DER DATENSCHUTZBEAUFTRAGTE
FÜR KIRCHE UND DIAKONIE

Datenschutzaufsichtsbehörde gemäß Kapitel 6 DSG-EKD für:

Ev.-Luth. Landeskirche Sachsens
Evangelische Landeskirche Anhalts
Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e.V.
Diakonisches Werk Evangelischer Kirchen in Mitteldeutschland e.V.

Datenschutzbeauftragter
Herr Pierre Große

Reichenbrander Str. 4
09117 Chemnitz

Tel.: 0351 4692-460
Fax: 0351 4692-469

Datenschutzbeauftragter@evlks.de

Handreichung

Anforderungen an Videokonferenzsysteme

Aktenzeichen
HAR.005.2020.01

Datum:
16.04.2020

Intention

Der Einsatz eines "Videokonferenzsystems“ bzw. einer „Anwendung für Web-Sessions" (im Weiteren Anwendung) für ein nutzer-übergreifendes Arbeiten von unterschiedlichen Standorten aus, ist per se nicht bedenklich in Bezug auf den Datenschutz. Jedoch widersprechen das außer Achtlassen der Sorgfalt in Bezug auf die technischen und organisatorischen Maßnahmen und fehlende Regularien dem Datenschutz.

Nachfolgende Anforderungen sollen bei der Auswahl und Einstellung einer entsprechenden Software helfen, um Datenschutzaspekte zu berücksichtigen. Die Regelungen zur Anschaffung von Software in der kirchlichen Stelle oder diakonischen Einrichtung sind ebenfalls zu beachten.

Das eigene Ausprobieren von Software-Lösungen durch Nutzer kann zu unbeabsichtigten Beeinflussungen mit anderer Software desselben Gerätes führen. Deshalb ist die Einbeziehung der EDV-Abteilung unabdingbar.

Business-Version

Für die dienstliche Verwendung sind Anwendungen ungeeignet, die für den privaten Einsatz vorgesehen sind bzw. für deren geschäftliche Nutzung es keine Lizenzen gibt und keine eigenen vertraglichen Regelungen abgeschlossen werden können. Damit sind Apps wie **WhatsApp oder FaceTime** grundsätzlich ungeeignet. Gleichgültig ob es sich um kostenfreie Softwarelösungen handelt, muss sich die verantwortliche Stelle im erforderlichen Umfang davon überzeugen, dass bei Nutzung der Anwendung alle erforderlichen Sicherheitsstandards für die dienstliche Kommunikation mit ihren Vertraulichkeits- oder Geheimhaltungsanforderungen erfüllt werden können.

Verschlüsselung; Datensicherheit

Werden über das Videokonferenzsystem besondere Kategorien personenbezogener Daten nach § 4 Nr. 2 DSG-EKD ausgetauscht, ist sowohl eine gesicherte Verbindung (Transportverschlüsselung) als auch – bei Speicherung derartiger Daten beim Dienstleister (Auftragsverarbeiter) – eine Verschlüsselung der Daten (Inhalts- bzw. End-to-End-Verschlüsselung) notwendig. Dies gilt auch, wenn kommunizierte Sachverhalte Betriebs- oder Geschäftsgeheimnissen unterliegen oder der Geheimhaltung bedürfen.

Bei bestehender Vertraulichkeits- und Geheimhaltungsverpflichtung ist von Anbietern abzusehen, welche einen Zugriff auf Inhaltsdaten nicht ausschließen, weil gegenüber diesen u. a. die Verpflichtung als „sonstige Mitarbeitende“ (siehe Abschnitt „Weitere organisatorische Maßnahmen“) nicht realisierbar ist.

Aufgrund dessen, dass in Software permanent Sicherheitslücken geschlossen werden, ist darauf zu achten, dass stets die aktuelle Version der Anwendung verwendet wird.

Möglichkeit, Aufnahmen der Videokonferenz zu regulieren

Anwendungen bieten inzwischen die Möglichkeit an, die Videokonferenz aufzunehmen, d. h. Daten über den Zeitraum der eigentlichen Konferenz hinaus zu speichern. Grundsätzlich ist das nur mit einer Einwilligung aller Teilnehmer einer Konferenz zulässig. Teilnehmenden an einer Videokonferenz sollte es freigestellt werden, die Kamera ihres Computers zu aktivieren, um ein Live-Bild von sich zu übertragen. Bei Aufzeichnung wird in der Regel auch der Ton erfasst. Bei fehlender Zustimmung kann Strafbarkeit wegen Verletzung der Vertraulichkeit des Wortes (§ 201 Abs. 1 StGB) vorliegen.

