

Weiter zu beachten

Die Nutzung von Online-Meeting-Tools bzw. Online-Meeting-Services kann mitbestimmungspflichtig durch die Arbeitnehmervertretung sein! Diese Einschätzung unterliegt nicht datenschutzrechtlicher Beurteilung. Es wird hierzu eine eigene Prüfung empfohlen.

Ausführlichere Informationen zum Thema

Arbeitshilfe Online-Meeting-Tools (KDSZ Frankfurt/M.):

<https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Online-Meeting-Tools-04-2022-KDSZ-FFM.pdf>

Handreichung zu Videokonferenzsystemen (LfDI Baden-Württemberg):

<https://www.baden-wuerttemberg.datenschutz.de/videokonferenzsysteme/>

Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten:

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

Kath. Datenschutzzentrum Frankfurt/M. Diözesandatenschutzbeauftragte

für die Mittel- und Südwestdeutschen Bistümer

(Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier

Domplatz 3, 60311 Frankfurt a.M.
Tel.: 069 8008718-800
E-Mail: info@kdsz-ffm.de

Die weiteren Diözesandatenschutzbeauftragten der Katholischen Kirche sind:

Norddeutsche Bistümer

(Erz-)Bistümer Hamburg, Hildesheim, Osnabrück, Münster (niedersächsischer Teil)

Katholische Datenschutzaufsicht Nord Diözesandatenschutzbeauftragter

Unser Lieben Frauen Kirchhof 20, 28195 Bremen
Tel.: 0421 330056-0
E-Mail: info@kdsa-nord.de

Ostdeutsche Bistümer und Katholischer Militärbischof

(Erz-)Bistümer Berlin, Dresden-Meißen, Erfurt, Görlitz, Magdeburg

Kirchliche Datenschutzaufsicht Diözesandatenschutzbeauftragter

Badepark 4, 39218 Schönebeck
Tel.: 03928 7179018
E-Mail: kontakt@kdsa-ost.de

Nordrhein-Westfälische Bistümer und VDD

(Erz-)Bistümer Aachen, Essen, Köln, Münster (nordrhein-westfälischer Teil), Paderborn

Katholisches Datenschutzzentrum Diözesan- und Verbandsdatenschutzbeauftragter

Brackeler Hellweg 144, 44309 Dortmund
Tel.: 0231 138985-0
E-Mail: info@kdsz.de

Bayerische Bistümer

(Erz-)Bistümer Augsburg, Bamberg, Eichstätt, München-Freising, Passau, Regensburg, Würzburg

Gem. Datenschutzaufsicht der bayerischen (Erz-)Dözesen Diözesandatenschutzbeauftragter

Kapellenstraße 4, 80333 München
Tel.: 089 21371796
E-Mail: jjoachimski@eomuc.de



Kath. Datenschutzzentrum
Frankfurt/M.

Auswahl und Nutzung von Online-Meeting-Tools



Auswahl und Nutzung von Online-Meeting-Tools

Dienste und Software für virtuelle Besprechungen und Schulungen, also Online-Meeting-Tools, sind aus dem Arbeitsalltag nahezu aller kirchlichen Einrichtungen nicht mehr wegzudenken. Bei der Beurteilung eines solchen Tools sind auch Aspekte des Datenschutzes zu beachten. Insbesondere seit dem sog. „Schrems II“-Urteil des EuGH vom 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. Dieser Flyer stellt kurz gefasste Hinweise bereit, die bei der Auswahl eines geeigneten Anbieters unterstützen sollen und gibt Anweisungen, worauf bei der Durchführung von Online-Meetings geachtet werden sollte.



Beurteilungskriterien bei der Auswahl

- On-Premises-Betrieb ist möglich; das Betreiben eines Online-Meeting-Tools unter eigener Kontrolle kann die Einhaltung von Anforderungen des Datenschutzes erleichtern, da mehr Gestaltungsspielraum besteht.
- Das Hosting hat in sicheren Staaten (EWR und Staaten mit Angemessenheitsbeschluss) zu erfolgen.
- Die Anbieter sind grundsätzlich Auftragsverarbeiter, sie müssen die Maßgaben der §§ 29, 30 KDG befolgen: u. a. die Weisungsbefugnis des Verantwortlichen anerkennen, Zulieferer benennen (insbesondere Hosting-Plattformen), bei Maßnahmen zur Wahrung der Betroffenenrechte unterstützen.
- Eine Verschlüsselung, die bereits voreingestellt sein muss. Die Verschlüsselung zwischen den Endpunkten der Kommunikation (Transportverschlüsselung) kann in vielen Fällen ausreichend sein, bei einem höheren Risiko für die Rechte und Freiheiten der betroffenen Personen wird jedoch eine Verschlüsselung notwendig sein, die personenbezogene Daten vor den Betreibern der beteiligten Server verbirgt (Ende-zu-Ende-Verschlüsselung).
- Der Anbieter soll alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich löschen.
- Es soll kein Zugriff auf Daten des Rechners (z. B. Adressenliste) durch den Messenger erfolgen.
- Lizenzbedingungen sind zu prüfen (z. B. nur privater Gebrauch, Business-Lizenzen, Teilnehmerbegrenzung, Altersbegrenzung).
- Die datenschutzfreundliche Erhebung und Behandlung von Logdateien sollte Berücksichtigung finden.
- Kein Tracking oder Profiling soll möglich sein, falls doch vorhanden, muss eine derartige Funktion abgeschaltet werden können.
- Verfolgt der Anbieter eigene Zwecke?

Notwendige technische und organisatorische Maßnahmen

- Die Datenschutzeinstellungen müssen manuell konfigurierbar sein, z. B. zur Begrenzung von Datenerhebung oder Datenweitergabe.
- Teilnehmende sind nach dem Need-to-know-Prinzip einzuladen.
- Das Tool bietet ein Rollenkonzept (privilegierter Moderator vs. einfache Teilnehmer).
- Ein Moderator kann unbefugt Teilnehmende abweisen oder entfernen.
- Personalisierte Zugänge sind für alle Teilnehmer einzurichten (Nutzername, Passwort, eventuell 2. Faktor).
- Screen-Sharing: nur für das Online-Meeting relevante Informationen anzeigen. Unnötige Inhalte und Fenster sind vorher zu schließen.
- Es ist sicherzustellen, dass im Hintergrund keine Informationen und insbesondere keine unbeteiligten Personen im Bild sichtbar werden (Hintergrundbilder oder „Blurring“ verwenden). Andere Personen sind auf laufende Videokonferenzen hinzuweisen.
- Bei Aufzeichnung von Videokonferenzen ist zu beachten:
 - Nur ein Moderator kann die Aufzeichnung starten.
 - Die Aufzeichnung von Videokonferenzen erfordert die informierte Einwilligung der Teilnehmenden.
 - Allen Teilnehmern wird unmissverständlich angezeigt, dass eine Aufzeichnung (gerade) stattfindet.
 - Konferenzaufzeichnungen werden automatisch durch den Anbieter nach einer festgelegten Speicherfrist gelöscht.