Bistum Dresden-Meißen
Bischöfliches Ordinariat

Dresden, 27. November 2020

Hinweise Nutzung Videokonferenz-Plattformen

Das kirchliche Leben hängt wesentlich von Gemeinschaft und Begegnung ab. Dies ist derzeit nicht oder nur sehr eingeschränkt möglich. Videoübertragungen und Videokonferenzen (VK) können ein Weg sein, dieses Defizit ein wenig zu lindern.

I. Datenschutz

Auch wenn uneingeschränkte Nutzung von VK wünschenswert wäre, sind die datenschutzrechtlichen Maßgaben zu beachten. Es muss leider damit gerechnet werden, dass Verstöße auch in diesen außergewöhnlichen Zeiten, sanktioniert werden. Bitte beachten Sie deshalb folgende Hinweise.

Videokonferenzen auf kommerziellen Plattformen (MS-Teams, GoToMeeting, Cisco-WebEx, …) dürfen nur für den Austausch von Informationen maximal der Datenschutzklasse I genutzt werden. Daten der Datenschutzklasse II und III dürfen nur im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden. Der Austausch von schutzbedürftigen Informationen, oberhalb der Klasse III, also Daten die dem Seelsorgegeheimnis unterliegen, ist auf den derzeit zur Verfügung stehenden elektronischen Wegen unzulässig.[1] Daten, die dem Beichtgeheimnis unterliegen, dürfen weder gespeichert, noch verarbeitet noch übertragen werden.

Die Verantwortlichkeit für die Einhaltung der Datenschutzvorschriften liegt zunächst bei der Stelle, die über Mittel und Zwecke einer Verarbeitung entscheidet. Dies ist im Regelfall der/die Einladende. Werden Sie von Dritten zu einer Besprechung eingeladen, müssen Sie von dort Hinweise zur Verarbeitung ihrer personenbezogenen Daten bekommen. Bekommen Sie diese Datenschutzhinweise nicht, sollten Sie diese einfordern. Die primäre Verantwortung des/der Einladenden führt nicht dazu, dass Sie selbst gegen datenschutzrechtliche Regularien verstoßen dürfen.

Laden Sie selbst zu einer Videokonferenz ein, sind Sie für die Einhaltung der datenschutzrechtlichen Regularien voll verantwortlich. Alle VK-Teilnehmer sind über die Verarbeitung ihrer personenbezogenen Daten bei Nutzung des Videokonferenzsystems, z.B. mit der Einladungs-E-Mail, zu informieren. Z.B. kann folgender Text verwendet werden: *"Datenschutzhinweis: Zur Durchführung der Online-Konferenz verwenden wir den Dienst XY. Hinweise zur Verarbeitung Ihrer personenbezogenen Daten entnehmen Sie bitte dem beigefügten Dokument."* Möglich ist auch, die Datenschutzhinweise (Anlage) an geeigneter Stelle auf der Homepage der Pfarrei zu integrieren und in der Einladung entsprechend zu verlinken.

---

[1] Zur **Datenschutzklasse I** gehören personenbezogene Daten, deren Missbrauch keine besonders schwerwiegende Beeinträchtigung des/der Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen. **Zur Datenschutzklasse II** gehören personenbezogene Daten, deren Missbrauch die/den Betroffene/n in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z.B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, usw. **Zur Datenschutzklasse III** gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse der/des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z. B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen usw. sowie Adressangaben mit Sperrvermerken.

Mit dem Videokonferenz-Anbieter muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden. Bei der Registrierung eines Accounts des Anbieters ZOOM erfolgt der Abschluss dieses Vertrags automatisch, indem die Nutzungsbedingungen von beiden Seiten akzeptiert werden (s.u.).

In Videokonferenzen muss Ende-zu-Ende-Verschlüsselung zur Anwendung kommen. Ohne diese Sicherheitsfunktion, kann aufgrund der aktuellen EuGH-Rechtsprechung kein angemessenes Datenschutzniveau angenommen werden.

II. praktische Hinweise für die Durchführung von Videokonferenzen

Es ist Ihnen selbst überlassen, ob die Kamera aktiviert wird oder nicht. Die Kamera sollte korrekt ausgerichtet und der Bildausschnitt passend gewählt werden. Sie sollten darauf achten, dass der sichtbare Hintergrund nicht ungewollt in die Privatsphäre eingreift. Es bietet sich an, dies vor der Videokonferenz zu testen. Manche Videokonferenzsysteme bieten die Möglichkeit, den Hintergrund weich zu zeichnen (Blurrfunktion). Wenn möglich, sollten Sie sich vor Teilnahme an einer Videokonferenz mit den Einstellungsmöglichkeiten des Systems vertraut machen.