Daher sollte einstellbar sein, dass vor dem Start der Aufnahme bei allen Teilnehmern eine Nachricht mit den nötigen Informationen erscheint, sowie die Option, zuzustimmen oder abzulehnen. Die Nachweisbarkeit der Einwilligung/Zustimmung ist sicherzustellen.

Blurr-Möglichkeit

Videokonferenz-Anwendungen bieten teilweise die Möglichkeit, den Hintergrund vollständig auszugrauen oder durch einen gewählten Hintergrund zu ersetzen, damit beispielsweise bei Home Office der heimische Hintergrund, durchs Bild laufende Personen oder beim Arbeiten außer Haus die fremde Umgebung nicht mit übertragen werden. Sofern dies in der Anwendung nicht möglich ist, sind in einer dienstlichen Nutzerordnung oder -richtlinie Anforderungen an die Nutzungsumgebung vorzugeben.

Einrichtung von Zugangsbeschränkungen, Datensparsamkeit

Der Zugang zu einer Videokonferenz ist eindeutig zu reglementieren, so dass ungebetene Gäste außen vor bleiben. Zugangsbeschränkungen wie Login (bei Gästen nur mit Zustimmung des Organisators der Videokonferenz) sind dringend erforderlich, sonst können auch ungebetene

oder nicht eingeladene Gäste an der Videokonferenz teilnehmen[1]. Es besteht die Gefahr von Geheimhaltungs- oder Vertraulichkeitsverletzungen.

Besondere Aufmerksamkeit ist auf extern angeschlossene Kameras und extern angeschlossene Mikrofone zu richten. Über diese kann unter Umständen Schadsoftware eingespielt oder unbemerkt ein Mitschnitt der Konversation vorgenommen werden. Auch ein sogenanntes Bombing ist möglich, wenn das Videokonferenzsystem Sicherheitsdefizite aufweist. Dabei klicken sich sogenannte Trolle[2], zum Beispiel durch Erraten der Meeting-ID, in laufende Videokonferenzen ein und fügen unerwünschte oder sogar illegale Inhalte ein.

Deshalb muss das Konferenzsystem einen Schutz vor nicht geladenen Gästen einer Videokonferenz aufweisen, indem beispielsweise zu einer Meeting-ID automatisch auch ein Passwort generiert wird, sobald eine neue Einladung erstellt wird.

Es sollte darauf geachtete werden, dass Zugangsdaten nur mit ausgewählten Partnern geteilt werden.

Chatverläufe und Daten- bzw. Dateiaustausch

Es ist sicherzustellen, dass Chatverläufe nur für den benötigten Zeitraum zur Verfügung stehen und danach automatisch gelöscht werden. Beim Chat dürfte dies nach Ende der Videokonferenz der Fall sein. Bei Dateiaustausch kann z. B. ein Zeitraum von wenigen Stunden oder einem Tag gewählt werden, innerhalb dessen die Videokonferenzteilnehmer Zeit haben, die Daten herunterzuladen und anderweitig abzulegen. Ergänzend sollte als organisatorische Maßnahme geregelt werden, welche Arten von Dokumenten (nicht) über das Konferenzsystem geteilt werden dürfen. Dies kann sowohl als Black- oder als White-Liste ausgestaltet werden (siehe unten).

Beschränkung von Logfiles

Solange Daten gespeichert sind, muss dafür immer ein Grund bzw. Zweck vorliegen und für die Verarbeitung eine Rechtsgrundlage nach § 6 DSG-EKD bekannt sein (Grundsatz der Rechtmäßigkeit). Logfiles können beispielsweise für die Fehlerbehebung durch die EDV oder den Dienstleister (AV-Vertrag s. u.) notwendig sein. Wichtig ist, dass die Daten dann nur zu diesem Zweck verwendet werden und nach Wegfall des Zwecks wieder gelöscht werden.

Einsatz bei Bewerbungsverfahren

Sollen Bewerbungsgespräche via Videokonferenz durchgeführt werden, bedarf dies der sorgfältigen Prüfung im Voraus. Die Anforderungen nach § 49 DSG-EKD sowie die Transparenzpflichten (§ 17 DSG-EKD) sind zu beachten. Die Löschung eventuell gespeicherter Daten nach Abschluss des Bewerbungsverfahrens ist sicherzustellen (§ 49 Abs. 7 DSG-EKD).

[1] So konnte die Fachzeitschrift c't an einer internen Sitzung zum Coronavirus mit Bayerns Innenminister Joachim Herrmann teilnehmen: https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html

[2] Trolle sind im Netzjargon Personen, die ihre Kommunikation im Internet auf Beiträge beschränkt, die auf emotionale Provokation anderer Gesprächsteilnehmer zielen.

