Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht 2021

2022

2023

2024

2025

2026

2027

Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht
2021

Herausgegeben von der
Diözesandatenschutzbeauftragten für die (Erz-)Bistümer Freiburg, Fulda,
Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Kath. Datenschutzzentrum Frankfurt/M. KdöR
Domplatz 3
Haus am Dom
D-60311 Frankfurt/M.
Tel. 069/800 8718 800
Fax 069/ 800 8718 815
E-Mail: info@kdsz-ffm.de
www.kdsz-ffm.de

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen an einigen Stellen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.
Bildnachweise: S. 1, S. 25, S. 35 Adobestock

Inhaltsverzeichnis

Keine Normalität – und was der Datenschutz mit der Flutwelle zu tun hat

Auch im zweiten Jahr der Pandemie trat in die Arbeit der Datenschutzaufsicht noch keine Normalität ein. Die Anfragen und Beschwerden im Zusammenhang mit Corona – ob es sich um die Fragen des Arbeitgebers nach dem Impfstatus, die Maskenpflicht oder die Löschung von Erfassungslisten handelte – nahmen eher zu, als dass sie weniger wurden.

Neben den zahlreichen Telefon- und Videokonferenzen, Homeoffice, Homeschooling, mobilem Arbeiten, die uns die Pandemie bescherte, konnten zumindest im Oktober einige Veranstaltungen und Prüfungen in Präsenz stattfinden, kleine Lichtblicke persönlicher Kontakte, die doch sehr vermisst wurden.

Auch das „Schrems II-Urteil“ des Europäischen Gerichtshofs ist noch nicht ganz „verdaut“. Ob durch ein neues Abkommen zwischen der EU und den USA oder durch die Standardvertragsklauseln ein rechtssicherer Datentransfer möglich sein wird, steht noch nicht fest. Ein „Schrems III“ o. ä. scheint nicht wirklich ausgeschlossen.

Weitere bundesrechtliche Regelungen wie das Betriebsrätemodernisierungsgesetz oder das TTDSG werden auch im kirchlichen Bereich Auswirkungen haben. Ausführliche Informationen hierzu finden sich deshalb ebenfalls in diesem Tätigkeitsbericht.

In der Gesetzgebung hat sich nicht nur im staatlichen Bereich einiges getan. Auch in der Katholischen Kirche war man nicht untätig. So hat beispielsweise die Vollversammlung der deutschen Bischöfe den kirchlichen Gesetzgebern im September 2021 durch Beschluss eine Rahmen-Personalaktenordnung an die Hand gegeben, die es ermöglichen soll, „ … Missbrauchsbeschuldigungen künftig in allen Diözesen verbindlich, einheitlich und transparent …“ zu dokumentieren. Hiermit macht sich die Deutsche Bischofskonferenz auf den Weg, dieses dunkle Kapitel des Missbrauchs in der Kirche weiter aufzuarbeiten.

Im Juli 2021 bescherte die Flutkatastrophe im Ahrtal auch dem Datenschutz ganz neue Fragestellungen. Es erreichten das Kath. Datenschutzzentrum Frankfurt/M. Meldungen, die von der Zerstörung ganzer Einrichtungen berichteten. Neben den hiermit verbundenen menschlichen Schicksalen, die auch die Mitarbeiterinnen und Mitarbeiter der Datenschutzaufsicht bewegten, war dies für die Einrichtungen datenschutzrechtlich herausfordernd. Wohl dem, der seine Daten in der Cloud speichert. Natürlich stellten sich die Fragen zu Datenverlusten oder möglichen Meldepflichten nicht an erster Stelle, aber sie stellten sich eben auch. Manche Schilderung war sehr eindringlich und hing auch lange nach. Deshalb bleibt an dieser Stelle, allen Betroffenen das Allerbeste zu wünschen.

Ursula Becker-Rathmair
Diözesandatenschutzbeauftragte und Leiterin des Kath. Datenschutzzentrums Frankfurt/M.

1 Entwicklung des Datenschutzes

1.1 Staatliche Gesetzgebung

1.1.1 Klarheit über datenschutzrechtliche Verantwortlichkeit im Betriebsratsbüro

Im Jahr 2021 ist das Betriebsrätemodernisierungsgesetz in Kraft getreten. Es schafft unter anderem eine gesetzliche Regelung für eine schon lange diskutierte Frage zur datenschutzrechtlichen Stellung der betrieblichen Interessenvertretung. Der Gesetzgeber stellt nunmehr in § 79a S. 2 BetrVG klar, dass auch im Betriebsratsbüro „der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften“ ist. Diese nunmehr gesetzlich normierte Feststellung, nach der die Belegschaftsvertretung keine eigene verantwortliche Stelle der Datenverarbeitung ist, kann nicht ohne Weiteres im kirchlichen Datenschutzrecht außer Acht gelassen werden, sodass auch eine Mitarbeitervertretung nicht als eine eigene Verantwortliche zu sehen ist.

Zudem sollen mit diesem Gesetz zur Förderung der Betriebsratswahlen und der Betriebsratsarbeit in einer digitalen Arbeitswelt die Mitbestimmungsrechte beim Einsatz Künstlicher Intelligenz (§ 80 Abs. 3 BetrVG) und bei der Ausgestaltung mobiler Arbeit in den Betrieben (§ 87 Abs. 1 Nr. 14 BetrVG) gestärkt werden. Ob diese Reformen der Betriebsverfassung auch Änderungen der Mitarbeitervertretungsordnung nach sich ziehen, wird sich erst noch zeigen.

§ 79a BetrVG – Datenschutz

Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber.

1.1.2 Neue Regeln für Cookies durch TTDSG

Zum Ende des Berichtsjahres ist noch das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Das Gesetz fasst die Datenschutzregelungen des Telemedien- und Telekommunikationsgesetzes zusammen, passt sie an die EU-Datenschutzgrundverordnung (DSGVO) an und setzt Vorgaben aus der ePrivacy-Richtlinie zum Einsatz von Cookies um. Auch deswegen kann das neue Gesetz mit dem sperrigen Namen für katholische Einrichtungen von Bedeutung sein, wenn diese beispielsweise Cookies auf ihren Internetpräsenzen einsetzen.

Die Regeln für das Einholen von Einwilligungen zur Verarbeitung von Nutzerdaten sind nunmehr strenger. Websitebetreiber können seit Inkrafttreten des TTDSG beim Cookie-Einsatz nicht mehr einfach auf ihr berechtigtes Interesse als Rechtsgrundlage verweisen.

Das Speichern von Informationen beispielsweise auf dem Smartphone des Users ist nach § 25 TTDSG zulässig, wenn dieser „auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat“. Verzichtet werden kann auf das Einholen der Einwilligung nur noch unter den engen Voraussetzungen des § 25 Abs. 2 TTDSG, zum Beispiel wenn dies zur Übertragung einer Nachricht erforderlich ist.

