myFlexNet
digital lernen | flexibel handeln

Vertraulichkeit in Videokonferenzsystemen

Wenn Videokonferenzformate eingesetzt werden, muss der Schutz persönlicher und fremder Daten gewährleistet sein. Maßgebliche Grundlagen wie Informationspflichten, Nutzung personenbezogener Daten, zu erbringende technische und organisatorische Leistungen sind aus der Datenschutzgrundverordnung = DSGVO abzuleiten.

Aus der Wahl des Videokonferenzsystems ergeben sich jedoch unterschiedliche Anforderungen.

Die Grenzen der Vertraulichkeit

So gut wie alles, was in Onlineseminaren geschieht, kann in guter Qualität digitalisiert festgehalten und verbreitet werden. Was kann von Bildungsanbietern getan werden, um vertrauliche Informationen so vertraulich wie möglich zu halten, also einen hinreichenden Datenschutz zu gewährleisten? Diese Fragestellung beinhaltet die schon banale Aussage, dass ein hundertprozentiger Schutz nicht garantiert werden kann: Sicherheitslücken und Missbrauchsmöglichkeiten beim Einsatz von Videokonferenzsystemen (VCR) lassen sich reduzieren, aber eben nicht hundertprozentig ausschließen. Die geltenden Datenschutzregeln setzen einen gesetzlichen Rahmen, sind aber nicht zwangsläufig bzw. mit vertretbarem Aufwand- durchsetzbar. Es kann also für die Anbieter von Trainings über VCR nur um das Ziel gehen, möglichst nicht juristisch angreifbar zu sein.

Welches Videokonferenzsystem wird eingesetzt?

Prinzipiell gibt es drei Optionen, Videokonferenzsysteme in Trainings einzusetzen

1. selbstbetriebene Videokonferenzsysteme
2. Betrieb durch einen externen IT-Dienstleister mit der speziellen Ausformung durch
3. Nutzung eines Online-Dienstes

Selbstbetriebene Videokonferenzsysteme haben den Vorteil, dass alle Datenflüsse innerhalb des Systems bleiben und damit selbst vom Betreiber kontrolliert werden können. Der Vorteil dieser Verfahren ist, dass weder eine Auftragsverarbeitungsvertrag oder eine Vereinbarung zur gemeinsamen Verantwortlichkeit mit einem externen IT- Dienstleister geschlossen werden muss. Verantwortlichkeit und Steuerung der Datenverarbeitungsprozesse verbleiben beim Bildungsanbieter. Für Bildungsanbieter stellen sich die Fragen, ob die eigenen Ressourcen ausreichen bzw. ob sich der personelle und materielle Aufwand rechnet.

Bei der Bereitstellung durch externe IT-Dienstleister muss ein Auftragsverarbeitungsvertrag abgeschlossen werden, ein so genannter AV-Vertrag. Vor allem muss geprüft und sichergestellt werden, dass durch den Dienstleister bzw. seine eingesetzte Software keine Daten an Dritte übermittelt werden dürfen.
(Für einen näheren Einblick in diese Thematik die nachfolgenden Links https://dsgvo-gesetz.de/art-28-dsgvo/ und

https://www.firma.de/unternehmensfuehrung/auftragsverarbeitungsvertrag-faqs-zum-av-vertrag-nach-dsgvo/.)

Die meisten Bildungsanbieter wählen wahrscheinlich Online-Videokonferenz-Tools (Software as a Service), also über das Internet angebotene Videokonferenz-Dienste. Auch hier muss ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Ein wesentliches Kriterium sind die vom Dienstleister ergriffenen technischen und organisatorischen Maßnahmen, welche vorab dahingehend zu prüfen sind, ob der eingesetzte Dienstleister einen hinreichenden Datenschutz bietet. Innerhalb der europäischen Union sind zwar die gesetzlichen Grundlagen über die Nutzung schützenswerter Daten gelegt worden; Problematisch wird es, wenn leistungsfähige und gern genutzte Diensteanbieter Daten nach Nicht-EU-Rechtsgrundlagen verarbeiten, die sich in datenschutzrelevanten Fragestellungen vom europäischen Recht zum Teil wesentlich unterscheiden.
Die Verhandlungsmacht und Durchsetzungsfähigkeit für Administrator und Unternehmen sind in dieser Hinsicht beschränkt, zumal nach der jüngsten Entscheidung des EuGHs und dem Wegfall des sogenannten EU-U.S. Privacy Shields derzeit nur eingeschränkte juristische Möglichkeiten zur Verfügung stehen. (Zu dem aktuellen Stand der beigefügte Link auf den Blog https://www.johner-institut.de/blog/regulatory-affairs/privacy-shield-abkommen/) Die hiesige Datenschutzkommission (DSK) empfiehlt – Stand Juni 2021 - deshalb diejenigen Anbieter grundsätzlich zu bevorzugen, die ihren Sitz in der Europäischen Union haben. Ob die damit zur Verfügung stehenden Angebote den Nutzeransprüchen genügen, wird an dieser Stelle nicht diskutiert.

