Videokonferenzsysteme in Kirche und Diakonie

Jede Software-Auswahl und -einführung bedarf eines planmäßigen Vorgehens in drei Schritten:

a) Interne Interessengruppen formulieren möglichst präzise ihren Bedarf.
b) Die Leitung initiiert eine Prüfung der Machbarkeit mit Vorgaben anhand interner und gesetzlicher Rahmenbedingungen. Verwaltung, MAV, QM, und IT erarbeiten mit Beratung durch den/die Datenschutzbeauftragte(n) (DSB) eine Beschlussvorlage für die Leitung.
c) Die Leitung entscheidet und sichert die Ergebnisse über einen Soll-/Ist Abgleich.

12-Punkte-Liste für die Überprüfung oder Planung des datenschutzkonformen Einsatzes einer Videokonferenzlösung

1. Liste: Welche datenschutzrelevanten Themen und Begriffe werden durch den Einsatz berührt (Beschäftigtendatenschutz, Auftragsverarbeitung, Zusammenarbeit über den kirchlichen Bereich hinaus, Sozialdatenschutz, Privatgeheimnisse nach § 203 StGB)?
2. Liste: Welche Verarbeitungen sind geplant bzw. betroffen (Sichtung und ggf. Ergänzung des Verarbeitungsverzeichnisses und der Beschreibung der Verarbeitungen)?
3. Einschätzung: Sind die Zwecke der Verarbeitung legitim und wann ist die Erforderlichkeit für eine Kommunikation z. B. per Video-/Chat- statt per Telefonkonferenz gegeben?
4. Liste: Welche Datenkategorien sollen verarbeitet werden?
5. Liste: Welche internen und externen Personen bzw. Gruppen (Konferenzpartner) werden betroffen sein (Beschäftigte, Berufsgeheimnisträger, Minderjährige, Patienten usw.)?
6. Gremien: Mitwirkungsrechte beachten! (MAV; ggf. Bewohnervertretungen)
7. Würdigung: Welche Rechtsgrundlage nach DSG-EKD erlaubt die Verarbeitung an sich? (Die Einwilligung sollte wegen der hohen Anforderungen das letzte Mittel der Wahl sein.)
8. Gibt es weitere Erlaubnistatbestände z. B. durch kirchliche Arbeitsrechtsregelungen wie eine Dienstvereinbarung oder die AVR oder andere spezialgesetzliche Regelungen?
9. Schwellwertanalyse: Besteht ein hohes Risiko für Betroffene? (Wenn ja, dann ist unter Anleitung der Datenschutzbeauftragten eine Datenschutz-Folgenabschätzung durchführen)
10. Datenschutz-Folgenabschätzung und Risikobehandlungsplan (Welche technisch-organisatorischen Maßnahmen müssen als Anforderungen an die Software und deren Benutzung gestellt werden – ggf. spezifisch für Gruppen von Betroffenen?)
11. Anforderungskatalog: Funktionen, Dokumentation, Service, Sicherheit, Datenschutz
12. Beschlussvorlage: Für welche Produkte kann bestätigt werden, dass sie die Anforderungen erfüllen und wie hoch ist der damit verbundene geschätzte Aufwand?

Diese Liste adressiert die verantwortliche Stelle als Organisator der Videokonferenz. Für die Fälle, bei denen Beschäftigte an extern organisierten Videokonferenzen teilnehmen (sollen), obliegt es den Dienstgebern, ihre Beschäftigten aufzuklären und dafür zu sensibilisieren, dass auch die externen Organisatoren Informationspflichten nach DSG-EKD, KDG oder der DSGVO haben.

Ergänzende Informationen aus bestehenden Veröffentlichungen der Aufsichtsbehörde

a) Hinweise zum Einsatz von Videokonferenzsystemen – kompakt vom 15. April 2020[1]
b) Handreichung – Anforderungen an Videokonferenzsysteme vom 16. April 2020[2]
c) Es gilt wie in ganz Europa: Jedwede Verarbeitung von personenbezogenen Daten unterliegt dem Verbot mit Erlaubnisvorbehalt. Neben einer Einwilligung führt § 6 DSG-EKD weitere Erlaubnistatbestände, wie beispielweise die Erfüllung eines Vertrages oder den Schutz lebenswichtiger Interessen an. Für besondere personenbezogene Daten, die eines höheren Schutzniveaus bedürfen, gilt § 13 DSG-EKD.
d) Für den Beschäftigtendatenschutz gilt ausschließlich § 49 DSG-EKD in Verbindung mit den Grundsätzen nach § 5, weil es sich hierbei um eine abgeschlossene Regelung handelt.

