Bund Evangelisch-Freikirchlicher Gemeinden in Deutschland K.d.ö.R.
www.baptisten.de

Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz
Johann-Gerhard-Oncken-Str. 7 | 14641 Wustermark
datenschutzbeauftragter@baptisten.de

Stellungnahme und Handlungsempfehlungen des Bundesbeauftragten für Datenschutz bei der Nutzung der Videokonferenzsoftware des Anbieters Zoom Video Communications, Inc.

Durch die Coronakrise und die damit einhergehenden Einschnitte, nicht nur für das alltägliche Leben, sondern vor allem auch das Gemeindeleben, suchen Gemeinden nach Möglichkeiten der Gemeinschaft. Das Internet bietet auch hier hervorragende Möglichkeiten, Gemeinschaft zumindest virtuell zu leben.
Viele Gemeinden greifen nicht nur auf die Möglichkeit des Gottesdienstabrufs bzw. Live-Streamings per Podcast oder YouTube zurück, sondern halten auch Web-Meetings ab.

I. AK-Internet und BigBlueButton

Der AK Internet (https://www.ak-internet.de) bietet Gemeinden eine tolle Plattform, solche Treffen abzuhalten. Dabei setzt der AK Internet auf die frei verfügbare Konferenzsoftware BigBlueButton, deren Quellcode für jedermann einsehbar ist. Das System wird auf einem eigenen Server in einem deutschen Rechenzentrum gehostet, es ist sichergestellt, dass alle datenschutzrelevanten Daten diesen Server nicht verlassen. Die Schwäche des Konferenzsystems BigBlueButton liegt jedoch leider bei den Endgeräten der sich einwählenden Nutzer: Sind diese nicht leistungsstark genug, ist die Videokonferenz mit mehr als 20 Personen derzeit nur schwer durchzuführen. Das Team der Entwickler von BigBlueButton arbeitet an einer Lösung. Grundsätzlich empfehle ich ausdrücklich, dem System des AK Internet vor allen anderen Lösungen den Vorzug zu geben. Der AK-Internet stellt auf seiner Internetseite https://miteinander.ak-internet.de weitere (auch datenschutzrechtliche) Informationen zur Verfügung. Auch bei Inanspruchnahme des Angebots des AK-Internet muss freilich darauf geachtet werden, einen ggf. notwendigen Auftragsverarbeitungsvertrag abzuschließen. Teilnehmer einer Konferenz sind über entsprechende Datenschutzerklärungen der verantwortlichen Stelle zu informieren. Dies kann z.B. durch die Verlinkung einer auf der Homepage der verantwortlichen Stelle befindlichen Datenschutzerklärung in einer Einladungs-E-Mail geschehen.

II. Zoom

Ein Shootingstar hat sich in den vergangenen Monaten mit als 300 Millionen Konferenzteilnehmern täglich klar an der Spitze der Konferenzsystemanbieter positioniert: Die Firma Zoom Video Communications, Inc. überzeugt durch ein äußerst anwenderfreundliches System. Die Kritik am US-amerikanischen Video-Dienst im Hinblick auf die (Daten-) Sicherheit reißt jedoch nicht ab, sodass eine datenschutzrechtliche Prüfung angezeigt ist.

1. Zoombombing

   In den vergangenen Wochen erregte Zoom vor allem Aufmerksamkeit durch das sogenannte „Zoom-bombing“. Dabei platzen nicht autorisierte Personen in Konferenzen herein und teilten dort unerwünschte (oft pornografische und rassistische) Inhalte. Dies geschah vorzugsweise in Unterrichtsangeboten oder aber auch Gottesdiensten. Jedes Zoom-Meeting erhält eine individuelle URL, die eigentlich nur den Konferenzteilnehmern bekannt sein sollten. Hacker schreiben jedoch automatisierte Skripte, die verschiedene URLs generieren und gleichzeitig testen, ob diese URL tatsächlich einer Konferenz zugeordnet ist. Ist dies der Fall, wird der Hacker über einen solchen Treffer informiert und platzt ungebeten in die Konferenz herein. Konferenzveranstalter können dies verhindern, indem sie Zoom-Meetings mit einem zusätzlichen Passwort schützen - dies hindert Hacker wirksam daran, selbst bei einem URL-Treffer an der Konferenz teilzunehmen.

Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz
Johann-Gerhard-Oncken-Str. 7 | 14641 Wustermark
datenschutzbeauftragter@baptisten.de

2. Aufmerksamkeitstracking

   Zu Recht kritisiert wurde auch eine Aufmerksamkeitstrackingfunktion. Diese analysiert die Kamerabilder der Teilnehmer und kann so feststellen, ob diese auch aufmerksam zuhören, indem sie überprüft, ob die Augen des Teilnehmers auf das Konferenzfenster blicken oder aber der Teilnehmer z. B. nebenbei in einem anderen Anwendungsfenster surft. Der Konferenzveranstalter erhielt eine entsprechende Nachricht.