Die Datenschutzkonferenz (DSK) hat fast zeitgleich mit dem Inkrafttreten des TTDSG eine Orientierungshilfe veröffentlicht, die sich schwerpunktmäßig mit dem in § 25 TTDSG normierten Grundsatz der Einwilligungsbedürftigkeit beschäftigt als auch mit dem Verhältnis des TTDSG zur DSGVO.

§ 25 TTDSG – Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

1.1.3 Infektionsschutz im ständigen Wandel

Umfangreiche Änderungen gab es im Infektionsschutzgesetz (IfSG) im Zuge der Bekämpfung der Corona-Pandemie, die ebenfalls den Erlass zahlreicher Corona-Verordnungen in den einzelnen Bundesländern nach sich zogen. Da sich die Zuständigkeit des Kath. Datenschutzzentrums Frankfurt/M. auf fünf Bundesländer erstreckt – Hessen, Rheinland-Pfalz, Saarland, Baden-Württemberg und Teile Thüringens – stellten die teils recht unterschiedlichen Landesregelungen, die zudem oft in kurzen zeitlichen Abständen geändert wurden, und die von den (Erz-)Bistümern noch zusätzlich erlassenen Anordnungen zum Infektionsschutz aber vor große Herausforderungen. So war beispielsweise in einem Bundesland der Zugang zum Gottesdienst kaum durch Infektionsschutzmaßnahmen reglementiert, in anderen Bundesländern gingen die (Erz-)Bistümer dagegen noch über die staatlichen Regelungen hinaus. Die Suche im Rahmen von eingereichten Beschwerden und gemeldeten Datenschutzverletzungen nach den aktuellen einschlägigen Rechtsgrundlagen für einzelne Maßnahmen in katholischen Einrichtungen erforderte daher zum Teil detektivische Detailarbeit.

So wurde zum Beispiel die Homeoffice-Pflicht eingeführt oder eine Impfnachweispflicht für bestimmte Mitarbeitergruppen. Diese und viele andere Schutzmaßnahmen zogen so manche Datenschutzverletzung nach sich und sorgten oft vor Ort für Ärger, der auch in Beschwerden bei der Datenschutzaufsicht mündete und so nochmals zusätzlich einen erheblichen Arbeitsaufwand zur Folge hatte.

1.2 Kirchliche Gesetzgebung

1.2.1 Einheitliche Personalaktenordnung für alle (Erz-)Bistümer

Die Vollversammlung der Deutschen Bischofskonferenz (DBK) hat am 22. September 2021 eine Rahmenordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten (Personalaktenordnung – PAO) beschlossen.

Die DBK möchte damit eine einheitliche und rechtssichere Personalaktenführung in ihrem Bereich sicherstellen und das laut Präambel „unter Beachtung der anerkannten Grundsätze der Personalaktenführung, namentlich der Transparenz, der Richtigkeit und Vollständigkeit, der Zulässigkeit der Information sowie der Vertraulichkeit“. Die neue PAO soll auch eine bessere Aufarbeitung des sexuellen Missbrauchs im Raum der Katholischen Kirche ermöglichen – „unter Wahrung der Privatsphäre und der Persönlichkeitsrechte der Bediensteten und Dritter“.

Die (Erz-)Diözesen in Deutschland haben dieses Gesetz – und damit die Standardisierung der Personalaktenführung – gemeinsam zum 1. Januar 2022 in Geltung gesetzt. Die sieben (Erz-)Bistümer im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M.

haben die Rahmenordnung in ihren jeweiligen Amtsblättern hierzu bis Ende des Jahres 2021 verkündet und zum Teil spezielle Ordnungen zur Weitergabe von Daten aus Personalakten von Klerikern an Dritte im Rahmen der Missbrauchsaufarbeitung erlassen.

Das Verhältnis der PAO zum KDG ist in § 2 des Gesetzes ausdrücklich geregelt. Danach gelten das KDG und die KDG-DVO, soweit sich aus der PAO nichts Abweichendes ergibt.

Ausdrücklich geregelt ist ebenfalls das Einsichtsrecht des Bediensteten in seine Personalakte (§ 13 PAO) – allerdings hat dies nur unter Aufsicht zu geschehen, um Manipulationen auszuschließen. Das Auskunftsrecht an Dritte findet sich in § 15 PAO; an dieser Stelle ist die Akteneinsicht ausdrücklich ausgeschlossen und die Vorschrift nennt Bedingungen, sollte keine Einwilligung des Betroffenen für die Auskunftserteilung gegeben sein.

Bei Streitigkeiten verweist die PAO in § 21 auf die Datenschutzgerichte und entsprechend auf die Kirchliche Datenschutzgerichtsordnung (KDSGO) – „unbeschadet der Möglichkeit der Verwaltungsbeschwerde (hierarchischer Rekurs)“. Ob diese Inanspruchnahme der kirchlichen Datenschutzgerichte von der KDSGO auch gedeckt ist, ist ihr allerdings nicht so ohne Weiteres zu entnehmen.

1.2.2 Spezielles Verwaltungsrecht für kirchlichen Datenschutz

Das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) ist seit 1. Januar 2021 die neue zentrale Verfahrensordnung für die katholische Datenschutzaufsicht. Allgemein wird das staatliche Verwaltungsverfahrensgesetz wegen seiner großen Bedeutung für das gesamte Verwaltungsverfahren auch als das „Grundgesetz der Verwaltung“ bezeichnet. Das KDS-VwVfG fußt aber nicht nur auf den einschlägigen staatlichen Vorschriften. In dem Regelwerk haben auch kirchenrechtliche Vorgaben, insbesondere aus dem Codex Iuris Canonici (CIC), Berücksichtigung gefunden. So wird beispielsweise in § 5 zur Anhörung oder in § 21 zum Widerruf eines rechtmäßigen Verwaltungsaktes ausdrücklich auf Regelungen des CIC verwiesen.

Das KDS-VwVfG regelt, was die Datenschutzaufsicht tut und wie sie es tun darf. Explizit geregelt sind darin beispielsweise was ein Verwaltungsakt überhaupt ist, zentrale Verfahrensgrundsätze, die Anhörung der Verfahrensbeteiligten und wer damit gemeint ist, die Akteneinsicht als das zentrale Recht in einem rechtsstaatlichen Verfahren, die grundsätzlich in der Dienststelle der kirchlichen Datenschutzaufsicht zu erfolgen hat sowie Fristen oder die Zustellung von Schriftstücken.

Sämtliche (Erz-)Bistümer im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. haben das KDS-VwVfG in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 23. November 2020 in Kraft gesetzt und jeweils in ihren Amtsblättern veröffentlicht.

