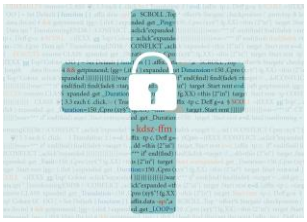

Katholisches Datenschutzzentrum
Frankfurt/M. KdöR

Beurteilungskriterien zur Auswahl eines Online-Meeting-Tools und Hinweise auf die zu berücksichtigenden technischen und organisatorischen Maßnahmen

Vorbemerkung

Auch über das Jahr 2020 hinaus bleiben Dienste und Software für virtuelle Besprechungen und Sitzungen, also Online-Meeting-Tools, für viele Einrichtungen im Zuständigkeitsbereich des Katholischen Datenschutzzentrums Frankfurt/M. relevant. Bei der Beurteilung eines Online-Meeting-Tools müssen auch Aspekte des Datenschutzes beachtet werden. Insbesondere seit dem sogenannten „Schrems II"-Urteil des Europäischen Gerichtshofs (EUGH) v. 16. Juli 2020 (C-311/18), welches den Einsatz von Online-Meeting-Tools drastisch erschwert, deren Anbieter in den USA und in anderen Ländern ohne Angemessenheitsbeschluss beheimatet sind, ist die Unsicherheit darüber, was zulässig ist und was nicht, stark gestiegen. Dieses Dokument stellt einige Hinweise bereit, die bei der Auswahl eines geeigneten Anbieters unterstützen sollen. Als eine erste Hilfestellung erhebt sie jedoch keinen Anspruch auf Vollständigkeit.
Vorab ist darauf hinzuweisen, dass zuerst geprüft werden sollte, ob eine geplante virtuelle Sitzung überhaupt als Videokonferenz erfolgen muss oder als Telefonkonferenz erfolgen kann. Im Sinne von Datensparsamkeit und Datenminimierung ist immer der Telefonkonferenz der Vorzug zu geben.

1. Welche Beurteilungskriterien sollten bei der Auswahl eines Online-Meeting-Tools herangezogen werden?

Zunächst gilt es bei der Auswahl des Online-Meeting-Tools festzulegen, welche Kriterien dafür relevant sind.

1.1 Besteht die Möglichkeit, ein Online-Meeting-Tool selbst zu betreiben?

Der Betrieb eines Online-Meeting-Tools unter eigener Kontrolle (gegebenenfalls unter Einbeziehung externer Unterstützung) kann die Einhaltung von Anforderungen des Datenschutzes erleichtern, da mehr Gestaltungsspielraum besteht.

1.2 In welchen Staaten werden personenbezogene Daten verarbeitet und werden personenbezogene Daten in Drittstaaten exportiert?

1.2.1 Verarbeitung in Deutschland / EWR

Wenn möglich, sind Online-Meeting-Tools aus Deutschland oder der EU bzw. dem EWR zu bevorzugen, da diese unmittelbar den Vorgaben der DSGVO (bzw. des KDG) unterliegen und somit ein angemessenes Schutzniveau gewährleistet ist. Es ist hierbei zu prüfen, dass der

Anbieter keine Auftragsverarbeiter (besonders für Cloud-Hosting) in einem Drittland ohne angemessenes Schutzniveau beschäftigt. Regelmäßig ist dies bei Anbietern der Fall, die dem CLOUD-Act der Vereinigten Staaten (US-CLOUD-Act) unterliegen.

1.2.2 Verarbeitung in einem Drittland

Nach § 40 Abs. 1 KDG ist die Datenübermittlung an oder in ein Drittland oder an eine internationale Organisation zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt und dieser Beschluss wichtigen kirchlichen Interessen nicht entgegensteht.

Liegt nach § 40 Abs. 1 KDG kein Angemessenheitsbeschluss vor, dann kann die Datenübermittlung zulässig sein, wenn in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind (§ 40 Abs. 2 Nr. 1 KDG) oder der Verantwortliche oder der Auftragsverarbeiter nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, davon ausgehen kann, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen (§ 40 Abs. 2 Nr. 2 KDG).

