KARINA FILUSCH / ALEKSANDRA SOWA

Problemfelder des kirchlichen Datenschutzes im Internet

Einsatz von Social Media, Apps und KI

Datengeheimnis
Datenschutz-Folgenabschätzung
Standard-Datenschutzmodell
TOMs

■ Die Kirchen nutzen das Internet nicht erst seit der Corona-Pandemie. So gut wie jede Kirchengemeinde verfügt über eine eigene Webseite und nutzt zB Social Media, Videokonferenz-Tools sowie Apps für Beichten und digitale Gottesdienste bzw. Messen. Vor diesem Hintergrund werden die folgenden ausgewählten juristischen Problemfelder näher beleuchtet: Wer ist verantwortlich für die Datenverarbeitung beim Einsatz von Social Media und Apps? Wer sind die Aufsichtsbehörden? Kann der Rechtsweg beschritten werden? Welche Besonderheiten gelten hier bei der Verarbeitung von sensiblen Daten? Was muss hinsichtlich der Verschwiegenheit und Offenlegung gegenüber Dritten sowie einer Drittlandübermittlung beachtet werden? Aus technischer Sicht sollten sich die Kirchen vor allem mit der Notwendigkeit und Umsetzung einer Datenschutz-Folgenabschätzung, dem Einsatz des Standard-Datenschutzmodells sowie der Errichtung von technischen und organisatorischen Maßnahmen (TOMs) auseinandersetzen.

■ Churches have not only been using the internet since the Corona pandemic. Almost every congregation has its own website and uses e.g. social media, video conferencing tools and apps for confessions and digital church services or masses. Against this background, the following selected legal problems will be examined in more detail: Who is responsible for data processing when using social media and apps? Who are the supervisory authorities? Can legal action be taken? What particularities apply to the processing of sensitive data? What needs to be considered regarding confidentiality and disclosure to third parties as well as third country transfer? From a technical point of view, churches should above all deal with the necessity and implementation of a data protection impact assessment, the use of the standard data protection model and the establishment of technical and organisational measures (TOMs).
Lesedauer: 19 Minuten

I. Einstieg

Das Internet sowie die Digitalisierung bringen vielfältige Möglichkeiten der Religionsausübung mit sich. 30 Jahre nach der Kommerzialisierung des Internets – zuerst mit der Erfindung des World Wide Web, anschließend mit dem Aufstieg von Social Media und der explosionsartigen Zunahme verschiedenartiger Apps – wimmelt es nur so von digitalen Glaubensangeboten, die die orthodoxen Glaubensgemeinschaften herausfordern. Das Internet vermischt neoliberale Erfolgsoptimierung mit buddhistischen Glaubenssätzen. Der offizielle Webauftritt der römisch-katholischen Kirche www.vatican.va trifft dort auf das „fliegende Spaghetti-Monster“[1], eine 2006 im Internetforum geschaffene Religionsparodie.

Als anno 2017 das neue Online-Angebot des Vatikans „www.vatican.va“ ins Internet ging,[2] hat das Nachrichtenportal „katholisch.de“ versucht, sich durch die Angebote, die vom Radio über Podcasts bis zu den Terminen des Papsts reichten – Twitter-Account und YouTube-Kanal inklusive –, durchzuklicken.[3] „Radio Vatikan ist Geschichte“, kommentierte die Autorin Agathe Lukassek und bedauerte dennoch, dass das neue Angebot nicht, wie früher, in 40 Sprachen verfügbar war: „‚Vatican News‘, das es zunächst in sechs westeuropäischen Sprachen und mit Konzentrierung auf Social-Media-Dienste aus den USA gibt, wirkt zum Start etwas weniger weltoffen.“[4]

Der lange Weg der Kirche zur Öffnung durch die Internetkanäle lässt sich hervorragend am Beispiel von „urbi et orbi“ erklären, den katholisch.de als den „größten Segen der Welt“ bezeichnete.[5] Zweimal im Jahr, zu Weihnachten und Ostern, wird den Gläubigen der (Sünden-)Ablass oder Amnestie durch den Papst persönlich am Petersdom erteilt. Dass man heute den Segen aus dem Vatikan über verschiedene Kommunikationskanäle empfangen kann, war ein langer Weg: „Bereits auf Papst Pius XII. geht eine … wichtige Veränderung der Segenstradition zurück. Im Jahr 1939 erklärte er, dass der Segen nicht nur von den auf dem Petersplatz versammelten, sondern auch von den Gläubigen vor Radiogeräten in aller Welt empfangen werden kann. Papst Johannes Paul II. erweiterte dies im Jahr 1985 zunächst auf das Fernsehen“[6], berichtete katholisch.de. In der Ankündigung des Segens zu Ostern 2023 war sogar von „Radio, Fernsehen und den neuen Kommunikationsmedien“ die Rede. Heißt: Gläubige auf der gesamten Welt könnten via Internet den Segen empfangen, wenn sie es so wollten und die Bandbreite mitspielte.