1.2.3 Gesetz zur Regelung des Rechtsinstruments nach § 29 KDG im Erzbistum Freiburg

Nach § 29 Abs. 3 KDG erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem kirchlichen Recht. Ein solches anderes Rechtsinstrument hat das Erzbistum Freiburg im Berichtszeitraum geschaffen (s. Kasten). Dies vermindert den Verwaltungsaufwand, beispielsweise wenn Verrechnungsstellen für Kirchengemeinden Daten verarbeiten, weil nicht mehr unzählige Auftragsverarbeitungsverträge zwischen den verschiedenen kirchlichen Rechtspersonen geschlossen werden müssen. Künftig kann hier auf das § 29-KDG-Gesetz als Rechtsgrundlage zurückgegriffen werden.

Das § 29-KDG-Gesetz vom 21. Mai 2021 und die hierzu erlassene Durchführungsverordnung (§ 29-KDG-Gesetz-DVO) im Bereich der Erzdiözese Freiburg sind am 1. Juni 2021 in Kraft getreten.

§ 29-KDG-Gesetz (Auszug)

Zur Regelung des Rechtsinstruments nach § 29 KDG über die Verarbeitung personenbezogener Daten im Auftrag wird das nachfolgende Gesetz erlassen:

§ 1 Anwendungsbereich

Dieses Gesetz gilt für kirchliche Stellen im Bereich der Erzdiözese Freiburg, die im weltlichen Rechtskreis öffentlich-rechtlich verfasst sind. Hierzu gehören neben der Erzdiözese insbesondere die Katholischen Dekanatsverbände, die Katholischen Gesamtkirchengemeinden und die röm.-kath. Kirchengemeinden. Es gilt auch für die sonstigen öffentlich-rechtlich verfassten selbstständigen Vermögensmassen, insbesondere die kirchlichen Stiftungen des öffentlichen Rechts der Erzdiözese Freiburg.

§ 2 Verarbeitung personenbezogener Daten im Auftrag

Die Verarbeitung personenbezogener Daten im Auftrag erfolgt gemäß § 29 Absatz 3 KDG aufgrund eines Vertrages oder aufgrund dieses Gesetzes. Hierbei sind insbesondere die Vorgaben nach § 29 Absatz 3 und 4 KDG zu beachten.

…

1.2.4 Patientendatenschutz reloaded

Im Laufe des Berichtsjahres 2021 haben die Bistümer Fulda, Limburg und Trier im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. das Seelsorge-Patientendatenschutzgesetz (Seelsorge-PatDSG) in ihren Amtsblättern veröffentlicht, so dass dieses nunmehr dort gilt. Limburg und Trier haben das Seelsorge-PatDSG in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) vom 23. November 2020 veröffentlicht. In Fulda wurde ebenfalls diese Fassung zugrunde

gelegt und nur leichte Änderungen am Text vorgenommen. So wurde beispielsweise auf die Revisionsklausel („Dieses Gesetz soll innerhalb von fünf Jahren ab Inkrafttreten überprüft werden.“) verzichtet.

Die Gesetze lösen jeweils die Ordnungen zum Schutz von Patientendaten in katholischen Krankenhäusern und Reha-Kliniken in den drei Bistümern ab.

Das Seelsorge-PatDSG soll Patientendaten bei der Seelsorge in katholischen Gesundheitseinrichtungen schützen. Gleich in der Präambel erfolgt der Hinweis, dass die Seelsorge so zu gestalten ist, „dass das Persönlichkeitsrecht auf Schutz der Patientendaten gewahrt wird“.

Das PatDSG regelt als besondere kirchliche Rechtsvorschrift den Schutz der Patientendaten in der Seelsorge – unabhängig von der Form und der Art ihrer Verarbeitung. Ansonsten finden das KDG und die hierzu ergangenen Durchführungsvorschriften wie gewohnt unmittelbar Anwendung. Dennoch erfolgt in § 6 des Gesetzes der Hinweis, dass für die Übermittlung von Patientendaten „ausreichende technische und organisatorische Schutzmaßnahmen nach dem KDG und der KDG-DVO zu treffen“ sowie die Mitarbeitenden „ausdrücklich auf diese Schutzmaßnahmen hinzuweisen und entsprechend in die Nutzung der Geräte, die Anwendungen und die Schutzmaßnahmen einzuweisen“ sind.

In den Begriffsbestimmungen wird klargestellt, dass Patientendaten, zu denen auch personenbezogene Daten von Angehörigen und Bezugspersonen gehören, Gesundheitsdaten im Sinne des KDG und damit besonders schützenswerte besondere Kategorien personenbezogener Daten darstellen.

Das PatDSG ist um die Stärkung der Datenschutzrechte von Patienten bemüht. So braucht es jetzt nach § 5 des kleinen Regelwerks in den drei Bistümern beispielsweise einer ausdrücklichen Einwilligung der Betroffenen für eine Weitergabe ihrer Patientendaten an deren Kirchengemeinden. Bisher musste der Patient einer Übermittlung explizit widersprechen oder es mussten Anhaltspunkte dafür bestehen, dass eine Übermittlung nicht angebracht ist.

1.3 Ausgewählte Rechtsprechung staatlicher Gerichte

1.3.1 Reichweite des Auskunftsanspruchs

Der Bundesgerichtshof (BGH) hat sich im Berichtszeitraum grundlegend mit dem Umfang des Auskunftsrechts nach Art. 15 DSGVO beschäftigt (Urteil vom 15. Juni 2021, Az.: VI ZR 576/19). Im Ursprungsverfahren machte der Kläger gegen den beklagten Versicherer Ansprüche auf Datenauskunft geltend. Das höchste deutsche Zivilgericht hat den daten-

schutzrechtlichen Auskunftsanspruch gemäß Art. 15 DSGVO inhaltlich ausgesprochen weit ausgelegt. So soll dieser „potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur umfassen, jedoch immer „unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt". Erfasst sind danach für das Gericht auch die zurückliegende Korrespondenz der Parteien, das „Prämienkonto" des Klägers und Daten des Versicherungsscheins sowie interne Vermerke und Kommunikation des Versicherers. Als Beispiel führt das Gericht an dieser Stelle ausdrücklich interne Vermerke über den Gesundheitszustand des Betroffenen an und solche, „die festhalten, wie sich der Kläger telefonisch oder in persönlichen Gesprächen geäußert hat".

Schreiben des Klägers an die Beklagte seien grundsätzlich ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO anzusehen. Der BGH weist in diesem Zusammenhang explizit darauf hin, dass auch die Tatsache, dass Schreiben dem Kläger bereits bekannt sind, für sich genommen den datenschutzrechtlichen Auskunftsanspruch nicht ausschließen. So erfahre die betroffene Person, ob die im Schriftverkehr enthaltenen personenbezogenen Daten aktuell verarbeitet, beispielsweise gespeichert, werden.