Verantwortlichkeiten beim Datenschutz klären

Generell sollte bei der Nutzung von Online-Diensten geprüft werden, ob der Anbieter die personenbezogenen Daten der Teilnehmer auch zu eigenen Zwecken verarbeitet und/oder Daten an Dritte weiterreicht, z. B. für Tracking und Analyse. Liegt eine Verarbeitung des Anbieters auch zu eigenen Zwecken vor, sollte vonseiten des Bildungsunternehmens eine Vereinbarung im Sinne des Art. 26 DSGVO geschlossen werden https://dsgvo-gesetz.de/art-26-dsgvo/. Da der Dienstanbieter sich nicht auf die gleiche Rechtsgrundlage berufen kann wie das nutzende Unternehmen, empfiehlt die DSK im Auftragsverarbeitungsvertrag festzuhalten, dass der Anbieter die personenbezogenen Daten der Teilnehmer nur auf Weisung des nutzenden Unternehmens und nicht für eigene Zwecke verarbeiten darf.

Die Nutzung personenbezogener Daten

Sofern kein Beschäftigungsverhältnis berührt ist, regelt Art. 6 Abs. 1 DSGVO https://dsgvo-gesetz.de/art-6-dsgvo/, dass die Verarbeitung persönlicher Daten rechtmäßig ist, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für vorher bestimmte Zwecke gegeben hat oder die Verarbeitung für die Erfüllung des Schulungsvertrags notwendig ist. Diese Bedingungen sollten in geltenden Schulungsverträgen ohnehin gewährleistet werden.
Ein spezieller Fall entsteht für Schulungsanbieter dann, wenn Mitarbeiterdaten eines beauftragenden Unternehmens (oder anderer Institutionen) innerhalb einer Videokonferenz erhoben und/oder genutzt werden sollen. 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,… „

Das beauftragende Unternehmen, das Mitarbeiter*innen in eine Schulung 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 im Rahmen der Vereinbarung eine entsprechende Versicherung des beauftragenden Unternehmens einholen.

Wenn sich Mitarbeiter*innen des beauftragenden Unternehmens während der Schulung im Home-Office befinden, muss gewährleistet werden, dass andere Teilnehmer keinen Einblick in die jeweilige Privatwohnung erhalten können, weil dies ohne Einwilligung der Betroffenen nicht datenschutzkonform ist. Um Missverständnissen vorzubeugen, bietet es sich an, die an der Schulung teilnehmenden Mitarbeiter*innen anzuweisen, den Hintergrund unscharf zu stellen oder auch einen virtuellen Hintergrund einblenden zu lassen; bei mehreren Anbietern von Videokonferenzsystemen ist diese Funktion mittlerweile Standard.

Zusätzlich muss - wie bei Präsenzseminaren auch - die Verarbeitung personenbezogener Daten von Personen geklärt werden, die nicht Teilnehmer einer Videokonferenz sind, z. B. bei Autoren von präsentierten Dokumenten und anderer Medien.

Informationspflichten des Verantwortlichen

Es 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. der seines/r Datenschutzbeauftragten aufzuführen. Art und Ziel der Verarbeitung müssen genau definiert werden und beschränken sich bei Videokonferenzen nur auf deren Durchführung. Vor allem für die Anfertigung von Aufzeichnungen muss eine eigene Rechtsgrundlage vorliegen; deswegen muss die Aufzeichnungsmöglichkeit in den Informationen explizit erwähnt sein. Hier sollten vor Beginn der Aufzeichnung entsprechende Einwilligungen der Teilnehmenden eingeholt werden.
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 herangezogen, ist dieser als Empfänger der Daten anzugeben.

Technische und organisatorische Leistungen

Um die Sicherheit zu erhöhen, können bei den meisten Konferenzsystemen Zusatzfunktionen wie private Chats, Screensharing, Aufnahmefunktionen und die Bereitstellung von sensiblen Dokumenten ausgeschaltet werden.
Veranstalter von Videokonferenzen sind dafür verantwortlich, dass das eingesetzte System auf dem neuesten Stand ist und alle bis zum Zeitpunkt der Videokonferenz bekannt gewordenen Sicherheitslücken beseitigt wurden.

Eine geeignete Nutzerauthentifizierung

Generell sollte eine Nutzerauthentifizierung erfolgen, um lediglich dem berechtigten Personenkreis (Teilnehmer*nnen 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 persönliche 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.

Welche Rollen sollten vorhanden sein?

Bei der Auswahl des jeweiligen Videokonferenzsystems sollte darauf geachtet werden, dass mindestens folgende Rollen eingerichtet werden können:

- Administrierende Person, die über Berechtigungen zur Festlegung von Parametern und zur Zuweisung der Moderationsrolle verfügt
- Moderierende Person, welche die Berechtigung hat, Videokonferenzen anzuberaumen, Personen einzuladen oder auszuschließen, Zutritt zu eröffnen und zu schließen und die Präsentationsrolle zuzuweisen.
- Präsentierende Person mit der Berechtigung, Dokumente und andere Medien bereitzustellen sowie Wortmeldungen und andere Beiträge zu steuern.
- Teilnehmende sollten nach der DSK innerhalb des VCR ausschließlich über die Berechtigung verfügen, die eigenen Aufzeichnungs- und Wiedergabegeräte zu steuern.

Wichtig ist auch, dass jede Person ihre Kamera und ihr Mikrofon jederzeit deaktivieren kann.

Schlussfolgerungen und 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.

Der Folgebeitrag beschäftigt sich mit best Practice Lösungen zu den hier angesprochenen Problembereichen, u.a. mit Auswahlkriterien für die Wahl geeigneter Anbieter.

Sehen Sie die Problematik anders 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

September 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.