Auch wenn die offiziellen Kommunikationsangebote der katholischen Kirche im Angebot der im Jahr 2017 neu gegründeten Plattform www.vatican.va immer stärker zentralisiert werden, behält man mitnichten das Monopol auf die Vermittlung der Informationen sowie Medienangebote zu religiösen Themen. Dubiose Webseiten bieten weiterhin Online-Beichten an. Auf TikTok und Instagram inszenieren sich radikale Christen als eine von progressiven Kräften unterjochte Minderheit. Die „Glaubensgemeinschaft der Prixton-Kirche“ bietet auf ihrer Webseite einen Online-Ablass an: „Die Hölle kann warten. Sparen Sie sich jetzt Tausende von Jahren an Fegefeuer! Holen Sie sich jetzt Ihre kostenlose Absolution mit Ablassbrief zum Ausdrucken. Eine Beichte ist nicht erforderlich. … Beim Thema Datenschutz sind wir ebenfalls rigoros und geben keine Informationen an den Weihnachtsmann weiter.“[7]

1 Vgl. https://www.pastafari.eu.
2 Katholisch.de, Neues Medien-Angebot des Vatikan ist online, v. 17.12.2017, abrufbar unter: https://www.katholisch.de/artikel/15855-neues-medien-angebot-des-vatikan-ist-online.
3 Lukassek, Vatikan News: So klicken Sie sich durch zum Papst, v. 20.12.2017, abrufbar unter: https://www.katholisch.de/artikel/15905-vatikan-news-so-klicken-sie-sich-durch-zum-papst.
4 Lukassek, Vatikan News: So klicken Sie sich durch zum Papst, v. 20.12.2017, abrufbar unter: https://www.katholisch.de/artikel/15905-vatikan-news-so-klicken-sie-sich-durch-zum-papst.
5 Martin, Urbi et Orbi: Der größte Segen der Welt, v. 25.12.2022, abrufbar unter: https://www.katholisch.de/artikel/15939-urbi-et-orbi-der-groesste-segen-der-welt.
6 Martin, Urbi et Orbi: Der größte Segen der Welt, v. 25.12.2022, abrufbar unter: https://www.katholisch.de/artikel/15939-urbi-et-orbi-der-groesste-segen-der-welt.
7 Vgl. http://www.prixton.org/de/ablass.php.

II. Ausgewählte juristische Problemfelder

Im Folgenden wird aus juristischer Sicht auf ausgewählte Fragen zu den Angeboten der Kirchen im Internet eingegangen: Dadurch, dass Kirchen eigene Datenschutzgesetze haben dürfen, ergibt sich die Frage nach der Anwendbarkeit des Rechts. Die Nutzung von Dienstleistern bedarf der Klärung, wer für die Datenverarbeitung verantwortlich ist. In diesem Zusammenhang stellt sich zudem die Frage nach der Verschwiegenheit, zB einer Beichtperson, bzw. der Offenlegung von Daten gegenüber Dritten sowie den Besonderheiten bei der Verarbeitung von sog. sensiblen Daten, zu denen Daten über die religiöse Überzeugung gehören; ferner, bei welcher Aufsichtsbehörde Beschwerden erhoben werden können und wie der Klageweg ausgestaltet ist.

1. Anwendbares Recht

a) Nationales Recht

Die Kirchen und Weltanschauungsgemeinschaften in Deutschland haben seit der Weimarer Reichsverfassung (WR) das verfassungsrechtlich garantierte Recht, eigene Datenschutzbestimmungen zu erlassen. Dies ergibt sich aus dem Selbstbestimmungsrecht der Kirche gem. Art. 104 GG iVm Art. 137 Abs. 3 WR. Die Religionsgemeinschaften haben in Deutschland demnach eine historisch gewachsene Befugnis, ihre Angelegenheiten unabhängig vom Staat selbst zu ordnen und zu verwalten, solange sich die selbstständige Rechtsetzung innerhalb der Schranken des staatlichen Rechts bewegt.[8]