Das Auskunftsrecht der betroffenen Person diene hinsichtlich der sie betreffenden personenbezogenen Daten dem Zweck, sich der Verarbeitung dieser Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Sie soll sich insbesondere vergewissern können, dass die sie betreffenden Daten richtig sind und in zulässiger Weise verarbeitet werden.

1.3.2 Erteilung einer „Datenkopie"

Für das Bundesarbeitsgericht (BAG) ist ein Klageantrag auf Überlassung einer Kopie von E-Mails nicht hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 der Zivilprozessordnung (ZPO), wenn die E-Mails, von denen eine Kopie zur Verfügung gestellt werden soll, nicht so genau bezeichnet sind, dass im Vollstreckungsverfahren unzweifelhaft ist, auf welche E-Mails sich die Verurteilung bezieht (Urteil vom 27. April 2021, Az.: 2 AZR 342/20).

Die Vorinstanz hatte noch angenommen, dass der Kläger zwar einen Anspruch auf Erteilung einer Kopie seiner personenbezogenen Daten im Rahmen des Auskunftsanspruchs habe, nicht aber auf die darüber hinaus verlangten Kopien seines E-Mail-Verkehrs sowie der E-Mails, die ihn namentlich erwähnen.

Der Kläger war im zugrunde liegenden Fall bei der Beklagten beschäftigt. Er begehrte mit seiner Klage unter anderem Auskunft über seine von der Beklagten verarbeiteten personenbezogenen Daten sowie die Überlassung einer Kopie dieser Daten gemäß Art. 15 Abs. 3 DSGVO.

Die Richter ließen aber ausdrücklich offen, ob das Recht auf Überlassung einer Kopie überhaupt die Erteilung einer Kopie von E-Mails umfassen kann. Jedenfalls müsse ein

solcher Anspruch entweder mit einem hinreichend bestimmten Klagebegehren oder, sollte dies nicht möglich sein, im Wege der Stufenklage nach § 254 ZPO gerichtlich geltend gemacht werden.

1.3.3 Bestimmter Klageantrag bei Antrag nach DSGVO

In einem weiteren Urteil zu dieser Thematik hat das höchste deutsche Arbeitsgericht entschieden, dass ein Klageantrag, der ergänzend zum Wortlaut von Art. 15 Abs. 1 Halbs. 2 DSGVO auslegungsbedürftige Begriffe enthält, über deren Inhalt nicht behebbare Zweifel bestehen, nicht hinreichend bestimmt ist (Urteil vom 16.12.2021, Az.: 2 AZR 235/21).

Eine Verwendung von auslegungsbedürftigen Begriffen sei abzulehnen. Denn eine Klärung des Auskunftsumfangs dürfe nicht in das Vollstreckungsverfahren verlagert werden.

Ein Beschäftigter wollte im Rahmen einer Kündigungsschutzklage auch „Auskunft über ‚Leistungs- und Verhaltensdaten', aber nicht über diejenigen, die in seiner Personalakte gespeichert sind". Das war den Richtern jedoch nicht hinreichend bestimmt genug. Bei den genannten Ausdrücken handele es sich um unbestimmte Rechtsbegriffe, deren vollstreckungsrechtliche Reichweite „völlig unklar" sei. Entsprechend hat das BAG die Klage als unzulässig abgewiesen.

1.3.4 Keine DSGVO in evangelischem Krankenhaus

Das Landgericht (LG) Siegen hatte sich im Jahr 2021 mit der Anwendbarkeit der DSGVO auf eine Klinik in Trägerschaft der Evangelischen Kirche zu beschäftigen (Beschluss vom 26.11.2021, Az.: 2 O 236/21). Es ist nach ausführlicher Begründung zu dem Schluss gekommen, dass eine Patientin eines evangelischen Krankenhauses ihren Datenauskunftsanspruch nicht auf Art. 15 DSGVO stützen kann, sondern lediglich auf § 19 des Datenschutzgesetzes der Evangelischen Kirche Deutschland (DSG-EKD).

Im vorliegenden Streit der Parteien über ärztliche Behandlungsfehler begehrte die Antragstellerin auch eine vollständige Datenauskunft sowie ein Schmerzensgeld wegen bislang nicht erteilter Auskunft auf Basis der DSGVO.

Die kirchenrechtlichen Datenschutzregeln seien vorrangig anwendbar, wenn sie mit der DSGVO in Einklang gebracht werden könnten und bereits vor Inkrafttreten der DSGVO bestanden hätten. Dies sei beim DSG-EKD der Fall.

Das LG habe die Anträge der Antragstellerin auch nicht als ein Auskunftsbegehren nach § 19 DSG-EKD auslegen können. Denn für ein solches Begehren sei nicht der Rechtsweg zur Zivilgerichtsbarkeit, sondern vielmehr der zu den evangelischen Verwaltungsgerichten eröffnet.

1.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte

1.4.1 Wiedereinsetzung in den vorigen Stand

Anfang 2021 hat sich das Interdiözesane Datenschutzgericht (IDSG) in einer Entscheidung mit der sogenannten Wiedereinsetzung in den vorigen Stand beschäftigt (Beschluss vom 2. Januar 2021, Az.: IDSG 09/2020). Diese ist auf Antrag zu gewähren, wenn jemand ohne Verschulden verhindert war, eine gesetzliche Frist einzuhalten. Die KDSGO enthält hierzu keine Regelungen. Die Grundsätze des § 60 der Verwaltungsgerichtsordnung (VwGO) sind aber, so das Gericht, entsprechend anzuwenden. Dies folge aus dem Grundsatz des effektiven Rechtsschutzes, wie er in der Präambel der KDSGO Ausdruck gefunden habe. Danach diene die Einrichtung der kirchlichen Datenschutzgerichte der Gewährleistung eines wirksamen Rechtsschutzes auf dem Gebiet des Datenschutzes. Im Fall einer unverschuldeten Fristversäumnis erfordere es das Gebot effektiven Rechtsschutzes, eine Wiedereinsetzung in den vorigen Stand zu ermöglichen.

Im zugrunde liegenden Fall wurde die Monatsfrist des § 8 Abs. 2 Satz 1 KDSGO wegen „Unklarheit“ im Bescheid über die Adressatenstellung nicht eingehalten. Nach dieser Vorschrift sind Anträge des Verantwortlichen gegen Bescheide der Datenschutzaufsicht innerhalb eines Monats nach Zugang des Bescheides zu stellen.

1.4.2 Zurechnung von Geldbußen

In einem weiteren Fall ging es vor dem IDSG um eine von einem Krankenhaus falsch versandte Rechnung und ein daraufhin von der Datenschutzaufsicht ausgesprochenes Bußgeld wegen Organisationsverschuldens (Beschluss vom 19. April 2021, Az.: IDSG 14/2020). Der Verantwortliche ging dagegen vor und machte geltend, dass ihm das Verhalten seiner Mitarbeiter nicht zugerechnet werden könne, weil es im kirchlichen Datenschutzrecht schlicht an einer Zurechnungsnorm fehle. Dem widersprach das Gericht. „Juristische Personen haften in Bezug auf Geldbußen als Verantwortliche gemäß dem Funktionsträgerprinzip für schuldhafte Datenschutzverstöße aller ihrer Mitarbeiter unabhängig davon, ob die Mitarbeiter eine Organstellung oder eine andere Führungsposition (§ 30 Abs. 1 OWiG) innehaben.“ So steht es ausdrücklich in einem der diesbezüglichen Leitsätze auf der IDSG-Website.