Während einer Videokonferenz können im Bildausschnitt der Kamera vertrauliche Informationen zu sehen sein, die sofort an alle anderen Teilnehmer übertragen werden. Der Aufenthaltsort eines Teilnehmers kann vertraulich sein und durch den Bildausschnitt preisgegeben werden. Ebenso können Personen, die sich im Hintergrund des Teilnehmers befinden, nun für alle Teilnehmer der Videokonferenz sicht- und hörbar sein.

Während einer Videokonferenz, kann in vielen Fällen eine Anwendung oder der Inhalt eines Bildschirms geteilt und anderen Konferenzteilnehmern gezeigt werden. Dabei entsteht die Gefahr, dass auf dem Bild oder Bildausschnitt vertrauliche Informationen eingeblendet werden, die sofort für alle Teilnehmer zu sehen sind. Beispiele hierfür sind das versehentliche Freigeben des falschen Fensters oder die Einblendung von Pop-up-Fenstern beispielsweise von empfangenen E-Mails. Es besteht weiterhin die Gefahr, dass derart offenbarte Informationen gespeichert werden, wenn etwa die laufende Konferenz aufgezeichnet wird oder andere Teilnehmer Screenshots aufnehmen. Dies kann durchaus auch unbemerkt geschehen. Schließen Sie deshalb bei Teilnahme an einer Videokonferenz unbedingt vorher alle für die Konferenz nicht benötigten Anwendungen.

Wird während einer Videokonferenz ein Desktop oder eine Anwendung auf dem Bildschirm geteilt, kann dessen Steuerung an einen anderen Konferenzteilnehmer weitergegeben werden. Dieser Teilnehmer kann unter Umständen diese Steuerung missbräuchlich verwenden. Möglich ist ein Zugriff auf vertrauliche Informationen oder die Herbeiführung von Schäden. Geben Sie deshalb bei einer Videokonferenz keine Steuerung Ihres Desktops oder einer Anwendung frei.

Melden sie sich beim Verlassen einer Videokonferenz immer ordnungsgemäß ab. Ansonsten besteht die Gefahr, dass unabsichtlich Informationen preisgegeben werden. Unbemerkt können Sie sowie Ihre Umgebung weiterhin sicht- und hörbar sein.

Sofern Sie selbst einladen, sollten Sie sich ggf. nicht scheuen, Teilnehmer von der VK auszuschließen, falls diese die Veranstaltung ernsthaft stören.

III. Empfehlung Anbieter

Aktuell bieten ein ganze Reihe seriöse und auch einige mehr oder weniger dubiose Anbieter VK-Plattformen an und wöchentlich werden es mehr. Es ist also unmöglich, eine abschließende Bewertung aller Anbieter zu leisten. Wie unter Ziff. I beschrieben, ist der/die Einladende für die Einhaltung des Datenschutzes verantwortlich. Aus heutiger Sicht können Sie unter Beachtung der Datenschutzrestriktionen (s.o.) Einladungen der Plattformen MS-Teams, GoToMeeting, Cisco-WebEx, Cisco-Jabber und ZOOM annehmen. Bezüglich der Plattform BigBlueButton kommt es darauf an, wer diese betreibt. V.a. wenn

öffentliche Einrichtungen (TU Dresden, Sächs. Staatsministerium für Kultus, …) den Betrieb leisten, können Einladungen problemlos angenommen werden.

Sofern Ihre Pfarrei selbst einladen will, kommt aus Sicht des Bischöflichen Ordinariats v.a. der Anbieter "ZOOM" in Betracht. Er bietet einen leistungsfähigen, einen funktionell vielfältigen und den datenschutzrechtlich besten Dienst für die Durchführung von Videokonferenzen und Online-Meetings an. Nur bei ZOOM kommt derzeit Ende-zu-Ende-Verschlüsselung zur Anwendung.

Lizenzierung ZOOM

Die Lizenzierung kann rel. einfach auf der ZOOM-Homepage erfolgen. Bitte nutzen Sie den Menüpunkt 'Unternehmen'. Eine günstige Möglichkeit, Lizenzen für eine Pfarrei zu erwerben bietet 'Stifter Helfen' (Haus des Stiftens gGmbH). Allerdings ist für diesen eine Akkreditierung (u.a. unter Prüfung der Gemeinnützigkeit) erforderlich. Diese nimmt angabegemäß ca. zwei Wochen in Anspruch.