Übergreifende Datenschutzbestimmungen für sämtliche Kirchen existieren bis dato nicht. Für die Evangelische Kirche in Deutschland (EKD) gilt das „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland" (DSG-EKD).[9] Für die römisch-katholische Kirche wurde dagegen durch die Vollversammlung der Diözesen Deutschlands das „Gesetz über den kirchlichen Datenschutz" (KDG) vereinbart, jedoch muss dieses durch jede einzelne Diözese für ihren Jurisdiktionsbereich in Kraft gesetzt werden.[10]

b) Unionsrechtliche Ebene

Mit Inkrafttreten der DS-GVO werden den Religionsgemeinschaften in Art. 91 DS-GVO auch auf europäischer Ebene weitreichende Befugnisse erteilt, um eigene Datenschutzbestimmungen zu treffen,[11] was somit eine Öffnungsklausel sui generis für die Kirchen darstellt.[12] Damit nicht jede Religionsgemeinschaft macht, was sie will, bestimmt Art. 91 DS-GVO, dass nationale Datenschutzregelungen mit der DS-GVO iSd Art. 91 Abs. 1 DS-GVO in Einklang gebracht werden müssen.[13] Das bedeutet, dass das nationale Kirchendatenschutzrecht grundsätzlich Anwendungsvorrang hat. Wenn jedoch eine Regelung des kirchlichen Datenschutzes der DS-GVO entgegensteht, hat die DS-GVO ihr gegenüber Vorrang.[14] Man kann es demzufolge darauf herunterbrechen, dass die religiösen Datenschutzgesetze auf europäischer Ebene somit den Mindestanforderungen der DS-GVO unterliegen.[15] Den europäischen Harmonisierungsbestrebungen im Datenschutz wird damit weitestgehend entsprochen.

c) Anwendbares Recht im konkreten Fall

Doch wann gilt das kirchliche Datenschutzgesetz und wann die DS-GVO im konkreten Anwendungsfall? Früher unterschied man folgendermaßen:[16] Der Selbstbestimmungsbereich der Kirche hätte sämtliche kircheneigenen Angelegenheiten betroffen, und das kirchliche Datenschutzrecht wäre anwendbar gewesen. Demzufolge würden zB auch christlich geführte Krankenhäuser dem kirchlichen Datenschutz unterliegen. Nicht umfasst wären allerdings Bereiche, die nicht genuin weltanschaulich sind – wie im Fall der Vermietung eines Wohnhauses, das im Eigentum eines Erzbistums steht. Heutzutage kommt die sog. Abwägungslehre zur Anwendung, wonach die rechtlichen Interessen der Kirche mit den Rechtsgütern der betroffenen Personen ins Verhältnis gebracht werden müssen.[17]

Wendet man diese an, scheint es für innerkirchliche Datenverarbeitungen kaum Probleme zu bereiten, das kirchliche Datenschutzrecht anzuwenden, da die innerkirchliche Datenverarbeitung unter das Selbstbestimmungsrecht der Kirche fällt. Komplexer wird der Sachverhalt, wenn die Datenverarbeitungen im Internet stattfinden und Drittanbieter wie Zoom als sog. Auftragsverarbeiter eingeschaltet werden oder wenn eine Kirchengemeinde ein Facebook-Profil betreibt, auf dem Beichten per Messenger-Chat angeboten werden. Muss sich dann Facebook an den jeweiligen kirchlichen Datenschutz halten oder an die DS-GVO?

2. Verantwortlichkeit

Der Begriff der verantwortlichen Stelle wird in § 4 Nr. 9 DSG-EKD bzw. § 4 Nr. 9 KDG definiert. Erfasst sind sowohl kirchliche als auch nicht-kirchliche Stellen, und beide Gesetze kennen auch die gemeinsame Verantwortlichkeit (§ 29 DSG-EKD bzw. § 28 KDG) und die Auftragsverarbeitung (§ 30 DSG-EKD bzw. § 29 KDG). Gem. § 29 Abs. 1 S. 2 DSG-EKD und § 28 Abs. 1 KDG muss der Vertrag für die gemeinsame Verantwortlichkeit definieren, welcher Vertragspartner die Verpflichtungen gemäß dem jeweiligen kirchlichen Datenschutzgesetz erfüllt. Des Weiteren kann die betroffene Person ihre Rechte bei und gegenüber jeder einzelnen verantwortlichen Stelle geltend machen, § 29 Abs. 3 DSG-EKD bzw. § 28 Abs. 3 KDG. Für die Online-Beichte über Social Media bedeutet dies im Einzelnen, dass zunächst geprüft werden muss, welches Recht anwendbar ist: das der jeweiligen Kirche oder das der DS-GVO? Diese Abwägung würde, da es sich um eine Beichte handelt, deren Abnahme eine der Kernaufgaben der Kirchen ist, unter das kirchliche Datenschutzrecht fallen. Zumindest kann dies nicht vollständig ausgeschlossen werden. Dies würde zB beim Einsatz einer Facebook-Fanpage bedeuten, dass in dem durch Facebook angebotenen Vertrag für die gemeinsame Verantwortlichkeit[18] festgelegt werden müsste, welcher Verantwortliche die Betroffenenrechte iSd § 29 Abs. 1 S. 2, Abs. 3 DSG-EKD bzw. § 28 Abs. 1 S. 2, Abs. 3 KDG wahrnimmt. Nicht alle Social-Media-Kanäle stellen diese Verträge zur Verfügung.