   Die Firma Zoom reagierte auf die Kritik und hat diese Funktion inzwischen standardmäßig deaktiviert. Die Funktion darf nur in begründeten Fällen und nach vorheriger Information aller Teilnehmer wieder aktiviert werden. Andernfalls verstößt die Konferenz gegen unser Kirchenrecht.

3. Facebookeinbindung in der iOS-App

   Im März 2020 wurde zudem bekannt, dass die iOS-App der Firma Zoom ohne vorherige Information der Nutzer Daten an die Firma Facebook übertrug. Dabei war es egal, ob der Nutzer tatsächlich über ein Facebook-Konto verfügte oder nicht. Zoom entschuldigte sich und erklärte, dass durch die geschaffene Möglichkeit für Nutzer, sich bei Zoom selbst mit ihrem Facebook-Konto einzuloggen, versehentlich die Datenübertragungsfunktion an Facebook in einem von Facebook bereitgestellten SDK nicht deaktiviert wurde.

   Das Problem ist inzwischen behoben.

4. Datentransfer über China und andere Nicht-EU-Länder

   Zoom stand weiter in der Kritik, den durch die Konferenz verursachten Datenverkehr (Traffic) über Länder wie China zu leiten und damit gegen geltendes Datenschutzrecht zu verstoßen. Zoom hat auch hier reagiert: Inzwischen können zahlende Kunden auswählen, durch welche Regionen ihr Traffic geroutet wird, und bestimmte Regionen gezielt deaktivieren. Es ist also beim Erstellen von Konferenzen unbedingt darauf zu achten, dass nur EU-Rechenzentren ausgewählt werden. Für die Nutzer der kostenlosen Version ist sichergestellt, dass kein Routing mehr über China stattfindet. **Etwas anderes gilt jedoch dann, wenn sich ein Teilnehmer aus der asiatischen Region einwählt. Konferenzen sind dann nicht mehr in datenschutzrechtlich zulässiger Weise durchführbar!**

5. Zugriff auf Windows-Benutzernamen und Passwörter

   Bis zum 01.04.2020 war es Angreifern auf einfache Art und Weise möglich, über die auf einem PC installierte Software Zoom auf Windows-Benutzernamen und Passwörter zuzugreifen und diese an einen eigenen Server zu übermitteln. Problematisch war die Schwachstelle deshalb, weil das abgefangene Passwort in einigen Fällen auch als Passwort für Online-Accounts von Microsoft wie Outlook oder Office365 dient. So hatten Angreifer die Möglichkeit, mit den abgefangenen Daten auch E-Mails der Opfer zu lesen oder in der Cloud gespeicherte Dokumente und Bilder anzusehen.

   Die Lücke ist inzwischen geschlossen.

Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz
Johann-Gerhard-Oncken-Str. 7 | 14641 Wustermark
datenschutzbeauftragter@baptisten.de

6. Zoom-Account-Passwörter

   Am 13.04.2020 wurde bekannt, dass die Benutzerdaten von 500.000 Zoom-Nutzern von Hackern im Internet zum Kauf angeboten werden. Experten sind sich jedoch einig, dass diese Daten nicht aus einem Hack der Zoom-Plattform stammen, sondern von den Tätern im Rahmen einer sogenannten Credential-Stuffing-Attacke zusammengetragen wurden. Bei einem solchen Angriff werden bereits im Netz kursierende Datensätze aus alten Hacks anderer Webangebote verwendet, um diese automatisiert auf ein neues Ziel, in diesem Fall Zoom, anzuwenden. Immer dann, wenn eine bereits bekannte Kombination aus E-Mail-Adresse und Passwort dabei als funktionierend erkannt wird, wird sie in den auf diese Weise neu entstehenden Datensatz aufgenommen.

   Es ist daher dringend angezeigt (und sollte selbstverständlich sein!), für den Dienst Zoom ein eigenes starkes Passwort zu generieren. Starke Passwörter können z. B. mit dem Gaijin Passwort Generator (https://www.gaijin.at/en/tools/password-generator) generiert werden.