Liegen die Voraussetzungen des § 40 KDG jedoch nicht vor, so kann unter den Voraussetzungen des § 41 KDG in Ausnahmefällen eine Datenverarbeitung in einem Drittland zulässig sein.

Das erwähnte „Schrems II“-Urteil des EuGH stellte klar, dass das zwischen der EU und den USA vereinbarte „Privacy Shield“-Abkommen keine einem Angemessenheitsbeschluss vergleichbare Garantie darstellt. Datenübermittlungen in die USA lassen sich seither nicht mehr durch Berufung auf § 40 Abs. 1 KDG rechtfertigen. [1, 2]

Mit Bezug auf geeignete Garantien für den Schutz personenbezogener Daten durch rechtsverbindliche Instrumente (§ 40 Abs. 2 Nr. 1 KDG) hat der EuGH festgestellt, dass EU-Standardvertragsklauseln (Standard Contractual Clauses, SCC) weiterhin grundsätzlich als Rechtsgrundlage für die Drittlandsübermittlung dienen können. Allerdings können sie dennoch ungenügend sein, wenn die Rechtsordnung des Drittlandes die dortigen staatlichen Stellen zu Datenzugriffen befugt, die in der EU nicht vergleichbar zulässig sind. Am Beispiel des konkreten Falles der Datentransfers in die USA hat der EuGH daher festgestellt, dass rein vertragliche Maßnahmen nicht ausreichend sein können und dass zusätzliche technische und organisatorische Maßnahmen nötig sein könnten, beispielsweise eine starke Ende-zu-Ende-Verschlüsselung (s. u. Abschn. 1.4 und 1.5).

1.3 Auftragsverarbeitung

Als Auftragsverarbeiter werden Dienstleister bezeichnet, die personenbezogene Daten ihrer Kunden oder Mitarbeiter entsprechend deren Weisungen verarbeiten.

Auch Anbieter von Video- und Online-Konferenzdiensten sind grundsätzlich als Auftragsverarbeiter anzusehen, sodass die Maßgaben der §§ 29 ff. KDG zu beachten sind. Ferner müssen die Angaben zu technischen und organisatorischen Maßnahmen sowie zu eingesetzten Subunternehmern geprüft werden.

Beispiele:

- Der Anbieter muss die Weisungsbefugnis des Kunden (= Verantwortlicher) anerkennen (inkl. Prüfungsbefugnis)
- Der Anbieter nennt im Vertrag seine Zulieferer (insbesondere Hosting-Plattformen)
- Der Anbieter sichert dem Verantwortlichen vertraglich die Unterstützung bei Maßnahmen zur Wahrung der Betroffenenrechte zu

Zumindest im Falle von Anbietern in Drittstaaten ohne Angemessenheitsbeschluss (s.o.) müssen die Auftragsverarbeitungsverträge die jeweils gültigen EU-Standardvertragsklauseln zum Datenschutz enthalten (3). Der Anbieter muss ggf. darauf hinweisen, dass es neben regulären Drittlandübermittlungen aufgrund der Jurisdiktion im Lande geltende rechtliche Verpflichtungen des Anbieters zur Weitergabe personenbezogener Daten geben kann (z.B. an Sicherheitsbehörden im Rahmen des US-CLOUD-Act). Wie oben erwähnt, kann es sein, dass diese vertraglichen Regelungen nicht ausreichen, um einen zulässigen Datentransfer zu ermöglichen. Jeder Verantwortliche ist verpflichtet, die Rechtslage im Drittland zu prüfen und gegebenenfalls vor dem Datentransfer in ein Drittland geeignete Maßnahmen zu ergreifen, um ein mit der Europäischen Union vergleichbares Datenschutzniveau sicherzustellen.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat Videokonferenzdienste verschiedener Anbieter untersucht, mit dem Schwerpunkt auf der Bewertung der Rechtskonformität der von den Anbietern angebotenen Auftragsverarbeitungsverträge [4].