Im Hinblick auf Auftragsverarbeitungen schreibt § 30 Abs. 1 S. 1 DSG-EKD vor, dass die kirchliche Stelle für die Einhaltung des DSG-EKD verantwortlich ist. Gem. § 29 Abs. 1 KDG muss die Datenverarbeitung im Einklang mit dem KDG stattfinden. Der Dienstleister müsste folglich auf die Regelungen aus dem jeweiligen Kirchendatenschutzrecht verpflichtet werden. Dies wird zudem aus § 30 Abs. 5 S. 1 DSG-EKD deutlich, wobei danach die Verpflichtung auf das DSG-EKD erfolgen soll oder auf „gleichwertige Bestimmungen", also die der DS-GVO. In § 29 Abs. 3 KDG wird ebenso auf die Anwendbarkeit der DS-GVO neben dem KDG abgestellt. § 30 Abs. 5 S. 3 DSG-EKD unter-

8 BeckOK DatenschutzR/Mundil, 44. Ed. 1.11.2021, DS-GVO Art. 91 Rn. 4; Martini/Botta DÖV 2020, 1045 (1045 f.); zu den Schranken ausf. Hoeren ZD 2023, 199 (200 f).
9 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) v. 15.11.2017, ABL. EKD 2017, 353 (Nr. 143).
10 Sydow/Marsch, DS-GVO/BDSG/Hense, 3. Aufl. 2022, DS-GVO Art. 91 Rn. 33.
11 Dazu ausf. Hoeren ZD 2023, 199 (201).
12 Martini/Botta DÖV 2020, 1045 (1047).
13 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 13; Martini/Botta DÖV 2020, 1045 (1047); Paal/Pauly, DS-GVO BDSG/Pauly, 3. Aufl. 2021, DS-GVO Art. 91 Rn. 4.
14 Hoeren ZD 2023, 199 (201 f.); Gola/Heckmann, DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 91 Rn. 1.
15 Vgl. Hoeren ZD 2023, 199 (203).
16 Hoeren ZD 2023, 199 (200).
17 Dürig/Herzog/Scholz, Grundgesetz/Korioth, 100. Aufl. 2023, WRV Art. 137 Rn. 47; v. Mangoldt/Klein/Starck, GG/Unruh, 7. Aufl. 2018, WRV Art. 137 Rn. 42.
18 Vgl. https://de-de.facebook.com/legal/terms/page_controller_addendum.

wirft den Dienstleister sogar direkt der kirchlichen Datenschutzaufsicht. Würde demnach ein Dienstleister als Auftragsverarbeiter eingesetzt werden, zB der Videokonferenz-Dienstleister Zoom für eine „persönliche" Beichte oder eine Messe, müsste er sich auf das DSG-EKD bzw. das KDG verpflichten und sich im Fall des DSG-EKD der kirchlichen Datenschutzaufsicht unterwerfen. Es ist jedoch nicht bekannt, dass einer der großen Auftragsverarbeiter eine solchen Verpflichtung bzw. Unterwerfung bisher zugesagt hat. Dies scheint auch vor dem Hintergrund der Vielzahl von Kirchengemeinden in Europa unwahrscheinlich, denen sich die idR international handelnden Dienstleister unterwerfen müssten.

3. Verschwiegenheit, Offenlegung und Datengeheimnis

IRd gemeinsamen Verantwortlichkeit bzw. Auftragsverarbeitung ist zudem ein weiterer Aspekt relevant: Wie ist die Übermittlung – zB einer Beichte – mithilfe eines Dienstleisters mit der Verschwiegenheitspflicht vereinbar, die die Kirche gegenüber ihren Gläubigen gem. § 26 S. 2 DSG-EKD iVm § 3 S. 1 DSG-EKD bzw. § 29 Abs. 4 lit. b KDG einhalten muss? Kirchen werden, sofern sie Dienstleister einsetzen, diese auf die Verschwiegenheit verpflichten müssen, ähnlich wie es zB die Anwaltschaft gegenüber ihrem Mail-Host machen muss.

Interessant ist in diesem Zusammenhang auch der Begriff der Offenlegung durch Übermittlung gegenüber nicht-kirchlichen Stellen gem. § 9 DSG-EKD bzw. § 10 KDG. Demnach ist eine Offenlegung lediglich unter strengen Voraussetzungen möglich, wie zB zur Erfüllung der kirchlichen Aufgaben (§ 9 Abs. 1 Nr. 1 DSG-EKD bzw. § 10 Abs. 1 lit. a KDG) oder beim Vorliegen eines berechtigten Interesses (§ 9 Abs. 1 Nr. 3 DSG-EKD bzw. § 10 Abs. 1 lit. b KDG). Dabei ist bei besonderen Kategorien von Daten – wie an dieser Stelle – im evangelischen Kirchendatenschutzgesetz eine Offenlegung gem. § 9 Abs. 3 DSG-EKD lediglich zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche möglich. Zudem dürfen die Daten gem. § 9 Abs. 5 DSG-EKD bzw. § 10 Abs. 4 KDG nur zu dem Zweck verwendet werden, zu dem sie offengelegt wurden. Dies dürfte zumindest bei Anbietern wie Facebook schwierig werden, da diese die Daten bekanntlich auch zu eigenen Zwecken nutzen.[19] Hingewiesen sei zudem auf das in § 26 DSG-EKD bzw. § 5 KDG geregelte Datengeheimnis, auf das Auftragsverarbeiter verpflichtet werden müssten.

