



## Einsatz von Videoconferencing-Tools (während der Corona-Krise)

Aufgrund der aktuellen Situation stehen wir vor der Aufgabe, wichtige Workshops, Besprechungen und Konferenzen mithilfe von Videokonferenzen und Online-Meetings durchzuführen. Dazu stehen Tools wie Skype, Zoom, **dfnconf** oder **Jitsi** zur Verfügung. Und auch wenn momentan wichtigere Dinge als die DSGVO im Vordergrund unserer Überlegungen stehen, so sollte man sich doch bewusstmachen, dass eine datenschutzgerechte Verwendung dieser Tools für Unternehmen und öffentliche Einrichtungen trotz Krisenzeiten wichtig ist.

Aus diesem Grund haben wir für Sie eine kleine Übersicht zusammengestellt, welche Punkte bei Nutzung einer Videokonferenz zu beachten sind und welche Maßnahmen getroffen werden sollten.

### 1. Wahl des Anbieters

- Grundsätzlich sollten EU-Programme wie dfnconf oder Jitsi solchen aus Drittländern vorgezogen werden, da sie mit den Vorgaben der DSGVO arbeiten und entweder bereits datenschutzfreundlich voreingestellt sind, oder diese Voreinstellungen mit geringem Aufwand getroffen werden können.
- Aktuell kann ZOOM in datenschutzrechtlich zulässiger Weise eingesetzt werden und ist daher als Alternative zu den teilweise überlasteten Systeme wie dfnconf zu sehen.
- Sollte ein Dienst aus einem Drittland (z.B. ZOOM) verwendet werden, so ist darauf zu achten, dass das Datenschutzniveau der DSGVO sichergestellt werden kann. Dies können z.B. sogenannte Standardvertragsklauseln sein.
- Egal, für welche Dienst Sie sich entscheiden, sowohl der Datenschutzbeauftragte als auch der Personalrat müssen informiert werden, da Sie die Arbeit mit dem Tool freigeben.

### 2. Datenschutzfreundliche Voreinstellungen

- Die Datenübertragung muss VERSCHLÜSSELT erfolgen.
- Es sollte eine GESCHÄFTLICHE NUTZUNG erlaubt sein, da manche Tools die datenschutzrechtliche Zusicherung nur im Zuge der Geschäftsnutzung garantieren (eventuell muss der Dienst dann bezahlt werden)
- Jegliche Aufzeichnungen oder Bildschirmübertragungen sollten mit einer SEPARATEN NACHFRAGE freigegeben werden müssen.
- LÖSCHUNG der Inhalte direkt nach Beendigung des Gesprächs.



- Es dürfen KEINE VERHALTENSPROFILE erstellt werden.

### **3. Erforderlichkeitsprüfung bei Aufzeichnung von Gesprächsinhalten**

Verschiedene Arten von Videokonferenzen erfordern u.U. verschiedene Arten der Aufzeichnung. So kann es sein, dass eine Konferenz wortgetreu niedergeschrieben werden muss, wohingegen ein Meeting zwischen Kollegen lediglich aufgezeichnet wird, um sich an bestimmte Aussagen zu erinnern oder Zusammenhänge darstellen zu können.

Aus diesem Grund sollte man sich vor jeder Videokonferenz folgende Fragen stellen:

- zu welchem Zweck möchte ich das Gespräch aufzeichnen (Erinnerung an zuvor Gesagtes, wortgetreue Niederschrift des Gesprächs etc.)
- gibt es datenschutzfreundlichere Lösungen (schriftliche Protokollführung während des Gesprächs o.ä.)
- Wann werden die Daten gelöscht? (sofort nach Gesprächsbeendigung, direkt nach der Niederschrift oder Freigabe der Texte.)

### **4. Datenschutzhinweise**

- Sie sind dazu verpflichtet die Kommunikationsteilnehmer unter anderem über die Zwecke, Arten und den Umfang der Verarbeitung ihrer personenbezogenen Daten im Rahmen der Konferenzen oder Webinare zu informieren (Art. 12, 13 DSGVO). Da Sie sowohl Ihre Studierenden, Forschungspartner oder Mitarbeiter belehren müssen, empfiehlt sich diese Informationen in Ihrer regulären Datenschutzerklärung aufzunehmen. Auf die Datenschutzerklärung können Sie dann per Link z. B. auf Login-Seiten oder in Einladungen zu einem Onlinemeeting hinweisen.

### **5. Auftragsverarbeitung (AV) und Technische-Organisatorische Maßnahmen (TOM)**

- Weil es bei einer Videokonferenz immer zu einer Datenübertragung kommt, muss ein sogenannter Auftragsverarbeitungsvertrag, kurz AV-Vertrag mit dem Anbieter des Dienstes geschlossen werden. Sie finden einen solchen Vertrag auch [hier](#). Viele Auftragnehmer von Online-Tools weisen jedoch auf Ihre eigenen Verträge hin, die dann digital unterzeichnet werden können. Wichtig ist hier, dass eine Prüfung des AV-Vertrages stattfindet. Vor allem die TOM sollten einen ausreichenden Schutz gewährleisten. Bei Fragen oder Unsicherheiten sollte hier immer der Datenschutzbeauftragte zu Rate gezogen werden.