Die Datenschutzerklärungen, die den Konferenzteilnehmern im Zuge der Konferenzteilnahme durch den Auftragsverarbeiter präsentiert oder zugänglich gemacht werden, sollten mit der vertraglich vereinbarten Datenverarbeitung verglichen werden, um gegebenenfalls Hinweise auf eine Datenverarbeitung des Auftragsverarbeiters zu finden, die mit dem Auftrag nicht in Einklang zu bringen ist. Gegebenenfalls muss die Datenschutzerklärung durch den Verantwortlichen noch ergänzt werden.

1.4 Werden Daten verschlüsselt versendet?

Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Hier ist besonders die Verschlüsselung der Daten relevant. § 27 KDG fordert, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Eine Verschlüsselung darf deshalb nicht „optional zuschaltbar“ sein, sondern sollte vorgegeben werden.
Es gilt im Einzelfall zu bestimmen, welche Art von Verschlüsselung benötigt wird. Dies hängt letztlich von der Art der Daten ab, die verarbeitet werden. So kann eine Verschlüsselung zwischen den Endpunkten der Kommunikation und beteiligten Servern (Transportverschlüsselung) ausreichend sein, bei einem höheren Risiko für die Rechte und Freiheiten der betroffenen Personen jedoch eine Verschlüsselung notwendig sein, die personenbezogene Daten vor den Betreibern der beteiligten Server verbirgt (Ende-zu-Ende-Verschlüsselung).

Als Hilfestellung können Zertifizierungen des Produktes oder des Anbieters durch unabhängige Institutionen herangezogen werden.

1.5 Werden übermittelte Dateien, aufgezeichnete Videomitschnitte oder Fotos nach einem festgelegten Zeitraum gelöscht?

§ 7 Abs. 1 lit. c) KDG fordert eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß. Die Beschränkung gilt für die Datenmenge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist darauf zu achten, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden.

Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende-Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z. B. durch staatliche Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server ins Leere.

1.6 Werden weitere Daten versendet?

Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden (§ 7 Abs. 1 lit. a) KDG). Der Betroffene hat nach §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch Online-Meeting-Tools.
Daher ist zu klären, ob nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet werden und ob der Anwender die Kontrolle über die bei ihm hinterlegten Kontaktdaten Anderer behält. Bei einigen gängigen Online-Meeting-Tools wird z. B. die komplette Kontaktliste an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt. Dies gilt es zu vermeiden.

1.7 Ist es notwendig, eine Business-Version zu verwenden?

Für die Verwendung in Einrichtungen eignen sich in der Regel keine Tools, die für den ausschließlich privaten Einsatz gedacht sind. Sollte man sich trotzdem für eine private Version entscheiden, gilt es darauf zu achten, dass die geschäftliche Nutzung erlaubt ist (da datenschutzrechtliche Zusicherungen auf Geschäftskunden beschränkt sein können).

In jedem Fall sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt werden. Von Anbietern wird teilweise die nicht-private Nutzung der privaten Versionen untersagt, teilweise wird lediglich die kommerzielle Anwendung untersagt. Das bedeutet, dass die Nutzung des Produkts durch ehrenamtliche Non-Profit-Organisationen möglich ist, für eine kommerzielle Nutzung aber der Erwerb einer Business-Version erforderlich ist.

Sollten auch Jugendliche an einer Telekonferenz teilnehmen müssen, ist darauf zu achten, dass ein Mindestalter entsprechend geregelt ist. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren.

Weiter sollte man vorab überprüfen, wie viele Personen in der Regel bei den Telekonferenzen teilnehmen und die Lizenzvereinbarungen dahingehend überprüfen, ob diese Menge von der Lizenz mitumfasst ist.
Zuletzt ist auch auf eine örtliche Begrenzung des Dienstes zu achten. Manche Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

1.8 Werden Logfiles (Protokolldateien) erstellt?

Logfiles sollten nur erstellt werden, soweit diese erforderlich sind. Diese können auch für die Fehlerbehebung durch den Dienstleister notwendig sein. Logfiles sind dann nur zu diesem Zweck zu verwenden und nach Wegfall des Zwecks wieder zu löschen.