Appell für Zusammenarbeit und gegenseitige Unterstützung

Der Aufwand zur Etablierung und Aufrechterhaltung datenschutzkonformer Arbeitsprozesse mit geeigneten Arbeitsmitteln ist nicht zu unterschätzen und eine stetige Aufgabe.

Der kirchliche Gesetzgeber hat im Einklang mit dem europäischen Datenschutzrecht keine Unterschiede oder Vereinfachungen beim geforderten Datenschutzniveau für kleine kirchliche Träger und Einrichtungen vorgesehen.

Daraus ergeben sich Herausforderungen, die kleine Organisationen möglicherweise nur im Rahmen von Kooperationen beherrschen können.

Prüfungen durch die Aufsichtsbehörde

Alle Datenschutzaufsichtsbehörden sind verpflichtet, die Einhaltung datenschutzrechtlicher Regelungen zu überwachen und durchzusetzen.

Mit den gesetzlich geregelten Befugnissen setzt der Datenschutzbeauftragte für Kirche und Diakonie dies durch anlasslose und anlassbezogene Schwerpunktprüfungen um.[3] Die 12-Punkte-Liste ist zusammen mit dem kirchlichen Datenschutzmodell (KDM)[4] eine der möglichen Grundlagen dafür.

20. August 2021

Der Datenschutzbeauftragte für Kirche und Diakonie

Aufsichtsbehörde für den Datenschutz gemäß Kapitel 6 DSG-EKD

- der Evangelisch-Lutherischen Landeskirche Sachsens
- der Evangelischen Landeskirche Anhalts
- des Diakonischen Werkes der Ev.-Luth. Landeskirche Sachsens e.V.
- des Diakonischen Werkes Evangelischer Kirchen in Mitteldeutschland e.V.

[1] https://dsbkd.de/hinweise-zum-einsatz-von-videokonferenzsystemen-kompakt/
[2] https://dsbkd.de/anforderungen-an-videokonferenzsysteme/
[3] zum Umfang der Befugnisse siehe § 44 DSG-EKD
[4] Das Kirchliche Datenschutzmodell (https://kirchliches-datenschutzmodell.de)

Anhang

Problematik bei US-amerikanischen Herstellern/Anbietern von Apps und Cloud-Diensten

Die meisten der bekannten Videokonferenzsysteme (z. B. GoToMeeting, Google Meet, Microsoft Skype, Teams, Zoom…) werden von Herstellern bzw. Dienstanbietern bereitgestellt, die einerseits wegen ihrer Geschäftstätigkeit hier europäisches Datenschutzrecht anwenden, gleichzeitig jedoch vorrangigem US-amerikanischem Recht unterliegen, wodurch es zur Kollision der Normen kommt.

Seit 16. Juli 2020 gelten die USA gemäß Urteil des Europäischen Gerichtshofs (EuGH) in Bezug auf den Datenschutz als unsicheres Drittland. In Bezug auf personenbezogene Daten sind jegliche Übermittlungen in die USA (und andere unsichere Drittländer) oder jegliche Verarbeitung auf IT-Systemen, die unter der Hoheit US-amerikanischer Unternehmen stehen, unzulässig, wenn nicht sichergestellt ist, dass unrechtmäßige Datenzugriffe, z. B. durch US-amerikanische Behörden, effektiv verhindert werden können.

Der bereits bestehende Einsatz von Lösungen wie den oben Genannten in Kirche und Diakonie muss der geltenden Rechtslage folgen oder sollte inzwischen, für den Fall, dass ein rechtskonformer Einsatz technisch nicht ermöglicht werden konnte, eingestellt und durch geeignete Lösungen ersetzt worden sein. Der EuGH hatte in seinem Urteil keine Übergangsfrist eingeräumt, so dass die Pflicht zu Umsetzung bereits seit der Urteilsverkündung besteht.

Deutsche und europäische Alternativen

Es gibt eine Reihe von Videokonferenzsystemen, die für ihre Angebote in Deutschland ausschließlich europäischem, britischem oder auch Schweizer Recht (Angemessenheit bestätigt) unterliegen (z. B. Nextcloud Talk, Teamviewer Meeting, Jitsi Meet, Wire, BigBlueButton. So erlaubt beispielsweise „Wire“ die Ende-zu-Ende-verschlüsselte Konferenz per Einladungslink an externe Gesprächsteilnehmer, die zur Teilnahme lediglich einen Webbrowser benötigen. So können auch Beratungsgespräche bei Bedarf anonym durchgeführt werden. Für Gesprächssituationen mit besonders sensiblen Informationen, z. B. in Videosprechstunden mit Patienten gibt es Empfehlungen der Kassenärztlichen Bundesvereinigung[5] und eine Liste zertifizierter Anbieter[6].