4. Aufsichtsbehörden bzw. Rechtsweg

a) Aufsichtsbehörden

Den betroffenen Personen steht es gem. § 46 DSG-EKD bzw. § 48 KDG frei, sich bei einer Aufsichtsbehörde zu beschweren. Bei wem kann die Beschwerde erhoben werden, wenn es sich um einen Fall aus dem Kirchendatenschutzrecht handelt?

Nach Art. 91 Abs. 2 DS-GVO soll eine unabhängige Aufsichtsbehörde installiert werden, die auch spezifischer Art sein kann, deren Zuständigkeiten, Aufgaben und Befugnisse sich jedoch nach Abschnitt VI DS-GVO richten. Demnach dürfen Kirchen eine eigene Aufsichtsbehörde einrichten, sofern diese eine unabhängige Aufsichtsbehörde ist.[20] § 40 DSG-EKD bzw. § 43 Abs. 1 S. 2–3 KDG regeln die Unabhängigkeit.

Die Datenschutzbeauftragten der Kirchen übernehmen in diesem Zusammenhang die Rolle einer staatlichen Datenschutzbehörde, wobei die Eingriffsmöglichkeiten der Datenschutzbeauftragten hinter denen der staatlichen Behörden zurückbleiben.[21] Weiterhin verlangt Art. 78 Abs. 2 DS-GVO, dass die Entscheidungen der jeweiligen Aufsichtsbehörde, also auch der kirchlichen, wirksam rechtlich überprüft werden können.[22] Wo kann eine Beschwerde konkret gemeldet werden?

Gem. § 39 DSG-EKD gibt es mehrere Aufsichtsbehörden: Nach Absatz 2 soll es eine für den Bereich der EKD und ihres Evangelischen Werks für Diakonie und Entwicklung sowie für die gesamtkirchlichen Werke und Einrichtungen geben. Nach Absatz 3 S. 1 können die Gliedkirchen sowie gliedkirchliche Zusammenschlüsse einzeln bzw. gemeinschaftlich eine Aufsichtsbehörde errichten, wobei die Gliedkirchen für ihre zugeordneten diakonischen Dienste, Einrichtungen und Werke eigene Aufsichtsbehörden gemäß Absatz 3 S. 2 einrichten können.

Gem. § 42 Abs. 1 KDG wird ein Diözesandatenschutzbeauftragter pro Diözese bestellt.

Diese Vielzahl an Aufsichtsbehörden im evangelischen bzw. katholischen Kirchendatenschutz erschwert es der betroffenen Person allerdings, den Überblick zu behalten und die zuständige Behörde ausfindig zu machen.

b) Rechtsweg

Eine gerichtliche Überprüfung der Entscheidung der Aufsichtsbehörde in der evangelischen Kirche kann gem. § 47 DSG-EKD über den Klageweg[23] bei den Verwaltungsgerichten der jeweiligen Landeskirche stattfinden.[24]

Nach § 49 KDG kann ebenso gegen Entscheidungen des Diözesandatenschutzbeauftragten geklagt werden. Die römisch-katholische Kirche in Deutschland hat sogar durch die Vollversammlung der Bischofskonferenz eine kirchliche Datenschutzgerichtsordnung (KDGGO) beschlossen, wonach es einen eigenen Instanzenzug gibt, bei dem in der ersten Instanz ein Interdiözesanes Datenschutzgericht eingerichtet wird, während die zweite Instanz ein Datenschutzgericht der Deutschen Bischofskonferenz ist.[25] In diesem Zusammenhang sind die Richter unabhängig gem. § 3 Abs. 3 KDGGO, und der staatliche Rechtszug ist dadurch nicht ausgeschlossen.[26]

Die durch diese Gerichte ausgesprochenen Entscheidungen unterliegen jedoch keiner kirchlichen Zwangsvollstreckung,[27] da diese lediglich dem Staat vorbehalten ist.

Kann eine Entscheidung eines kirchlichen Datenschutzgerichts staatlich überprüft werden? Das BVerwG hat erkannt, dass eine staatliche Überprüfung dieser Entscheidungen erfolgen kann, sofern der kirchliche Rechtsweg ausgeschöpft ist und es um die Überprüfung einer kirchlichen Maßnahme mit staatlichem Recht geht.[28]

5. Sensible Daten

Daten über die religiöse und weltanschauliche Überzeugung zählen zu den sog. sensiblen Daten gem. § 13 Abs. 1 DSG-EKD iVm § 4 Nr. 2 lit. a DSG-EKD bzw. § 11 KDG iVm § 4 Nr. 2 KDG.