1.9 Wie lange werden personenbezogene Daten gespeichert?

Hier ist sicherzustellen, dass Dateien und personenbezogene Daten nur für den benötigten Zeitraum zur Verfügung stehen und danach automatisch gelöscht werden. Bei einer Telekonferenz dürfte dies nach Ende des Telefonats der Fall sein. Werden Dateien ausgetauscht, kann z. B. ein Zeitraum von wenigen Stunden oder einem Tag gewählt werden, innerhalb dessen die Teilnehmer Zeit haben, die Daten herunterzuladen und anderweitig abzulegen. Ergänzend sollte als organisatorische Maßnahme geregelt werden, welche Arten von Dokumenten (nicht) über das Online-Meeting-Tool geteilt werden dürfen. Dies kann sowohl als Black- oder als Whitelist ausgestaltet werden.

1.10 Findet ein Tracking oder Profiling statt?

Es sollten keine Verhaltensprofile der Teilnehmer gebildet werden. Es sollte ein Entscheidungskriterium sein, dass der Anbieter bzw. die verwendete Software kein Tracking oder Profiling durchführen kann, alternativ sollte eine Funktion für Tracking oder Profiling abgeschaltet werden.

1.11 Verarbeitet der Anbieter personenbezogene Daten zu eigenen Zwecken?

Eine Verarbeitung personenbezogener Daten zu eigenen Zwecken des Anbieters sollte vermieden werden. Falls dies doch geschieht, sollten diese Zwecke eindeutig und so speziell wie möglich beschrieben sowie in ihrer Anzahl eng begrenzt und mit dem KDG vereinbar sein. Ebenfalls ist hier auf Transparenz gegenüber den betroffenen Personen zu achten.

2. Welche technischen und organisatorischen Maßnahmen sind bei der Verwendung des gewählten Tools zu berücksichtigen?

Nach der Entscheidung für den Anbieter ist zu prüfen, welche technischen und organisatorischen Maßnahmen anzuwenden sind. Welche insbesondere hierfür relevant erscheinen, finden Sie untenstehend.

2.1 Können die Datenschutzeinstellungen innerhalb des Online-Meeting-Tools manuell angepasst werden?

Bei vielen Tools ist es notwendig, die Datenschutzeinstellungen richtig zu konfigurieren, um einer möglichen unzulässigen Datenverarbeitung vorzubeugen. Hier sollte insbesondere ein besonderes Augenmerk auf der Datensparsamkeit liegen.

2.2 Wer nimmt an der Telekonferenz teil?

Einladungen sollten nur an Personen vergeben werden, die für die behandelten Themen die nötige Freigabe haben. Dies kann durch die Einrichtung von Zugangsbeschränkungen (z. B. über

Login-Daten) oder durch die einzufordernde Zustimmung des Organisators bei der Teilnahme von Gästen geschehen.

Zudem sollte geregelt sein, dass Zugangsdaten nicht an Dritte weitergegeben werden dürfen, da dann nicht gewährleistet werden kann, dass lediglich die Personen teilnehmen, die die nötige Freigabe haben. Für regelmäßige Sitzungen in geschlossenem Teilnehmerkreis sollten individuelle Zugänge verwendet werden, um Fremde fern zu halten [4]. Die Teilnehmer sollten dann idealerweise zufällig generierte Passwörter benutzen.

Beispiele:

- Es gibt ein Rollenkonzept (privilegierter Moderator vs. einfache Teilnehmer).
- Ein Moderator kann unbefugt Teilnehmende abweisen oder entfernen.
- Das Tool selbst gewährt den Zugang zu einer Konferenz standardmäßig nur nach Abfrage personenindividueller Merkmale (typischerweise mit Nutzername und Passwort).
- Für Videokonferenzen im Rahmen von regelmäßigem Schulunterricht im Klassenverband werden individuelle Zugänge verwendet, um bei einer unerlaubten Weitergabe eines Zugangs diesen gezielt sperren zu können.

