahme an allen „Zoom“ Meetings kann und soll ohne dortige Registrierung oder Anmeldung erfolgen. Eine Teilnahme an Lehrveranstaltungen über "Zoom" ist in der Regel über Internet-Browser möglich. Die Verwendung im Browser über HTML5 erfordert keine vorherige Installation. Allerdings müssen sich die Teilnehmer an einem Meeting bei Zoom einloggen. Dafür kann unser Single-Sign-On oder ein selbstregistrierter Account bei Zoom verwendet werden. Diese Variante unterscheidet sich aber u.U. im Funktionsumfang und im Nutzungserlebnis von der Clientsoftware von Zoom, die installiert werden muss.

Grundsätzlich darf von den Studierenden nicht verlangt werden, mit Klarnamen einer Sitzung beizutreten. Davon kann es aber Ausnahmen geben: Bei Seminaren mit Anwesenheitspflicht oder zur Sicherstellung einer geschlossenen Veranstaltung darf die Lehrperson die Klarnamen verlangen. Bei BigBlueButton findet eine Anbindung an Stud.IP statt, die Namen werden ohnehin als Klarnamen übernommen. Dies ist aber insofern nicht problematisch, als BigBlueButton eine Lösung ist, die vollständig von Universität und GWDG kontrolliert wird.

Das kann auch bedeuten, dass für andere Formate wie interaktiv ausgerichtete Arbeitsgruppen eine Pflicht zur Teilnahme auch mit Video und Ton geben kann, da diese sonst nicht sinnvoll durchführbar sind. Ein Chat allein als Rückkanal ist dafür nicht immer ausreichend.

Die Teilnahme an "Zoom" für Veranstaltungen der Universität soll für die Studierenden als Zuhörende so weit wie möglich anonym gegenüber dem System ermöglicht werden. Eine aktive Beteiligung – unter Preisgabe weiterer persönlicher Daten - ist freiwillig. Für die datengeschützte und datensichere Nutzung von "Zoom" gelten unter anderem folgende Grundsätze:

- Bei der Teilnahme an Meetings können zu Beginn oder im Verlauf der Name und die E-Mailadresse abgefragt werden. Hier besteht grundsätzlich kein Zwang zur Eingabe Ihres Klarnamens oder einer gültigen E-Mail-Adresse. Die Studierenden können ein selbst gewähltes Pseudonym und eine beliebige – auch nicht gültige – E-Mail-Adresse verwenden.

- Wenn zum Schutz gegen unbefugte Teilnahme an der Veranstaltung eine Teilnahmekontrolle erforderlich ist, so kann mit den Lehrenden ein Verfahren vereinbart werden, wie die Anonymität gegenüber dem System gewahrt bleibt. Dies kann z.B. über eine Liste von

verwendeten Aliasnamen erreicht werden, die in Stud.IP gepflegt wird. So erfolgt eine Anonymisierung gegenüber dem System aber nicht gegenüber den Teilnehmenden der Veranstaltung.

- Bei der Teilnahme an Meetings können die Studierenden ein Avatar-Bild einstellen. Es besteht in Veranstaltungen kein Zwang, ein Bild von der Person einzustellen.

- Die Studierenden können die Übertragung Ihrer Video- und Audiodaten manuell verhindern, bspw. durch Ausschalten in der Software oder durch das Überkleben der Kamera auf Ihrem Endgerät.

3.5 Weitere datenschutzfreundliche Voreinstellungen

Die Cookie- Einstellungen können auf der Startseite von Zoom minimiert werden. Insbesondere ist sicher zu stellen, dass keine externen Analysedienste Zugriff zu den Daten haben.

Der „Aufmerksamkeitstracker“, der feststellen lässt, ob die Zoom-Seite gerade ein aktives Fenster ist, ist mittlerweile von Zoom auf die Voreinstellung „Aus“ gestellt worden. Der Veranstalter darf diesen Modus nicht aktivieren.

3.6 Installationspflicht von Programmen

Es ist kritisch zu sehen und kann nur in konkreten Einzelfällen erlaubt sein, Studierende zu verpflichten, eine Software auf ihren Privatrechnern zu installieren. Dies kann in besonderen Situationen wie Prüfungen der Fall sein. Die Software müsste aber extrem sicher und verlässlich sein.

Eine solche Installation ist bei richtiger Anwendung weder bei BigBlueButton noch bei Zoom nötig, da entweder ein Login über das Single-Sign-On der GWDG oder aber eine (anonyme) Nutzung von Zoom über html5 im Browser möglich ist.

3.7 Zur Einwilligung bei Aufzeichnungen

Die Einholung einer Einwilligung in Web-/Videokonferenzen kann durch Zustimmung z.B. durch Veränderung des Status der Teilnehmenden (z.B. Statussetzen in Big Blue Button), Eingabe einer Reaktion (z.B Thumbs-Up-Emoticon in Zoom) oder durch die Eingabe eines Chat-Beitrags im Web-/Videokonferenzraum erfolgen. Die Einwilligung der Betroffenen sollte zu Beweiszwecken stets dokumentiert werden. Die Betroffenen können ihre Einwilligung jederzeit widerrufen und sich durch Abschalten von Mikrofon und Videobild der Aufnahme entziehen. In diesem Fall sollte ihnen die Gelegenheit gegeben werden, in anderer Weise mit dem Dozierenden zu kommunizieren bzw. Fragen zu stellen, etwa durch Chat oder E-Mail.