---

19 EuGH MMR 2018, 591 (593) mAnm Moos/Rothkegel = ZD 2019, 455 mAnm Hanloser – Fashion ID.

20 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 12; Ehmann/Selmayr, DS-GVO/Kranig, 2. Aufl. 2018, DS-GVO Art. 91 Rn. 7; BeckOK DatenschutzR/Mundil, 44. Ed. 1.11.2021, DS-GVO Art. 91 Rn. 21.

21 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 16.

22 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 16.

23 Ausf. Martini/Botta DÖV 2020, 1045 (1048 ff.).

24 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 16.

25 Sydow/Marsch, DS-GVO/BDSG/Hense, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 34; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 16.

26 Sydow/Marsch, DS-GVO/BDSG/Hense, 3. Aufl. 2022, DS-GVO Art. 9 Rn. 34.

27 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Seifert, 2019, DS-GVO Art. 91 Rn. 16; Alternativen für die Zwangsvollstreckung: Martini/Botta DÖV 2020, 1045 (1051).

28 BVerwG NVwZ 2014, 1101 (1104).

Die Verarbeitung solcher Daten ist grundsätzlich verboten, außer es greift ein Ausnahmetatbestand nach § 13 Abs. 2 DSG-EKD bzw. § 11 Abs. 2 KDG. In Betracht kommt hierbei insbesondere die Einwilligung nach § 13 Abs. 2 Nr. 1 DSG-EKD bzw. § 11 Abs. 1 lit. a KDG. Nach § 13 Abs. 2 Nr. 4 DSG-EKD bzw. § 11 Abs. 2 lit. d KDG ist die Verarbeitung sog. sensibler Daten möglich, sofern:

- die Verarbeitung durch eine verantwortliche Stelle im Rahmen ihrer rechtmäßigen Tätigkeit
- und unter der Voraussetzung erfolgt, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der verantwortlichen Stelle oder auf Personen bezieht, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten,
- und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Beide Alternativen sehen eine Einwilligung der betroffenen Person vor, wenn sie zB eine Online-Beichte in Anspruch nehmen will.

6. Drittlandübermittlung

Setzt eine Kirche Social Media ein, kommt sie spätestens ab diesem Zeitpunkt mit der Thematik des Drittlandtransfers in Berührung. Die Diskussion darüber, wie eine Datenübermittlung in die USA trotz des gekippten Privacy Shield durch das Schrems-II-Urteil[29] noch legal erfolgen kann, ist zumindest vorerst beendet, da es seit dem 10.7.2023 einen neuen Angemessenheitsbeschluss der EU-Kommission mit den USA gibt.[30] Die Regelung der DSG-EKD und die des KDG sind vergleichbar mit denen der DS-GVO. Gem. § 10 Abs. 1 DSG-EKD bzw. § 40 KDG ist eine Datenübermittlung in ein Drittland nur zulässig, wenn es einen Angemessenheitsbeschluss der EU-Kommission gibt oder Standardvertragsklauseln verwendet werden. Ist dies nicht gegeben, kann die Datenübermittlung nach § 10 Abs. 2 DSG-EKD bzw. § 41 KDG dennoch zulässig sein, nämlich zB wenn eine Einwilligung der betroffenen Person vorliegt. Somit entsprechen die Regelungen weitestgehend Art. 45, 46 und 49 DS-GVO. Die Kirchen stehen demnach vor genau den gleichen Herausforderungen wie weltliche Verantwortliche, die Daten in ein Drittland transferieren.

III. Ausgewählte technische Problemfelder

Die DS-GVO beschränkt sich nicht nur auf die Definition der Anforderungen an den Datenschutz, sondern enthält konkrete Hinweise zu den technischen und organisatorischen Maßnahmen (TOMs),[31] mit deren Hilfe ein angemessenes Schutzniveau erreicht werden kann. Konkret befasst sich Art. 32 DS-GVO, der eine Aufzählung von Maßnahmen – von der Anonymisierung bis hin zur Verschlüsselung – enthält, mit denen Datenschutzrisiken adressiert werden können, vorrangig mit den TOMs. Dabei ist es sinnvoll, zu betonen, dass „nicht Daten zu schützen, sondern die Risiken der Verarbeitungsvorgänge zu verringern sind“[32]. Deswegen bilden Methodiken, wie das Standard-Datenschutzmodell (SDM) der Datenschutzkonferenz eine Grundlage für geeignete Prozesse, bei denen die Arten der Verarbeitung sowie betroffene Daten und die damit verbundenen Datenschutzrisiken identifiziert, analysiert und erst dann geeignete TOMs abgeleitet werden.