Ergänzung zu Nr. 2 auf der 12-Punkt-Liste

Mit Videokonferenzsystemen werden neben den Personendaten auch gesprochene Worte, geschriebene Texte, Fotos vom Bildschirm oder Videoaufzeichnungen usw. verarbeitet. Wie sehr diese Daten zu schützen sind, ergibt sich meistens schon durch die Art des Gespräches, z. B.:

- Bewerbungsgespräch
- Schwangerschaftskonfliktberatung
- Suchtberatung
- Mitgliederversammlung mit Wahlen
- MAV-Sitzung
- …

[5] https://www.kbv.de/html/videosprechstunde.php
[6] https://www.kbv.de/media/sp/liste_zertifizierte-Videodienstanbieter.pdf

Beschäftigte sind nicht ohne Rechte (und Pflichten)

Für Beschäftigte und deren externe Gesprächsbeteiligte besteht bei Nutzung US-amerikanischer Dienste die Gefahr einer anlasslosen staatlichen Überwachung ihrer Daten, gegen die in den USA keine ausreichenden Rechtsschutzmöglichkeiten bestehen. Mit ihren Rechten als Betroffene müssen Beschäftigte das nicht akzeptieren. Kritik und Fragen können Dienstgeber nicht dadurch „umschiffen“, indem sie ein solches Videokonferenztool als Arbeitsmittel für alle einführen und – nicht selten, ohne die pflichtgemäße Einbeziehung der Mitarbeitervertretung – vorschreiben.

Ein Appell gilt den Mitarbeitervertretungen, dafür zu sorgen, dass Beschäftigte geschult und regelmäßig über ihre Rechte und Pflichten auch im Datenschutz informiert werden. Beschäftigte können sich ohne Umwege direkt bei der Aufsichtsbehörde beschweren, wenn sie wissen oder vermuten, dass ihre Datenschutzrechte verletzt worden sind.

Privat oder kirchlich ist nicht egal.

Privatpersonen verwenden mit WhatsApp, TikTok, Facebook, Instagram, Discord usw.) Apps und Dienste mit großer Verbreitung und „bezahlen“ diese kostenfreien Angebote mit ihren persönlichen Daten. Einige dieser Angebote haben Funktionen für Chat- und Videokonferenzen integriert. Deren Nutzung wird Firmen und damit auch Trägern und Einrichtungen aus Kirche und Diakonie denkbar einfach gemacht.

Doch was Privatpersonen für sich selbst entscheiden können, steht für die geschäftliche Nutzung unter dem Vorbehalt der Erfüllung aller datenschutzrechtlichen Anforderungen durch die verantwortliche kirchliche Stelle. Durch die besondere Konstellation[7] beim Betreiben einer Fanpage auf Facebook durch Organisationen werden neben datenschutzrechtlichen sogar kirchenpolitische Fragen berührt, wenn zu überlegen ist, ob es im kirchlichen Interesse liegt, gemeinsam als wirtschaftliche[8] Partner von Unternehmen wie Facebook oder Instagram bei deren Art der Verarbeitung von personenbezogenen Daten mitzuwirken?

Die Zulässigkeit und der durch technisch-organisatorische Maßnahmen flankierte Einsatz unterliegt den gleichen hier bereits ausführlich dargestellten Bedingungen und sollte wie bei klassischen Videokonferenzsystemen mittels der vorgestellten 12-Punkte-Liste geprüft werden.

[7] Mit Urteil vom 05.06.2018 (Az. C-210/16) hatte der EuGH entschieden, dass für Daten, die beim Besuch einer Facebook-Seite verarbeitet werden, eine geteilte Verantwortlichkeit zwischen Fanpage-Inhaber und Facebook für die Datenhandhabung besteht

[8] Mit Beiträgen bei Facebook und Instagram Menschen zu gewinnen, sich für einen Bundesfreiwilligendienst in Einrichtungen der Diakonie zu bewerben, hat neben den vordergründig genannten Vorteilen für die angesprochene Zielgruppe auch ganz handfeste wirtschaftliche Gründe für die Einrichtungen. In diesem Sinne treten Facebook und Instagram und die diakonische Einrichtung mit ihrer Fanpage als Partner mit je eigenen wirtschaftlichen Interessen auf. Dabei vergrößert die Fanpage der kirchlichen Einrichtung den Wirkungskreis des Plattform-Anbieters.