Bei den Aufzeichnungen auf denen ausschließlich der/die Vortragende zu sehen und zu hören ist, wird nur die Zustimmung des Referierenden benötigt, da die Persönlichkeitsrechte der anderen Teilnehmenden nicht berührt werden. Sollte ein Gespräch oder Diskussion aufgenommen werden, müssen alle Teilnehmenden, die sich beteiligen, darüber informiert werden und sich mit einer Veröffentlichung einverstanden erklären.

Eine Aufzeichnung soll nur in der lokalen Cloud gespeichert werden, nicht in der Zoom-Cloud.

Mit unterschiedlichen Methoden (Screencasting-Software, Smartphones, etc.) ist technisch die Aufzeichnung auch außerhalb des Systems möglich. Aufzeichnungen sollen ausschließlich durch die Lehrenden erfolgen. Eine Aufzeichnung ohne Einwilligung aller Betroffenen (Lehrende und Studierende) ist sowohl urheberrechtlich als auch persönlichkeitsrechtlich unzulässig und strafbar. Darauf ist ausdrücklich hinzuweisen.

Zur Frage, ob eine Einwilligung als Rechtsgrundlage für die Nutzung von Zoom in Betracht kommt, ist sich der Datenschutz nicht ganz einig.

Die entsprechenden Handreichungen für Studierende und Lehrende sind abrufbar:

Studierende Zoom: www.uni-goettingen.de/de/document/download/351a7a63d4ab1faaac6e656bf68e20d9.pdf/Handreichung%20f%C3%BCr%20Studierenden%20zur%20Nutzung%20von%20Zoom.pdf

Lehrende Zoom: www.uni-goettingen.de/de/document/download/83fe99ecee994f8a4b7484063e9039a4.pdf/Handreichung%20f%C3%BCr%20Lehrenden%20zur%20Nutzung%20von%20Zoom.pdf

Aufzeichnungen: www.uni-goettingen.de/de/document/download/2f28b812ba3b3687b188f539b4ca7d16.pdf/Handreichung%20zu%20Aufzeichnungen.pdf

4 Datenschutzrechtliche Rahmenbedingungen für den Einsatz von Videokonferenzen in der digitalen Gremienarbeit

Für den Einsatz von Videoconferencing-Systemen gelten zunächst die zur digitalen Lehre gemachten Ausführungen entsprechend.

Als Rechtsgrundlage kommt vor allem Art. 6 Abs. 1 lit. e) DSGVO i.V.m. § 3 NHG in Betracht. Solange die Beschränkungen von Präsenzkonferenzen anhalten, ist grundsätzlich die Erforderlichkeit des Einsatzes von Videoconferencing-Systemen für die Gremienarbeit gegeben. Dabei gilt unter dem Gesichtspunkt der Erforderlichkeit nur ein Einsatz von BBB als gerechtfertigt, soweit dies technisch in hinreichender Form durchführbar ist.

Bei Verarbeitung von Daten mit besonderem Schutzbedarf ist die anzuwendende Lösung für Videoconferencing BigBlueButton. Diese Lösung ist technisch für bis ca. 25 Personen mit gleichzeitigen Videos oder ca. 50 Teilnehmer mit Audio-Teilnahme geeignet.

Bei Gremien mit stärkerem Anteil vertraulicher und personenbezogener Kommunikation, Berufungskommissionen und persönlicher Beratung ist unbedingt der Vorrang von BigBlueButton als einzusetzendes System zu beachten und Zoom nur dann heranzuziehen, wenn sich bei Gruppen z.B. über 25 Teilnehmern, die gleichzeitig mit Video beteiligt sein müssen und ein sinnvoller Einsatz von BBB technisch nicht als durchführbar erweist.

Die Verarbeitung von sensiblen Daten der Teilnehmer oder Dritter (Art. 9 Abs. 1 DSGVO: Daten, aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung) ist nur zulässig aufgrund einer Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO oder zur Erfüllung aus dem Arbeits- oder Sozialrecht erwachsender Rechte oder Pflichten erforderlich ist.

Soweit ausnahmsweise eine Aufzeichnung erfolgen sollte, ist diese nur mit Einwilligung zulässig. Rechtsgrundlage ist Art. 6 Abs. 1 UAbs 1 lit. a) DSGVO sowie bei Verarbeitung sensibler Daten Art. 9 Abs. 2 lit. a) DSGVO. Darüber sind die Teilnehmer vorher aufzuklären, wobei die Hinweise nach Art. 13 einzubeziehen sind: https://studip.uni-goettingen.de/dispatch.php/siteinfo/show/5. (für weitere Hinweise zum Einholen der Einwilligung s.o. unter A.8.).

--CIO, 05.05.2020

--DSB, 05.05.2020

--Angenommen in der KIM, 30.04.2020