Die Begriffe „technisch-organisatorische Maßnahme“, „Schutzmaßnahme“ oder „risikominimierende Maßnahme“ werden im Kontext des SDM gleichbedeutend behandelt. Im Gegensatz zu gängigen Standards für Informationssicherheit, die meistens drei (Integrität, Vertraulichkeit, Verfügbarkeit), selten vier (Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität) Schutzziele kennen, arbeitet das SDM mit sieben Gewährleistungszielen: Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung, Intervenierbarkeit und Datenminimierung. Diese Gewährleistungsziele werden durch den Einsatz geeigneter TOMs erreicht.

Auf der technischen Seite gehören zu den Hauptmaßnahmen zB: Verschlüsselung von Daten, Anonymisierung, Pseudonymisierung, Back-ups, Tests oder Protokollierung (Monitoring). Technische Mittel werden durch organisatorische Maßnahmen bzw. organisatorische (Sicherheits-)Kontrollen ergänzt, wie zB Zugriffs- und Zugangsberechtigungen, Vier-Augen-Prinzip, Least- oder Need-to-Know-Prinzip, Changemanagement oder Löschkonzepte. „Zu den Gewährleistungszielen kann man die jeweils wichtigsten Hauptmaßnahmen nennen“[33]. ZB kann das Ziel der Gewährleistung der Vertraulichkeit von Daten mittels Verschlüsselung (Ende-zu-Ende-Verschlüsselung bei der Kommunikation oder dem Datentransfer) erreicht werden. „Dabei gibt es nicht immer genau eine Maßnahme zum Erreichen genau eines Gewährleistungsziels; eine Maßnahme kann auch die Risiken mehrerer Ziele gleichzeitig verringern …“[34]. Am Beispiel der Verschlüsselung erläutert, bedeutet das: Die Maßnahme kann sowohl das Gewährleistungsziel „Vertraulichkeit“ adressieren, indem Daten verschlüsselt archiviert oder im Back-up gespeichert sind oder Ende-zu-Ende-verschlüsselt übertragen bzw. versendet werden, ohne dass interne oder externe Angreifer Kenntnis von den Inhalten erlangen können, als auch „Integrität“, da die Daten gegen Eingriffe in ihre Echtheit oder Veränderung und Manipulation geschützt sind, solange sie verschlüsselt bleiben.

Angenommen, eine Beicht-App bietet den Service, dem Sündigen eine Beichte abzunehmen, indem diese als Audiodatei gespeichert und auf elektronischem Weg einer Beichtmutter bzw. einem Beichtvater übermittelt wird. Dieser entscheidet nach dem Abhören der Beichte über das Ausmaß der Buße und erteilt Absolution (oder nicht), die dem Delinquenten auf elektronischem Weg (als Audiodatei oder Textnachricht) übermittelt wird. Um die Grundanforderungen an eine Beichte zu erfüllen, müssen beide Parteien anonym bleiben – sowohl für sich gegenseitig als auch für interessierte Dritte oder potenzielle Angreifer. Dies bedeutet den Einsatz von Anonymisierung, Zugriffs- und Zugangsberechtigungen, Verschlüsselung sowie des sog. Least-to-Know-Prinzips, um sowohl den Inhalt der Beichte als auch den der Absolution vertraulich zu halten.

Die Auswahl der sinnvollen und notwendigen Maßnahmen zur Verringerung der Risiken der Verarbeitung wird allerdings gänzlich anders aussehen, wenn die Beicht-App statt einer menschlichen Beichtperson eine Software – einen Algorithmus oder eine KI – einsetzt, die automatisch zB auf Grundlage historischer Daten aus dem Internet die angemessene Buße sowie die Absolution ermittelt und dem Beichtenden ad hoc mitteilt.

Damit die Maßnahmen nicht nur geeignet scheinen, sondern geeignet und vollständig sind, empfiehlt sich der Einsatz der sog. Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DS-GVO. Wenn von der Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen ausgeht, ist eine DSFA nicht nur eine Empfehlung, sondern obligatorisch.[35] Eine Methodik für die DSFA gem. Art. 35 DS-GVO[36] wurde auf

29 EuGH ZD 2020, 511 mAnm Moos/Rothkegel – Schrems II.
30 Vgl. https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en; s.a. ZD-Interview mit Schmitz und Spies ZD 2023, 517.
31 In den kirchlichen Datenschutzgesetzen geregelt in § 27 DSG-EKD bzw. § 26 KDG; sie entsprechen weitestgehend den Regelungen in der DS-GVO.
32 Rost, Das Standard-Datenschutzmodell (SDM), 2022, S. 126.
33 Rost, Das Standard-Datenschutzmodell (SDM), 2022, S. 126.
34 Rost, Das Standard-Datenschutzmodell (SDM), 2022, S. 126.
35 Vgl. Rost, Das Standard-Datenschutzmodell (SDM), 2022, S. 169.
36 In den kirchlichen Datenschutzgesetzen geregelt in § 34 DSG-EKD bzw. § 35 KDG; sie entsprechen weitestgehend den Regelungen in der DS-GVO.

Grundlage des SDM entwickelt und ermöglicht eine strukturierte Ermittlung von TOMs durch Anwendung eines Plan-Do-Check-Act-Phasenmodells.

Ob eine DSFA, zB für eine Beicht-App, jedoch überhaupt obligatorisch ist, hängt davon ab, ob von der Verarbeitung personenbezogener Daten ein hohes Risiko für Betroffene ausgeht. Festgestellt wird dies iRe Schwellwertanalyse,[37] die – im Gegensatz zur DSFA – für jede Verarbeitung durchgeführt werden muss.

Bedenkt man den Status der religiösen und weltanschaulichen Überzeugung als sensible Daten, die sowohl gemäß DS-GVO als auch DSG-EKD oder KDG strikten Einschränkungen hinsichtlich der Verarbeitung unterliegen, ist der Einsatz geeigneter Standards und Modelle iSv „Privacy-by-Design" sinnvoll und wünschenswert. Ob man sich hierbei auf die in Deutschland verbreiteten und erprobten Standards und Modelle, wie SDM, stützt oder eigene Standards entwickelt, ist in diesem Zusammenhang ohne Belang, solange im Ergebnis die Risiken von Verarbeitungsvorgängen verringert werden.

IV. Fazit

Das Zweite Vatikanische Konzil veröffentlichte 1971 die Pastoralinstruktion über die Instrumente der sozialen Kommunikation. Danach seien Gemeinschaft und Fortschritt der menschlichen Gesellschaft oberste Ziele sozialer Kommunikation und ihrer Instrumente wie Presse, Film, Hörfunk und Fernsehen. In weiser Voraussicht heißt es weiter: „[Die Instrumente] entwickeln sich ständig weiter und stehen einer wachsenden Zahl von Menschen … in zunehmendem Maße leichter zur Verfügung. Sie umgreifen mehr und mehr ihre Denk- und Lebensweise und dringen durch ihre Technik immer tiefer darin ein."[38] Es folgen Grundsätze und pastorale Weisungen über den Umgang der katholischen Kirche mit diesen neuen Kommunikationsformen. Die Potenziale neuer Medien werden demnach erkannt und – wie das Beispiel der diesjährigen Übertragung des päpstlichen Segens „urbi et orbi" zeigt – vorsichtig genutzt. Je intensiver jedoch die Nutzung wird und je vielfältiger die Technologien (Apps, KI etc.), desto stärker muss auf die geltenden Normen und Regulierungen Rücksicht genommen werden. Gleichwohl bleibt den Kirchen auf Grund des geltenden Selbstbestimmungsrechts nach wie vor der Weg offen, eigene Normen zu erlassen und Standards zu entwickeln.

Schnell gelesen …

- Die evangelische und die katholische Kirche in Deutschland haben ihre eigenen Datenschutzgesetze, die grundsätzlich Anwendungsvorrang haben – außer sie widersprechen der DS-GVO, dann hat diese Vorrang.
- Die Kirchen können selbst Verantwortliche sein, aber auch gemeinsam mit Dienstleistern verantwortlich sein, und sie können sich Auftragsverarbeitern bedienen.
- Es gibt eine Vielzahl von Datenschutzaufsichtsbehörden nach den beiden kirchlichen Datenschutzrechten.
- Eine Klage gegen die Entscheidung der kirchlichen Datenschutzaufsicht ist möglich.
- Auch im kirchlichen Datenschutzrecht besteht die Problematik des Drittlandtransfers.
- Die Anforderungen an die TOMs sind auf Grund der Sensibilität der Daten hoch.
- Die Anfertigung einer DSFA wird oftmals verpflichtend sein.

Karina Filusch, LL.M.,
ist Rechtsanwältin, Fachanwältin für IT-Recht, zertifizierte Datenschutzbeauftragte und Dozentin in Berlin.

Dr. Aleksandra Sowa
ist Sachverständige für IT-Sicherheit, zertifizierte Datenschutzbeauftragte und -auditorin sowie Buchautorin.

37 Vgl. Rost, Das Standard-Datenschutzmodell (SDM), 2022, S. 110 ff., 169 ff.
38 Päpstliche Kommission für die Instrumente pastoraler Kommunikation, Pastoralinstruktion „Communio et progressio": Über die Instrumente der sozialen Kommunikation, veröffentlicht im Auftrag des II. Vatikanischen Ökumenischen Konzils, v. 23.5.1971, abrufbar unter: https://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_23051971_communio_ge.html.