Die Richter versäumen es nicht, in diesem Zusammenhang darauf hinzuweisen, dass die Geltung des Funktionsträgerprinzips im Datenschutzrecht nach der DSGVO durchaus umstritten ist. Sie folgen diesbezüglich aber ausdrücklich „der Rechtsprechung des Landgerichts Bonn und der überwiegenden Auffassung in der Literatur, wonach nur das Funktionsträgerprinzip nach dem Vorbild des europäischen Kartellrechts in der Lage ist, die Einheitlichkeit und die Effektivität der Verhängung von Geldbußen gemäß Art. 83 DSGVO zu gewährleisten“.

Das für die Geldbußen gemäß der DSGVO geltende Funktionsträgerprinzip sei somit auch bei der Verhängung von Geldbußen nach kirchlichem Datenschutzrecht gemäß § 51 KDG anzuwenden. Die Übertragung des europarechtlichen Funktionsträgerprinzips auf das kirchliche Bußgeldrecht werde bereits durch die Präambel des KDG nahegelegt. Danach wolle das KDG den Einklang des kirchlichen Datenschutzrechts mit der DSGVO herstellen. Im Übrigen, so das Gericht weiter in seiner Begründung, gebiete der Grundsatz der Effektivität des Datenschutzes die Anwendung des Funktionsträgerprinzips.

> **„Geldbußen gegen einzelne Mitarbeiterinnen oder Mitarbeiter scheiden nach Auffassung der Richter auf der Grundlage der Definition des Verantwortlichen bei der Datenverarbeitung durch juristische Personen grundsätzlich aus.“**

Geldbußen gegen einzelne Mitarbeiterinnen oder Mitarbeiter scheiden nach Auffassung der Richter auf der Grundlage der Definition des Verantwortlichen bei der Datenverarbeitung durch juristische Personen grundsätzlich aus. Sie seien allenfalls möglich beim sogenannten Mitarbeiterexzess und bei Beschäftigten, die wegen ihrer besonderen Rechtsstellung – beispielsweise als Betriebsrat – weisungsfrei handeln. Wenn anstelle des Funktionsträgerprinzips das nationale Ordnungswidrigkeitenrecht angewendet würde, könnten die meisten Datenschutzverstöße nicht mit einer Geldbuße sanktioniert werden, weil sie von Mitarbeitenden ohne Führungsfunktion begangen wurden. Das IDSG hatte bereits in seinem Beschluss vom 14. Dezember 2020 (Az.: IDSG 01/2020) – wenn auch noch ohne ausdrückliche Nennung des Begriffs „Funktionsträgerprinzip“ – darauf hingewiesen, dass dem Rechtsträger als dem Verantwortlichen nicht nur das Verhalten von Organen, sondern auch das Verhalten anderer Beschäftigter zugerechnet wird (siehe hierzu schon die Ausführungen im Tätigkeitsbericht für das Jahr 2020).

Die Anwendung des Funktionsträgerprinzips bestätigt das Gericht auch noch einmal in einem Beschluss vom 12. Juli 2021 (Az.: IDSG 21/2020). In diesem Fall ging es um die Aushändigung eines Entlassungsberichts an den Ehemann einer Patientin trotz eines Sperrvermerks im Krankenhausinformationssystem. Auch hier wurde ein Bußgeld verhängt.

1.4.3 Empfindliche „Wunsch-Großeltern“

In einer Klage hatte sich das IDSG im Berichtsjahr mit einem Vorfall zu beschäftigen, bei dem die Praktikantin eines Caritasverbands Informationen an registrierte „Wunsch-Großeltern“ geschickt hatte – und das aus Versehen mit einem offenen E-Mail-Verteiler (Beschluss vom 29. November 2021, Az.: IDSG 04/2019).

Eine angeschriebene „Wunsch-Oma“ befürchtete daraufhin, dass sie, komme ihr Engagement an die Öffentlichkeit, womöglich on- und offline verspottet würde. Das Gericht sah zwar in dem offenen Versand eine Datenschutzverletzung, die von der Klägerin begehrte

Feststellung, dass es sich um einen „schwerwiegenden Datenschutzverstoß“ handelte, verweigerte es aber. Eine solche Qualifizierung finde sich weder im KDG noch in der KDSGO, daher sei der Antrag unzulässig.

1.4.4 Unverschuldete Fristversäumnis

In der ersten veröffentlichten Entscheidung der 2. Instanz, dem Datenschutzgericht Deutsche Bischofskonferenz (DSG-DBK), geht es wie bereits zuvor schon unter 1.4.1 um das wichtige, aber auch umstrittene Thema der Wiedereinsetzung in den vorigen Stand (Beschluss vom 28. April 2021, Az.: DSG-DBK 04/2020). Im zugrunde liegenden Fall wurde die Jahresfrist, in der ein Antrag auf Überprüfung einer Entscheidung der Datenschutzaufsicht beim IDSG gestellt werden muss, gerissen. Das DSG-DBK stellt klar, dass diese in § 2 Abs. 3 S. 1 KDSGO normierte Frist mit der DSGVO in Einklang steht und nicht das staatliche Datenschutzniveau unterläuft. Die entsprechenden Fristen des staatlichen deutschen Rechts in § 58 Abs. 2 VwGO (Jahresfrist bei Nichtvorhandensein einer Rechtsbehelfsbelehrung) und § 74 VwGO (Monatsfrist als Regelfall) stünden vor diesem Hintergrund mit der DSGVO in Einklang. Da die in § 2 Abs. 3 S. 1 KDSGO normierte Jahresfrist der längeren der beiden in der VwGO normierten Fristen entspreche, stehe auch diese kirchliche Norm mit der DSGVO in Einklang und verkürze die Möglichkeiten der prozessualen Durchsetzung datenschutzrechtlicher Rechte nicht in unzulässiger Weise.

Es handele sich bei § 2 Abs. 3 S. 1 KDSGO um eine prozessuale Norm, unter anderem mit der Folge, dass eine Wiedereinsetzung in den vorigen Stand entsprechend § 60 VwGO bei einer unverschuldeten Fristversäumung möglich sein soll – was vorliegend jedoch von den Richtern verneint wurde.