2.3 Auf was muss beim Screen-Sharing geachtet werden?

Es ist unbedingt darauf zu achten, dass nur für das Online-Meeting relevante Informationen zu sehen sind. Es empfiehlt sich, unnötige Inhalte und Fenster zu schließen und einen separaten Desktop einzurichten, auf dem keine Dateien oder Verknüpfungen zu sehen sind.

2.4 Was ist im Hintergrund der Teilnehmer zu sehen?

Es muss darauf geachtet werden, dass keine Informationen im Hintergrund der Teilnehmer zu sehen sind, die nicht für die anderen Teilnehmer der Konferenz bestimmt sind. Es sollte insbesondere sichergestellt werden, dass keine unbeteiligten Personen im Bild sichtbar werden. In Räumen, in denen mehrere Personen zugegen sind, oder eintreten können, müssen die Personen auf laufende Videokonferenzen hingewiesen werden.

Beispiel: Da auch Personen von privaten Räumen aus an Videokonferenzen teilnehmen sollen, wird ein Online-Meeting-Tool verwendet, welches das Verschleiern von Hintergründen (Hintergrundbilder oder „Blurring“) erlaubt.

2.5 Darf die Videokonferenz aufgezeichnet werden?

Viele Tools bieten mittlerweile die Möglichkeit, die Videokonferenz aufzunehmen. Dies ist in den meisten Fällen nur mit einer Einwilligung aller Teilnehmer zulässig. Daher sollte das Tool so eingestellt werden können, dass vor Start der Aufnahme bei allen Teilnehmern eine Nachricht mit den nötigen Informationen erscheint sowie die Option besteht, zuzustimmen oder abzulehnen.

Beispiele:

- Nur ein Moderator kann die Aufzeichnung starten.
- Allen Teilnehmern wird unmissverständlich angezeigt, dass eine Aufzeichnung (gerade) stattfindet.
- Die Aufzeichnungsfunktion kann zentral für alle Nutzer – auch für Moderatoren – deaktiviert werden.

- Die automatische Löschung von Konferenzaufzeichnungen auf Seiten des Anbieters muss nach einer festgelegten Speicherfrist stattfinden.

2.6 Wie kann Datenschutzverstößen durch Teilnehmer vorgebeugt werden?

Insbesondere sind die Teilnehmer entsprechend zu informieren und zu sensibilisieren, welche Daten über das Tool (vor allem auch mit Externen) geteilt werden dürfen.

3. Weitere Hinweise

Ob und ggf. welche arbeitsrechtlichen – vor allem mitarbeitervertretungsrechtlichen – Aspekte bei der Nutzung von Online-Meeting-Tools bzw. Online-Meeting-Services zu beachten sind, unterliegt nicht datenschutzrechtlicher Beurteilung. Es wird hierzu eine eigene Prüfung empfohlen.

4. Schlussbemerkung

Aufgrund der Menge an Online-Meeting-Tools ist es nicht möglich, eine allgemeinverbindliche Lösung anzubieten. Dieses Dokument soll daher als Entscheidungshilfe dienen, sich – in Abhängigkeit der jeweils vorliegenden Situation – für einen passenden Anbieter zu entscheiden. Jeder Verantwortliche ist freilich verpflichtet, die Werkzeuge, die er nutzen möchte, eingehend auf deren Vereinbarkeit mit den Datenschutzvorschriften zu prüfen.

5. Literatur

1. Datenschutz-Orientierungshilfe des Kath. Datenschutzzentrums Frankfurt/M. August 2020
2. Kernaussagen des Urteils des EuGH vom 16. Juli 2020 im Verfahren Schrems II (Publikation des Bundesbeauftragten für den Datenschutz und die Informationssicherheit vom 8.10.2020)
3. EU Standardvertragsklauseln - DeutschDorothee Wiegand: Ungebetene Gäste, in c't magazin für computer technik, Nr. 5, 13.02.2021
4. Untersuchung der Berliner Beauftragten für Datenschutz und Informationsfreiheit von Videokonferenzdienste verschiedener Anbieter, mit dem Schwerpunkt auf der Bewertung der Rechtskonformität der von den Anbietern angebotenen Auftragsverarbeitungsverträge: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf