**Katholisches Datenschutzzentrum Frankfurt/M.**

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

## Vorbemerkung:

Derzeit erreichen das Katholische Datenschutzzentrum Frankfurt/M. vermehrt Anfragen nach der datenschutzgerechten Nutzung von Online-Meeting-Tools bzw. Online-Meeting-Services. Es ist für Einrichtungen, Organisationen und Unternehmen von essenzieller Bedeutung, zu erfahren, auf welche Kriterien zu achten ist, wenn ein Online-Meeting-Tool bzw. ein Online-Meeting-Service benutzt werden soll. Um bei der Menge der heutigen Anbieter den Überblick nicht zu verlieren und den passenden zu finden, stellt dieses Dokument einige Hinweise bereit, die bei der Auswahl des richtigen Anbieters unterstützen sollen. Diese Zusammenstellung versteht sich als eine erste Hilfestellung, die keinen Anspruch auf Vollständigkeit erhebt.

Vorab ist darauf hinzuweisen, dass zuerst geprüft werden sollte, ob das virtuelle Treffen als Video- oder als Telefonkonferenz erfolgen muss bzw. 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-Services festzulegen, welche Kriterien dafür relevant sind.

### 1.1 Gibt es ein eigenes Videochat-Tool?

Sollten Sie ein eigenes internes Videochat-Tool besitzen, ist dieses vorrangig heranzuziehen, da hier in der Regel keine Datenverarbeitung durch einen Dritten/Auftragsverarbeiter stattfindet.

### 1.2. In welchem Land befindet sich der Serverstandort?

#### 1.2.1 Serverstandort Deutschland/ EU

Wenn möglich, sind Online-Meeting-Services 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.

### 1.2.2 Serverstandort 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 nicht vor, so kann unter den Voraussetzungen des § 41 KDG in Ausnahmefällen eine Datenverarbeitung in einem Drittland zulässig sein.

## 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.

## 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 insbesondere 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. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind. Dies kann durch eine sichere Datenhaltung in der Applikation, die die Daten z. B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt, gewährleistet sein.

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

### 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?

Weiter 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-Services 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.

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-Services.

### 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 privaten Einsatz gedacht sind. Sollten Sie 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 der Telekonferenz dürfte dies nach Ende des Meetings 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 den Online-Meeting-Service geteilt werden dürfen. Dies kann sowohl als Black- oder als Whitelist ausgestaltet werden.

### 1.10 Findet ein Profiling statt?

Es sollten keine Verhaltensprofile der Teilnehmer gebildet werden oder diese Funktion sollte abgeschaltet werden können. Sollte die Möglichkeit der Abschaltung des Profilings bestehen, so ist diese vorzunehmen.

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

Nach der Entscheidung für den Anbieter muss noch geprüft werden, welche technischen und organisatorischen Maßnahmen anzuwenden sind. Welche insbesondere hierfür relevant erscheinen, finden Sie untenstehend.

### 2.1 Können die Datenschutzeinstellung innerhalb des Online-Meeting-Services manuell angepasst werden?

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

### 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.

### 2.5 Dürfen die Zugangsdaten an Dritte weitergeben werden?

Zugangsdaten sollten nicht an Dritte weitergegeben werden, da dann nicht gewährleistet werden kann, dass lediglich die Personen teilnehmen, die die nötige Freigabe haben.

### 2.6 Darf die Telekonferenz 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.

### 2.7 Wie kann Datenverstößen vorgebeugt werden?

Vor allem 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. Fazit

Aufgrund der Menge an Online-Meeting-Services 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.