1.4.5 Kein vorbeugender Rechtsschutz

Im zweiten veröffentlichten Beschluss verneint das oberste deutsche kirchliche Datenschutzgericht die Möglichkeit, einen Antrag auf Gewährung vorbeugenden Rechtsschutzes zu stellen (Beschluss vom 20. Mai 2021, Az.: DSG-DBK 02/2020). Ein solcher Antrag sei nach der KDSGO unzulässig. Denn die kirchlichen Datenschutzgerichte würden nach § 2 Abs. 1 S. 1 KDSGO nur über Entscheidungen von Datenschutzaufsichten der Katholischen Kirche und über gerichtliche Rechtsbehelfe der betroffenen Person gegen den Verantwortlichen oder den kirchlichen Auftragsverarbeiter entscheiden. Dies setze aber voraus, dass ein Datenschutzverstoß bereits stattgefunden haben müsse.

1.4.6 Der Pfarrer kennt seine Schäfchen

Eine weitere vom DSG-DBK veröffentlichte Entscheidung lässt uns tief in das das Jahr 2021 alles bestimmende Thema „Corona“ eintauchen (Beschluss vom 12. Juli 2021, Az.: DSG-DBK 01/2021). Es geht in dem umstrittenen Richterspruch darum, ob ein Pfarrer

nach den Gottesdiensten die Teilnehmerlisten auf ihre Richtigkeit und Vollständigkeit überprüfen darf. Im Gegensatz zur zuständigen Datenschutzaufsicht sehen die beiden kirchlichen Datenschutzgerichte darin keine Datenschutzverletzung.

Ein Pfarrer könne Einsicht in die Gottesdienstbesucherliste nehmen, um die Vollständigkeit der Liste zu kontrollieren und die Einhaltung des Corona-Schutzkonzepts zu prüfen.

Rechtliche Grundlage für die Einsichtnahme in die Gottesdienstlisten finde sich in § 6 Abs. 1 lit. d) KDG, wonach die Verarbeitung personenbezogener Daten zulässig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist. Als Veranstalterin von Gottesdiensten oblägen der Rechtsmittelgegnerin die Verpflichtungen des staatlichen Rechts, hier konkret der damals geltenden Corona-Schutzverordnung des Bundeslands.

1.4.7 Teilweiser Kirchenaustritt geht nicht

Mit diesem Verfahren vor dem DSG-DBK sollte der IDSG-Beschluss vom 9. Dezember 2020 gekippt werden (Az.: IDSG 05/2019), über das bereits im Tätigkeitsbericht 2020 berichtet worden war („Kein teilweiser Kirchenaustritt durch Datenschutz“). Die 2. Instanz bestätigte jedoch in vollem Umfang die erstinstanzliche Entscheidung: „Bei einem Kirchenaustritt kann nicht gem. § 18 Absatz 1 Satz 1 KDG die Eintragung einer Ergänzung im Taufregister verlangt werden, wonach die betroffene Person aus der Katholischen Kirche als ‚Körperschaft des öffentlichen Rechts‘ ausgetreten ist“ (Beschluss vom 16. September 2021, Az.: DSG-DBK 05/2020). Der Kläger ist mit seinem Plan, dass sich sein Kirchenaustritt auf das Ausscheiden aus der öffentlich-rechtlichen Körperschaft beschränkt und keine innerkirchlichen Wirkungen hat, auch in der nächsten Gerichtsinstanz gescheitert.

Wie schon das IDSG verweist das DSG-DBK darauf, dass es nicht der datenschutzrechtlichen Beurteilung unterliegt, welche Bedeutung die Austrittserklärung des Klägers für das Verhältnis zwischen ihm und der Katholischen Kirche hat. Denn es handele sich hierbei nicht um eine Frage der Richtigkeit bzw. Unrichtigkeit personenbezogener Daten nach dem KDG, hier des § 18 Abs. 1 KDG. Vielmehr gehe es insoweit um die nach innerkirchlichem Recht zu beurteilende Beziehung zwischen einem Mitglied einer Religionsgemeinschaft und der Religionsgemeinschaft. Ob es eine Mitgliedschaft in der Körperschaft des öffentlichen Rechts gibt, die von der Mitgliedschaft in der Religionsgemeinschaft als Glaubensgemeinschaft zu trennen ist und die deshalb isoliert aufgegeben werden kann, beantworte sich nach dem theologischen Selbstverständnis der Religionsgemeinschaft und ihrem darauf aufgebauten innergemeinschaftlichen Recht.

Dieses theologische Selbstverständnis habe jedoch keinen Niederschlag in den datenschutzrechtlichen Bestimmungen gefunden.

Ausgewählte Entscheidungen der beiden kirchlichen Gerichte in Datenschutzangelegenheiten IDSG und DSG-DBK sind auf der Website der Deutschen Bischofskonferenz veröffentlicht:

www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten

2 Schwerpunkte der Tätigkeiten im Berichtszeitraum

2.1 Datenschutzverletzungen

Die Zahl der gemeldeten Datenschutzverletzungen im Berichtszeitraum ist im Vergleich zu den Vorjahren leicht angestiegen und diese waren zum Teil immer noch durch die Pandemie geprägt, etwa Datenpannen im Homeoffice, Corona-Regelungen am Arbeitsplatz oder Livestreams von Gottesdiensten.

Die „Alltagsthemen“ beschäftigten die Datenschutzaufsicht daneben in gewohnter Weise – mit zahllosen Meldungen zu Einbrüchen in Kindertagesstätten und geklauten elektronischen Geräten, gehackten Servern, falsch versandten Arztbriefen oder E-Mails, die mit offenem Verteiler versandt wurden. Tagesgeschäft eben.

Doch dann kam auf einmal die Flut und legte sich wie eine Schlange um Schuld und andere Ortschaften im beschaulichen Ahrtal. Das Flüsschen Ahr verwandelte sich in kurzer Zeit in einen reißenden Strom und zerstörte unzählige Gebäude sowie die Infrastruktur im Tal. Es dauerte nicht lange, da gingen die ersten Meldungen zu Datenschutzverletzungen von katholischen Einrichtungen beim Datenschutzzentrum Frankfurt/M. ein. Die teils erschütternden Meldungen und persönlichen Schilderungen aus dem Katastrophengebiet bewegten die Mitarbeiterinnen und Mitarbeiter sehr. Vor allem die Berichte aus dem Epizentrum der Katastrophe, der Gemeinde Schuld, in der sich viele Einrichtungen befunden haben, ließen einen fassungslos zurück. Kindergärten und andere katholische Institutionen wurden einfach weggeschwemmt oder stark beschädigt. Die verheerenden Folgen der Flut waren zu Beginn gar nicht absehbar. Ganze Schränke mit Unterlagen und Datenbeständen wurden unauffindbar aus den Gebäuden gespült, Computer, Laptops, Kameras und Handys folgten ihnen.

Auch andere Orte im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. wie die Gemeinde Kordel wurden durch die Flutkatastrophe schwer getroffen. Hier trat die Kyll über die Ufer und beschädigte viele Gebäude. Wasser- und Schlammmassen

schoben sich durch die Kitas und zerstörten alles auf ihrem Weg – auch Kinderakten mit Entwicklungsdokumentationen und zahlreiche Datenträger.

Dass so schnell nach der Jahrhundertflut von den verantwortlichen Stellen an den Datenschutz gedacht wurde, zeigt dessen hohen Stellenwert. Da zu diesem Zeitpunkt aber überhaupt noch nicht absehbar war, wie hoch der Verlust an personenbezogenen Daten war und welche Risiken für diese bestehen, wurden schnell auf telefonischem und elektronischem Wege pragmatische Lösungen gefunden.

Diese Flutkatastrophe hat deutlich aufgezeigt, dass manche Situationen nicht vorhersehbar und mithin nicht planbar sind. Insoweit hat sich der Datenschutzaufsicht die Frage nach einer Ahndung von Datenschutzverletzungen nicht gestellt. Technische und organisatorische Maßnahmen stellen dennoch einen zwingenden Bestandteil des Datenschutzes dar, dessen Einhaltung geboten ist. Aus betroffenen Krankenhäusern kam unter anderem die Rückmeldung, dass aufgrund der Erfahrungen durch das Hochwasser verstärkt nach Alternativen zu papierbasierten Lösungen gesucht wird. Würde die Flutkatastrophe an dieser Stelle die Digitalisierung wirklich vorantreiben, hätte sie wenigstens irgendetwas Gutes gebracht.

2.1.1 Gelegenheit macht Diebe

Geschichten, die das (Krankenhaus-)Leben schreibt. Eine Klinik meldete im Berichtszeitraum eine Datenschutzverletzung, die geschieht, wenn Menschen ihren Gefühlen am Arbeitsplatz zu viel Raum geben. Eine Krankenhausmitarbeiterin schaute sich die Patientenakte der aktuellen Lebensgefährtin ihres Ex-Freundes etwas genauer an, obwohl sie in einer ganz anderen Abteilung beschäftigt war und fotografierte sogar Inhalte ab. Dies blieb der aktuellen Freundin nicht verborgen und sie brachte das Ganze ins Rollen. Die neugierige Ex gab nach kurzer Zeit ihr Fehlverhalten zu und begründete es mit den persönlichen Verflechtungen und den darauf fußenden Konflikten, die sie zu der Tat getrieben hätten. Diese blieb auch alles andere als folgenlos. Die Schnüffeleien haben erhebliche arbeitsrechtliche Konsequenzen für die Mitarbeiterin und frühere Freundin nach sich gezogen.

Die auch von der Datenschutzaufsicht angestoßenen Untersuchungen im Klinikum ergaben, dass sich eine andere Mitarbeiterin beim Verlassen ihres Arbeitsplatzes nicht ordnungsgemäß abgemeldet hatte und so der ehemaligen Lebensgefährtin die Einsicht in die Patientenakte erst ermöglicht hat. Eine Überprüfung der Berechtigungen führte in diesem Zusammenhang zu notwendigen Korrekturen.

2.1.2 Ungesunde Transparenz

Eine Pfarrgemeinde hatte Mitte des Jahres 2021 den Grundsatz der Transparenz im Datenschutz wohl etwas zu wörtlich genommen. Sie teilte auf ihrer Homepage und in lokalen

> **Die Notwendigkeit von regelmäßigen Schulungen der Mitarbeiterinnen und Mitarbeiter im Datenschutz zeigt sich durch solche Begebenheiten immer wieder eindrücklich.**

Medien mit, dass das Pfarrbüro wegen der Erkrankung der Pfarrsekretärin geschlossen sei. Und da die Mitarbeiterin vier Wochen wegen ihrer Krankheit ausfiel, wurde auch konsequenterweise diese Information viermal in den genannten Medien veröffentlicht. Wie meist, steckt auch hinter dieser Datenschutzverletzung kein böser Wille. Doch da es vorliegend immerhin um sensible Gesundheitsdaten ging, konnte das Kath. Datenschutzzentrum Frankfurt/M. nicht von einer Beanstandung in Form eines Bescheids absehen. Eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten in Form der Offenlegung, hier die öffentliche Nennung der Arbeitsunfähigkeit der Pfarrsekretärin, war weit und breit nicht ersichtlich. Die Notwendigkeit von regelmäßigen Schulungen der Mitarbeiterinnen und Mitarbeiter im Datenschutz zeigt sich durch solche Begebenheiten immer wieder eindrücklich.

2.1.3 Streitschlichtung mal anders

Ein wahrlich literarisches Highlight und dazu noch ein sehr lehrreiches verbarg sich in der Meldung einer Datenschutzverletzung eines betrieblichen Datenschutzbeauftragten eines Krankenhauses. Ein Ordner mit Streitakten war aus einem verschlossenen Büro spurlos verschwunden. Nachdem die üblichen Verdächtigen wie Beschäftigte oder die MAV sich ahnungslos zeigten, stellte sich heraus, dass eine Reinigungskraft den Ordner, der gefährlich nahe am Mülleimer gestanden hatte, resolut mitentsorgt hatte. Da sich in Klageakten aber nun einmal zahlreiche personenbezogene Daten befinden, erfolgte die Nachricht an die Datenschutzaufsicht.

Dem betrieblichen Datenschützer stellte sich dann die Frage, ob eventuell Betroffene benachrichtigt werden müssen, ob also ein Risiko für deren Daten besteht. Dies verneinte er nach einer Einschätzung der Risiken und begründete dies auf immerhin zwei eng bedruckten Seiten. Die Ausführungen gaben tiefe und dabei äußerst interessante Einblicke in die Wege des Restmülls in einem Klinikum bis zu dessen Vernichtung. Der Autor ging dabei vom schlimmstmöglichen Fall aus.

Was nämlich passieren könnte, wenn sich doch ein Blatt aus einer Akte aus einem mit allerlei Unrat versetzten gepressten Restmüllballen lösen und vom Winde verweht würde. Und was würde ein Finder mit ausreichend krimineller Energie wohl damit anfangen – womöglich Krankenhausleistungen erschleichen? Das Kath. Datenschutzzentrum Frankfurt/M. konnte sich nach diesem aufschlussreichen Exkurs in die Müllentsorgung der detailreichen Risikoabwägung nur anschließen und – nach einem Hinweis auf den offensichtlichen Schulungsbedarf im Datenschutz der am Vorfall Beteiligten – die Angelegenheit sauber abschließen.