7. Verschlüsselung

   Zoom-Konferenzen verfügen über keine Ende-zu-Ende-Verschlüsselung. Es ist also nicht sichergestellt, dass die Verbindung zwischen den einzelnen Teilnehmer-Endgeräten verschlüsselt ist. Lediglich die Verbindung zwischen den Teilnehmern und dem Zoom-Server ist verschlüsselt. Bei Zoom selbst jedoch liegen alle Daten unverschlüsselt vor. Der Anbieter hat damit uneingeschränkten Zugriff auf sämtliche Konferenz-Daten. Zoom muss es aufgrund des Auftragsverarbeitungsvertrages (hierzu sogleich mehr) nach § 19 DSO-Bund (bzw. Art. 28 DSGVO) freilich unterlassen, diese Daten zu eigenen Zwecken oder durch unbefugte Weitergabe zu nutzen, da es andernfalls vertragsbrüchig werden würde und sich empfindlichen Strafen ausgesetzt sähe. Trotzdem ist die Nutzung von Zoom in den Fällen zu unterlassen, in denen vertrauliche Informationen ausgetauscht werden, also zum Beispiel zum Zwecke der Seelsorge oder für solche Gebetskreise, in denen personenbezogene Daten ohne ausdrückliche Einwilligung der betroffenen Personen ausgetauscht werden. Die bloße Bekanntgabe eines Gebetsanliegens bzw. die Bitte einer betroffenen Person, sich einem Anliegen durch Gebet anzunehmen, stellt keine datenschutzrechtliche Einwilligung dar. Es sollte in diesen Fällen auf die Plattform des AK-Internet zurückgegriffen werden.

   Die Firma Zoom hat ein sog. Feature-Freeze der eigenen Software verhängt, dies bedeutet, dass derzeit keine neuen Funktionen entwickelt werden. Stattdessen soll die Sicherheit der Software weiter verbessert werden. So wurde am 09.04.2020 angekündigt, das beschriebene Verschlüsselungsproblem innerhalb von 45 Tagen zu beheben. Am 13.05.2020 teilte man nun mit, am 22.05.2020 lediglich ein erstes Verschlüsselungskonzept vorstellen zu wollen.

III. Sonstige Datenschutz- und Sicherheitsvorwürfe

Der wohl prominenteste deutsche Datenschützer, der hamburgische Beauftragte für Datenschutz und Informationsfreiheit Prof. Dr. Johannes Caspar, bezweifelte zuletzt in einem Interview für das Handelsblatt die Datensicherheit Zooms und äußert Bedenken. Dabei wird er jedoch nicht konkret. Es ist durchaus denkbar, dass der Behörde weitere Informationen vorliegen, die derzeit nicht öffentlich zugänglich sind. Beachtlich ist auch, dass die New Yorker Generalstaatsanwältin Letita James laut einem Bericht der New York Times wegen der Datenschutz- und Datensicherheitspraxis Untersuchungen gegen Zoom eingeleitet hat. Der

Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz
Johann-Gerhard-Oncken-Str. 7 | 14641 Wustermark
datenschutzbeauftragter@baptisten.de

Dienst habe unter anderem nicht schnell genug reagiert, solche Sicherheitslücken zu stopfen, die Angreifern den direkten Zugriff auf die Webcams der Zoom-Nutzer ermöglichten. Zoom steht stark unter Beschuss, es ist durchaus denkbar, dass solche Sicherheitslücken oder gegen das Datenschutzrecht verstoßende Verfahren öffentlich werden, die eine Nutzung des Dienstes datenschutzrechtlich ausschließen. **Verantwortliche Stellen sollten sich daher überlegen, ob es sinnvoll ist, Jahresabonnements mit der Firma Zoom abzuschließen.**

IV. Pflichten von verantwortlichen Stellen bei der Zoom-Nutzung

Zoom verarbeitet personenbezogene Daten von Teilnehmern (E-Mail-Adresse, Name, aber auch Konferenzinhalte) im Auftrag der verantwortlichen Stelle, die die Konferenz veranstaltet. Es ist daher zunächst darauf zu achten, dass „Inhaber" des Zoom-Kontos die verantwortliche Stelle selbst oder eine andere Stelle des Bundes und nicht ein Gemeindemitglied oder Freund der Gemeinde ist. Vor **(!)** der Nutzung von Zoom ist ein Vertrag zur Auftragsverarbeitung nach § 19 DSO-Bund, Art. 28 DSGVO mit Zoom abzuschließen. Nach § 19 DSO-Bund darf die verantwortliche Stelle nur mit solchen Auftragsverarbeitern zusammenarbeiten,

> *„ … die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Schutz der Rechte der betroffenen Person gewährleistet und*
>
> *a) konform zu den Anforderungen dieser Ordnung erfolgt, wenn der Auftragsverarbeiter eine Stelle des Bundes ist oder anderenfalls;*
>
> *b) konform zu den Anforderungen dieser Ordnung oder der Verordnung EU 2016/679 erfolgt. … "*