Empfohlene Einstellungen

Zunächst sind Rechenzentrumsregionen für das Data-Routing (Deutschland/ Europa) festzulegen. Nachfolgend sollte die Aufzeichnung von Bild und Ton standardmäßig deaktiviert werden. Verarbeitung von personenbezogenen Daten sollte nur für die Erbringung des Videokonferenzdienstes (d.h. keine Verarbeitung von Analyse-, Telemetrie- und Diagnosedaten für eigene Zwecke des Videokonferenzdienstes) erlaubt werden.

Sichern Sie jede VK mit einem Kennwort und richten Sie einen Warteraum für die Teilnehmer ein. Treffen Sie die Festlegung, dass der Moderator anwesend sein muss, bevor die Veranstaltung beginnt. Sperren Sie die VK bei Bedarf; neue Teilnehmer können dann später nicht mehr beitreten. Legen Sie fest, dass der VK nur Personen mit einer bestimmten E-Mail-Domain beitreten können. Nutzen Sie ggf. die Einschränkung von Zugriffsrechten, d.h., Sie können z.B. festlegen, welche Personen ihren Bildschirm freigeben können.

Eine Übersicht der möglichen Sicherheitseinstellungen stellt ZOOM hier https://zoom.us/de-de/security.html bereit.

IV. Empfehlungen Technik

Videokonferenz-Apps und Browsernutzung

Die Videokonferenz-Plattformen versuchen i.d.R. eigene Applikationen auf den Rechnern zu installieren. Tatsächlich werden bestimmte (tlw. nachrangige) Funktionalitäten erst durch die Nutzung der Apps nutzbar. Allerdings impliziert die aus der Installation erwachsende Programmvielfalt in der Wartung durchaus Folgekosten. Es wird deshalb empfohlen, zunächst stets die Browser-Version der jeweiligen Plattform zu nutzen, auch wenn die Anbieter den entsprechenden Link absichtlich i.d.R. eher klein darstellen. Für Videokonferenzen sollte generell der Browser 'Google-Chrome' oder 'MS-Edge' (bzw.. 'Safari' in der Apple-Welt) genutzt werden. Bitte beachten Sie die ggf. erforderlichen Datenschutz-Einstellungen auf dem jew. Browser. Lediglich für die Plattform auf die Sie selbst einladen, sollte die App installiert werden.

Reservierung

Sofern die Pfarrei mehrere VK-Räume durch mehrere Anwender nutzen will, stellt sich die Frage der zeitlichen Reservierung. Hierfür können Papier-Kalender ebenso wie elektronische Systeme (z.B. MS-OUTLOOK, …) genutzt werden.

Bandbreite und IT-Sicherheit

Für eine VK wird pro Teilnehmer bei normaler Videoauflösung eine Bandbreite von ca. 2 Mbit/S benötigt. Falls in Ihrer Pfarrei mehrere Personen an mehreren Computern an einer oder mehreren VK teilnehmen, empfiehlt es sich, die Bandbreite des DSL-Anschlusses zu prüfen (Vertrag) und ggf. zu erweitern.

Für die Nutzung von VK-Plattformen kann die entsprechende Konfiguration der Firewall erforderlich werden. Es wird empfohlen, nur die notwendige Ports frei zu schalten.

Arbeitsplätze

Sofern Laptops zur Verfügung stehen, reichen die eingebauten Kameras, Mikrophone und Lautsprecher für seltenen Gebrauch i.d.R. aus. Zur Verbesserung der Nutzbarkeit oder für Desktop-PC empfiehlt es sich, Aufsteck-Kameras (die Geräte in der 50 €-Preisklasse reichen völlig aus), Headsets oder kleine aktive Lautsprecher zu nutzen.

Streaming von Veranstaltungen

Sofern Sie bspw. Gottesdienste streamen wollen, sollte v.a. eine semiprofessionelle Kamera (Preisklasse ab ca. 1.000 €), entsprechende Beleuchtung, ein hinreichend leistungsfähiger Computer sowie passende Übertragungstechnik (Kabel, Router, Switche, …) zum Einsatz kommen. Hier empfiehlt sich bereits in der Phase der Bestellung, professionelle IT-Unterstützung in Anspruch zu nehmen.

Technik Konferenzräume

Soll die Videokonferenz-Nutzung regelmäßig durch mehrere Personen in einem Raum ermöglicht werden, können All-In-One-Geräte (z.B. Polycom Poly Studio oder Logitech MeetUp) in der Preisklasse von ca. 1.000 € empfohlen werden. Diese Geräte verfügen über ausreichend große Lautsprecher sowie sich automatisch auf die/den Sprecher(in) ausrichtende Mikrofone und Kameras. Die Installation erfolgt rel. einfach auf dem zu nutzenden Computer.