Weitere organisatorische Maßnahmen

Wie die Videokonferenzlösung genutzt werden darf und welche Einschränkungen bestehen, sollte geregelt sein, beispielsweise in einer Verfahrensanweisung oder in einer Nutzerrichtlinie. So sind die Mitarbeiter dahingehend zu sensibilisieren, welche Daten und/oder Unterlagen sie (vor allem mit Externen) teilen dürfen. Aus "Black-/White-Listen" sollte hervorgehen, welche Daten geteilt bzw. nicht geteilt werden dürfen. Auf dem geteilten Bildschirm sollten keine Benachrichtigungen über neue Mails erscheinen. Verfügt ein Mitarbeiter über mehrere Bildschirme, sollte der für die Videokonferenz verwendete Bildschirm nicht der als Hauptanzeige konfigurierte Bildschirm sein.

Sofern eine Geeignetheit zur Verhaltens- und Leistungsauswertung besteht, sind entsprechende Verfahren mitbestimmungspflichtig.

Anwendungen für Videokonferenzen werden meist als „Software as a Service“ (SaaS) betrieben. Damit liegt in der Regel eine Auftragsverarbeitung vor, die eines Vertrages nach § 30 DSG-EKD (AV-Vertrag) bedarf. Ein Vertrag nach Art. 28 DSGVO ist gemäß § 30 Abs. 5 Satz 2 DSG-EKD möglich. Die weiteren Anforderungen an die Auswahl des Auftragsverarbeiters, die Prüfung und Dokumentation der Vertragsausführung sowie die vertragsrechtlichen Regelungen aus § 30 DSG-EKD sind zu beachten. Bei der Prüfung sind die technischen und organisatorischen Maßnahmen (§ 27 DSG-EKD bzw. bei nichtkirchlichen Dienstleistern Art. 32 DSGVO) des Anbieters zu berücksichtigen.

Findet eine Übermittlung in ein Drittland (außerhalb der EU/des EWR) statt, sind zusätzlich die Voraussetzungen nach § 10 DSG-EKD zu erfüllen.

Ist nicht ausgeschlossen, dass der Anbieter personenbezogene Daten bzw. Inhalte aus der Kommunikation zwischen einem Berufsgeheimnisträger i. S. v. § 203 StGB und seinem Patienten bzw. Klienten zur Kenntnis nehmen kann, ist der Anbieter als „sonstiger Mitwirkender“ auch auf § 203 StGB zu verpflichten. Andernfalls bleibt die strafrechtliche Verantwortung für Vertraulichkeitsverletzungen durch den Anbieter beim Berufsgeheimnisträger. Eine allgemeine Geheimhaltungsklausel im AV-Vertrag ist nicht ausreichend.

Für die Nutzer des Video-Konferenzsystems sind die Informationen nach § 17 DSG-EKD in geeigneter Weise (u. a. verständlich und leicht zugänglich) zur Verfügung zu stellen. Sofern der Anbieter entsprechende Informationsflächen bereitstellt, über welche die eigenen Datenschutzhinweise integriert werden können, sind diese zu nutzen. Die Informationen sollten spätestens beim Betreten des virtuellen Videokonferenzraumes möglichst über Buttonlösungen zugänglich sein.

Für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf wird auf die Technische Leitlinie Sichere TK-Anlagen (BSI TL-02103) des Bundesamt für Sicherheit in der Informationstechnik[3] sowie dessen Hinweise zur Auswahl eines geeigneten Video-

[3] https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_htm.html

konferenzsystems, einschließlich Kriterienkatalog mit Gewichtungspunkten hingewiesen.[4] Datenschutzrechtliche Kerninformationen zu einzelnen Diensten können der Anlage II zur GDD-Praxishilfe DS-GVO XVI „Videokonferenzen und Datenschutz“ entnommen werden[5].

Die Nutzung des Videokonferenzsystems sollte im Verzeichnis der Verarbeitungstätigkeiten nach § 31 DSG-EKD dokumentiert werden.

Der bzw. die zuständige betriebliche Datenschutzbeauftragte ist einzubeziehen, um die Ordnungsmäßigkeit der Verarbeitung sicherzustellen. Es ist zu prüfen, ob eine Datenschutzfolgenabschätzung nach § 34 DSG-EKD vorzunehmen ist. Ggf. ist eine solche durchzuführen und entsprechend § 34 Abs. 4 DSG-EKD zu dokumentieren. Geht aus der Datenschutzfolgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko zur Folge hat und kann das Risiko nicht durch technische oder organisatorische Maßnahmen minimiert werden, ist nach § 34 Abs. 9 DSG-EKD die Datenschutzaufsichtsbehörde zu konsultieren.

Stand: 16.04.2020

Der Datenschutzbeauftragte für Kirche und Diakonie

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/TKAnlagen/TLSTK_II-Teil_3%E2%80%93Beschaffungsleitfaden.pdf
[5] https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz