myFlexNet
digital lernen | flexibel handeln

Vertraulichkeit in Videokonferenzsystemen- ein Praxisbeispiel

Wenn Videokonferenzformate eingesetzt werden, muss der Schutz persönlicher und fremder Daten gewährleistet sein. In unserer Praxis bedeutet dies, dass Regeln zur Erfüllung von Informationspflichten, der Nutzung personenbezogener Daten sowie zu erbringender technischer und organisatorischer Leistungen aus der Datenschutzgrundverordnung = DSGVO abgeleitet werden.

Es darf vermutet werden, dass hierzulande hauptsächlich über Internet angebotene Videokonferenz-Dienste, so genannte „Software as a Service“ –Systeme, eingesetzt werden: zum Beispiel Zoom, Microsoft-Teams, Big Blue Button o.a. eingesetzt werden.

Anhand eines dieser Dienste – **BigBlueButton (BBB**) - wird die Behandlung datenschutzkritischer Themen beispielhaft dargestellt.

Eine geeignete Nutzerauthentifizierung

Generell sollte eine Nutzerauthentifizierung erfolgen, um lediglich dem berechtigten Personenkreis (Teilnehmer*Innen und Moderator*Innen) Zugriff auf die Videokonferenzsitzungen und deren Daten zu gestatten.
Der Authentifizierungsaufwand sollte sich nach dem Risiko für die betroffenen Personen richten, das sich bei einem Bruch der Vertraulichkeit oder Integrität der Inhaltsdaten ergeben könnte.
Bei normalen Risiken sollte eine Authentifizierung mit Nutzernamen und geeignetem Passwort genügen, während bei einem hohen Risiko (z. B. bei stark schützenswerten Informationen wie persönlichen Gesundheitsdaten) schon eine Zwei-Faktor-Authentifizierung der Standard sein sollte.

Ein Gastzugang, der ohne vorherige Nutzerauthentifizierung auskommt, kann nach den Richtlinien der DSK angeboten werden, wenn

- Risiken für die Betroffenen gering sind, die durch eine nicht autorisierte Teilnahme entstehen,
- sichergestellt ist, dass nur Personen teilnehmen, die sich untereinander kennen
- nicht autorisierte Personen erkannt und ausgeschlossen werden können, bevor sie aktiv an der Videokonferenz teilnehmen können.

BBB räumt die Möglichkeit von Gastzugängen ein. Wenn die im vorigen Abschnitt genannten Kriterien erfüllt sind, ist dies eine sinnvolle Lösung im Sinne einer datenschutzgerechten Nutzerauthentifizierung. Praktischerweise sollte dieser Prozess von der moderierenden bzw. präsentierenden Person gesteuert werden.

Externe Speicherung persönlicher Daten

Im Gegensatz zu selbstbetriebenen Videokonferenzsystemen bleiben die Datenflüsse bei BBB u. a. nicht automatisch innerhalb des Systems und können somit nicht vollständig vom Betreiber bzw. dem Bildungsunternehmen kontrolliert werden. Sofern BigBlueButton nicht mit einem eigenen Server betrieben wird, sollte die Nutzung immer mit einem **Vertrag zur Auftragsverarbeitung** (AV) abgesichert werden.

Damit kann sich das nutzende (Bildungs-) Unternehmen vertraglich über die Verarbeitung der personenbezogenen Daten von Teilnehmer*innen und Lehrkräften absichern. Dieser Vertrag sollte klarstellen,

- welche Userdaten der Hosting-Anbieter vom Unternehmen erhält und speichert,
- wie lange der Anbieter die Daten speichert,
- warum der Anbieter die Daten erhebt und aufbewahrt und
- welche Rechte und Pflichten Anbieter und Unternehmen haben
- Da der Dienstanbieter sich nicht auf die gleiche Rechtsgrundlage berufen kann wie das nutzende Unternehmen, wird empfohlen, im Auftragsverarbeitungsvertrag festzuhalten, dass der Anbieter die personenbezogenen Daten der Teilnehmer nur auf Weisung des nutzenden Unternehmens und nicht für eigene Zwecke verarbeiten darf.

Unternehmen müssen in ihrer **Datenschutzerklärung** darauf hinweisen, wenn sie mit einem Hosting-Anbieter einen Vertrag zur Auftragsverarbeitung geschlossen haben. Dabei muss sichergestellt werden, dass durch den Dienstleister (BBB) bzw. seine eingesetzte Software keine Daten an Dritte übermittelt werden dürfen.

Um hierzulande gegen die Verletzung von Datenschutzrechten durch einen externen Dienstanbieter zu klagen, muss sichergestellt sein, dass dessen datenschutzrelevante Handlungen auch tatsächlich der deutschen bzw. europäischen Rechtsprechung unterliegen und nicht denen eines externen Rechtssystems, in dem womöglich andere Regeln gelten. Dies ist bei BigBlueButton der Fall.

Schlussfolgerungen: Ein eigener Server hilft, den administrativen Datenschutzaufwand bei der Zusammenarbeit mit BBB zu reduzieren; wenn dies nicht möglich ist, sollte unbedingt ein sorgfältig formulierter Vertrag zur Auftragsverarbeitung abgeschlossen werden.

Zum Nachlesen:
https://dsgvo-gesetz.de/art-28-dsgvo/ und
https://www.firma.de/unternehmensfuehrung/auftragsverarbeitungsvertrag-fags-zum-av-vertrag-nach-dsgvo/.

Interne Speicherung persönlicher Daten

Nutzt das Bildungsunternehmen BigBlueButton, egal ob von ihm selbst betrieben oder gemäß eines Vertrags zur Auftragsverarbeitung, setzt die **Teilnahme an einer Videokonferenz die informierte und freiwillige Einwilligung** der Betroffenen voraus. Da für die Nutzung durch Lehrkräfte Konten erforderlich sind, müssen dort, anders als bei den Teilnehmern, auch Daten zur Erstellung und Nutzung eines Kontos berücksichtigt werden. Gegenüber Lehrkräften gelten zusätzliche datenschutzrelevante Regelungen: Zum einen sollten sie informiert und verpflichtet werden, die im Auftrag ihres Unternehmens verwendeten persönlichen Daten von Teilnehmer*Innen nach DSGVO zu schützen. Zum

anderen sollten Regelungen zur Erfassung und Speicherung ihrer eigenen persönlichen Daten getroffen sein, entweder im Individual-Arbeitsvertrag oder durch Kollektivvereinbarungen wie Betriebsvereinbarungen.

Unternehmen erheben über BigBlueButton automatisch Userdaten. Darauf müssen sie in ihrer **Datenschutzerklärung** hinweisen. Dabei müssen sie benennen,

- warum sie welche Daten erheben, d. h. der Zweck der Datenspeicherung muss dargelegt werden
- wie lange sie diese Daten speichern wollen. Grundsätzlich sind Unternehmen befugt, Daten so lange zu speichern, wie sie für den Zweck, für den sie erhoben wurden, erforderlich sind. Danach müssen die Daten gelöscht werden. Bezugspunkt für die Beurteilung der Erforderlichkeit ist im konkreten Fall der jeweils festgelegte Verwendungszweck. Die Speicherung der Daten muss also notwendig sein, um die jeweilige Aufgabe vollständig, rechtmäßig oder in angemessener Zeit erfüllen zu können. Eine darüber hinaus gehende Aufbewahrung muss gesetzlich legitimiert sein, wie etwa durch steuerrelevante Tatbestände.
- welche Rechtsgrundlage ihnen die Datenverarbeitung nach der DSGVO erlaubt und
- dass Nutzer der Datenerhebung und Datenspeicherung jederzeit widersprechen können.

Eine Einwilligung der Nutzer*Innen zur Speicherung von Userdaten ist also eigentlich immer erforderlich. Der Zugang zu BBB kann über eine URL, also über Browser gewährleistet werden; dementsprechend müssen nicht zwingend Kontendaten wie zum Beispiel eine Mailadresse in BBB hinterlegt sein; sie sind aber im Regelfall zum Versand der URL-Adresse und sonstigem Informationsaustausch auf dem Server der Bildungseinrichtung hinterlegt.
Sofern die persönlichen Daten nur für eine Bildungsmaßnahme erhoben und gespeichert wurden und diese abgeschlossen ist, sollte die gesetzliche Legitimation für eine weitere Aufbewahrung immer regelmäßig überprüft werden.

Aufzeichnungsmöglichkeit von Videokonferenzen

Ein spezielles Problem besteht in der **Aufzeichnungsmöglichkeit von Videokonferenzen**
„BigBlueButton zeichnet in Videokonferenzräumen, in denen die Aufnahmefunktion nicht deaktiviert wurde, im Hintergrund die Videokonferenz in Form einer so genannten RAW-Datei auf. Aus dieser kann, sofern die Aufnahmefunktion im Laufe der Videokonferenz genutzt wird, im Anschluss eine Datei erzeugt werden, die für Veröffentlichungen geeignet ist.