Es ist letztlich auf die DSGVO abzustellen, der die Verordnung EU 2016/679 zugrunde liegt. Ich sehe die Voraussetzungen des § 19 DSO-Bund bzw. Art. 28 DSGVO in Übereinstimmung mit anderen Datenschutzexperten derzeit als erfüllt an. Seit dem 08.04.2020 erfolgt der Abschluss des Auftragsverarbeitungsvertrages automatisch durch Registrierung eines Zoom-Accounts und Annahme der Zoom-Nutzungsbedingungen, durch die automatisch alle unter www.zoom.us/legal verlinkten Dokumente in das Vertragsverhältnis einbezogen werden. Dies ist Ziff. 19 der Nutzungsbedingungen zu entnehmen. Dort heißt es:

> *19. PRIVACY AND OTHER POLICIES. Use of the Services is also subject to Zoom's Privacy Policy, a link to which is located at the footer on Zoom's website. The Privacy Policy, and all policies noticed at www.zoom.us/legal are incorporated into this Agreement by this reference.*

Zu Deutsch (Übersetzung durch den Autor):

> *„19. Datenschutz und andere Richtlinien. Die Nutzung des Dienstes ist zudem Gegenstand der Zoom-Datenschutzrichtlinien, auf die ein Link im Footer der Zoom-Webseite verweist. Die Datenschutzrichtlinien sowie alle Richtlinien, die Gegenstand der Seite www.zoom.us/legal sind, werden durch Verweis in diese Nutzungsbedingungen einbezogen."*

Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz
Johann-Gerhard-Oncken-Str. 7 | 14641 Wustermark
datenschutzbeauftragter@baptisten.de

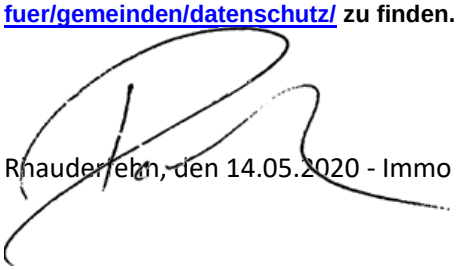
In den vergangenen Wochen haben mich mehrfach E-Mails verantwortlicher Stellen erreicht, die Bedenken im Hinblick auf den Abschluss eines englischsprachigen Vertrages haben. Bestehen solche Bedenken und wird aus diesem Grund ein Vertrag mit Zoom nicht abgeschlossen, sollte es selbstverständlich sein, dass der Dienst von der verantwortlichen Stelle nicht genutzt werden darf. Dies scheint aber vielfach geschehen zu sein.

Dies stellt einen Verstoß gegen das geltende Datenschutzrecht dar. Diese Verstöße sind gem. § 21 DSO-Bund dem Datenschutzrat zu melden - die betroffenen Personen sind nach § 22 DSO-Bund zu informieren.

V. Handlungsempfehlungen für verantwortliche Stellen

1. Verantwortliche Stellen sollten zunächst prüfen, ob der Einsatz von Zoom wirklich unerlässlich ist und nicht beispielsweise auf das Angebot des AK Internet zurückgegriffen werden kann.
2. Entscheidet sich die verantwortliche Stelle dennoch für Zoom, so ist
   a) sicherzustellen, dass eine ggf. rechtlich übergeordnete Stelle den Einsatz von Zoom genehmigt hat.
   b) sicherzustellen, dass Inhaber des Zoom-Kontos die verantwortliche Stelle oder eine andere Stelle des Bundes ist.
   c) sicherzustellen, dass der Datenverkehr nur durch europäische Regionen geleitet wird.
   d) sicherzustellen, dass die Aufmerksamkeitsfunktion (Aufmerksamkeitstracking) deaktiviert ist.
   e) sicherzustellen, dass die neuste Version der Zoom-Nutzungsbedingungen akzeptiert und damit ein Auftragsverarbeitungsvertrag geschlossen wurde.
   f) die Datenschutzerklärung der Homepage der verantwortlichen Stelle um Zoom zu erweitern. E-Mails, die zu einer Zoom-Konferenz einladen, müssen auf diese Datenschutzhinweise in der Erklärung hinweisen!
   g) sicherzustellen, dass der Austausch vertraulicher und sensibler Informationen/Daten unterbleibt!

Hinweis: Formulierungsbeispiele und Mustererklärungen sind unter https://www.baptisten.de/angebote-fuer/gemeinden/datenschutz/ zu finden.



Rhauderfehn, den 14.05.2020 - Immo Radtke, LL.M. | Bundesbeauftragter für Datenschutz