Deswegen sollten Räume für Videokonferenzen in BigBlueButton prinzipiell mit deaktivierter Aufnahmefunktion erstellt werden, egal ob nachgelagerte Sicherungsmöglichkeiten wie der Betrieb des Systems über den eigenen Server existieren oder nicht. Nur so kann sichergestellt werden, dass keine automatische Aufzeichnung und Speicherung im Hintergrund erfolgt.

Personenbezogene Daten bei Firmenseminaren

Ein spezieller Fall entsteht für Schulungsunternehmen dann, wenn Mitarbeiterdaten einer beauftragenden Institution innerhalb einer Videokonferenz erhoben und/oder genutzt werden sollen, etwa zur Anwesenheitskontrolle. Hier sind beide Parteien an den § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) gebunden: „Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung

der Rechte der betroffenen Person angeht,… „

Ein Unternehmen, das Mitarbeiter*Innen in eine Schulung in Videokonferenzform entsendet, muss darauf achten, dass immer eine Interessenabwägung nach § 26 Abs. 1 BDSG https://dsgvo-gesetz.de/art-26-dsgvo/ durchgeführt werden muss. Diese muss vor allem dann durchgeführt werden, wenn mit dem Videokonferenzsystem auch eine Mitarbeiterüberwachung verbunden ist, z. B. durch Kontrolle der An- und Abwesenheiten. Wenn dies der Fall ist, muss zusätzlich auch die Zustimmung des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG https://www.gesetze-im-internet.de/betrvg/__87.html eingeholt werden, sofern vorhanden. Bildungsanbieter sollten sich eine entsprechende Versicherung im Rahmen eines Lehrgangsvertrags des beauftragenden Unternehmens einholen.

Wenn sich Mitarbeiter*Innen des beauftragenden Unternehmens während der Schulung im Home-Office befinden, muss gewährleistet werden, dass andere Teilnehmende keinen Einblick in die jeweilige Privatwohnung erhalten können, weil dies ohne Einwilligung der Betroffenen nicht datenschutzkonform ist. BigBlueButton bietet zwar noch keine eigene Möglichkeit für die Einblendung eines virtuellen Hintergrunds an, ermöglicht aber die Integration bestimmter virtueller Hintergrundsysteme, z.B. https://snapcamera.snapchat.com/ Auf diese Möglichkeit könnten die Teilnehmer*Innen hingewiesen werden.

Informationspflichten des Verantwortlichen

Wie schon erwähnt, gilt die Pflicht des Verantwortlichen, die Schulungsteilnehmer*Innen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung gem. Art. 13, 14 DSGVO https://dsgvo-gesetz.de/art-13-dsgvo/ zu informieren. Damit diese erfahren, an wen sie sich wenden können, sind Verantwortliche für die Durchführung der Videokonferenzen unter Nennung ihrer Kontaktdaten und ggf. des Datenschutzbeauftragten aufzuführen. Art und Ziel der Verarbeitung müssen genau definiert werden und beschränken sich bei Videokonferenzen nur auf deren Durchführung.
Zusätzlich ist auch die Rechtsgrundlage der Verarbeitung anzugeben und, soweit die Verarbeitung auf Art. 6 lit. f DSGVO gestützt wird, die einschlägigen berechtigten Interessen des Verantwortlichen. Was die Dauer der Speicherung personenbezogener Daten betrifft, geht diese grundsätzlich nicht über die Dauer der Konferenz hinaus, da die Videodaten lediglich für die Durchführung der Videokonferenz erforderlich sind. Wird ein externer Dienstleister wie BigBlueButton herangezogen, ist dieser als Empfänger der Daten anzugeben.

Ausblick

Die Umsetzung datenschutzrechtlicher Regeln bei der Organisation und Durchführung von Videokonferenzen ist unumgänglich, vor allem weil damit zu rechnen ist, dass die Aufsichtsbehörden in Bälde die Einhaltung der geltenden Regeln kontrollieren und ggfs. sanktionieren werden.

Wie sehen Sie die Problematik oder haben Sie Anregungen zu diesem Thema? Welche Fragen sind bei Ihnen offengeblieben?

Schreiben Sie an: Stefan Brandt-Pollmann; Servicestelle beim BZH- Bildungszentrum Handel und Dienstleistungen gGmbH, brandt-pollmann@bz24.de

Dezember 2021

Quellennachweise:

https://pixabay.com/de/photos/online-meeting-videokonferenz-5183791/
https://pixabay.com/de/photos/datenschutz-sicherheit-hacker-cyber-4521074/

Das Projekt „FlexNet Handel“ wird im Rahmen des Programms „Digitale Medien in der beruflichen Bildung“ vom Bundesministerium für Bildung und Forschung und dem Europäischen Sozialfonds gefördert.