2.2 Beschwerden

Die Anzahl der Beschwerden bewegte sich im Jahr 2021 ungefähr auf dem Niveau des Vorjahres – und diese waren ebenfalls noch durch die Pandemie geprägt. So wurde sich beispielsweise über die Angabe des genauen Impfdatums beim Besuch des Gottesdienstes beschwert oder dass PCR-Testergebnisse von Heimbewohnern an einen größeren Verteiler gemailt wurden. Weitere Beschwerden betrafen etwa unerwünschte Spendenaufrufe oder unzureichende Auskünfte im Rahmen von Auskunftsbegehren und eine Beschwerde hatte das heimliche Kopieren einer WhatsApp-Nachricht durch einen Pfarrer zum Gegenstand.

2.2.1 Verflixte Technik

Während der virtuellen Sitzung eines Kirchengemeinderats wurde von einem der Teilnehmer der Bildschirm geteilt, um mit den anderen in der Online-Runde Inhalte zu teilen. Da die Technik wohl nicht so wollte wie der Präsentierende, war zunächst der Bildschirmhintergrund des PCs zu sehen. Und darauf war deutlich das Foto einer Mitarbeiterin der Nachbarkirchengemeinde zu erkennen, die den Teilnehmerinnen und Teilnehmern noch aus ihrer früheren Tätigkeit in eben dieser Gemeinde bekannt war. Es dauerte nicht lange, da erfuhr die Angehimmelte von dem Ereignis und fiel aus allen Wolken.

Ermittlungen im Rahmen der Beschwerde ergaben, dass das Foto der Homepage ihrer Pfarrei entnommen wurde und sie der Veröffentlichung im Internet zugestimmt hatte. Dem heimlichen Verehrer war die gesamte Angelegenheit natürlich äußerst unangenehm, zumal sie hohe Wellen vor Ort geschlagen hat. Arbeitsrechtliche Konsequenzen blieben ebenfalls nicht aus. Doch rein aus datenschutzrechtlicher Sicht ist die Sache weit weniger heikel. Derweil wurde es auf der Website einsam um das Konterfei des Pfarrers. Die anderen Fotos wurden entfernt.

2.2.2 Kundendaten auf Homepage

Teuer wurde es für eine katholische Einrichtung, die auf ihrer Homepage ein Lehrvideo präsentierte, in dem zwar darauf geachtet wurde, dass keine Personen zu erkennen sind, sehr wohl aber Echtdaten von Kunden und deren Bestellungen. Eine Beschwerde brachte hier die Sache ins Rollen. Die verantwortliche Stelle räumte der Datenschutzaufsicht gegenüber als Grund für die Datenschutzverletzung menschliches Versagen ein – was nachvollziehbar ist, weil das Video vorher von verschiedenen Stellen geprüft wurde. Obwohl der Film zügig von der Website entfernt wurde, konnte dies ein Bußgeld nicht verhindern.

2.2.3 Mitgefangen, mitgehangen

Mit einer Beanstandung davongekommen ist eine katholische Kirchengemeinde, in deren Kindergarten die App „KiTaPlus“ eingesetzt wurde. Es handelt sich dabei um eine Verwaltungssoftware für Kitas, die auch als Kommunikationstool für Eltern und Einrichtungen dient. Nach einem Blick in die App musste eine Mutter, die spätere Beschwerdeführerin, feststellen, dass ihre Daten und die des Kindes auch vom Vater einsehbar sind, obwohl sie sich wegen Schwierigkeiten mit ihrem Ex-Mann extra unter anderem eine Geheimnummer zugelegt hatte. Im Rahmen der Sachverhaltsermittlung stellte sich heraus, dass zum einen keine Einwilligungen von den Eltern für die Datenverarbeitung eingeholt wurden und zum anderen, dass der Hersteller versäumt hat, Möglichkeiten in der Software vorzusehen, die Zugriffe auf bestimmte Daten verhindern. Nach diesem Vorfall hat der Hersteller der App zwar die Problematik erkannt und bereits angekündigt, eine Anpassung hinsichtlich der Variante getrenntlebender Eltern vorzunehmen. Doch im zugrunde liegenden Fall musste sich der Verantwortliche die Unzulänglichkeiten der Herstellerfirma zurechnen lassen. Zudem ist zukünftig genau darauf zu achten, für welche Verarbeitungstätigkeiten Einwilligungen erforderlich sind.

2.3 Anfragen

Nochmals gestiegen ist die Anzahl der Anfragen. Der Beratungsbedarf ist – auch, aber nicht nur bedingt durch die Pandemie – nach wie vor sehr hoch. Es zeigte sich im Berichtszeitraum auch, dass sich der Trend fortsetzt, die Datenschutzaufsicht bereits in einem frühen Stadium einzubinden.

Bei Abstimmungen zwischen kirchlichen und staatlichen Stellen wurde das Kath. Datenschutzzentrum Frankfurt/M. ebenfalls früh ins Boot geholt, um dem Datenschutz den nötigen Raum zu verschaffen. Dies betraf beispielsweise den Austausch von Sozialdaten im Betreuungsbereich, den Einsatz von Videokonferenz- und Office-Tools in katholischen Einrichtungen oder die Kontaktdatennachverfolgung in Gottesdiensten, die teilweise von den Bundesländern im Zuständigkeitsbereich unterschiedlich geregelt wurde und länderübergreifende (Erz-)Bistümer vor knifflige Fragen stellte.

2.4 Gerichtsverfahren

Im Berichtsjahr 2021 wurden lediglich zwei weitere Klagen gegen das Kath. Datenschutzzentrum Frankfurt/M. erhoben – eine wegen eines Bescheids im Zusammenhang mit dem Übergang von Patientendaten bei einer Praxisübernahme und eine zweite durch einen klagefreudigen Petenten wegen einer vermeintlichen Untätigkeit der Datenschutzaufsicht.

2.5 Prüfungen

Im Berichtsjahr wurde mit der datenschutzrechtlichen Prüfung von katholischen Kindertagesstätten begonnen. Per Zufallsgenerator wurden jeweils Einrichtungen aus den sieben (Erz-)Bistümern ausgewählt. Der Zufall führte das jeweilige Prüfteam, bestehend aus der Diözesandatenschutzbeauftragten sowie einem IT- und einem Rechtsreferenten, dann auch in landschaftlich reizvolle Gegenden im Zuständigkeitsgebiet des Kath. Datenschutzzentrums Frankfurt/M. Die durchgeführten Prüfungen erfolgten in der Regel vor Ort in der Einrichtung, einmal auch corona-bedingt virtuell.

Um den datenschutzkonformen Umgang mit personenbezogenen Daten im Rahmen des Betriebs einer Kita umfassend prüfen zu können, wurde dem Träger der Einrichtung mit dem Anschreiben ein eigens entwickelter Fragebogen und ein Begleitdokument mit Hinweisen zum Ablauf der Prüfung übersandt.

Ein eigens entwickelter Fragebogen mit Begleitdokumenten und Hinweisen

Katholisches Datenschutzzentrum
Frankfurt/M. KdöR

Fragebogen
zur Durchführung von Datenschutzprüfungen
in Kindertageseinrichtungen

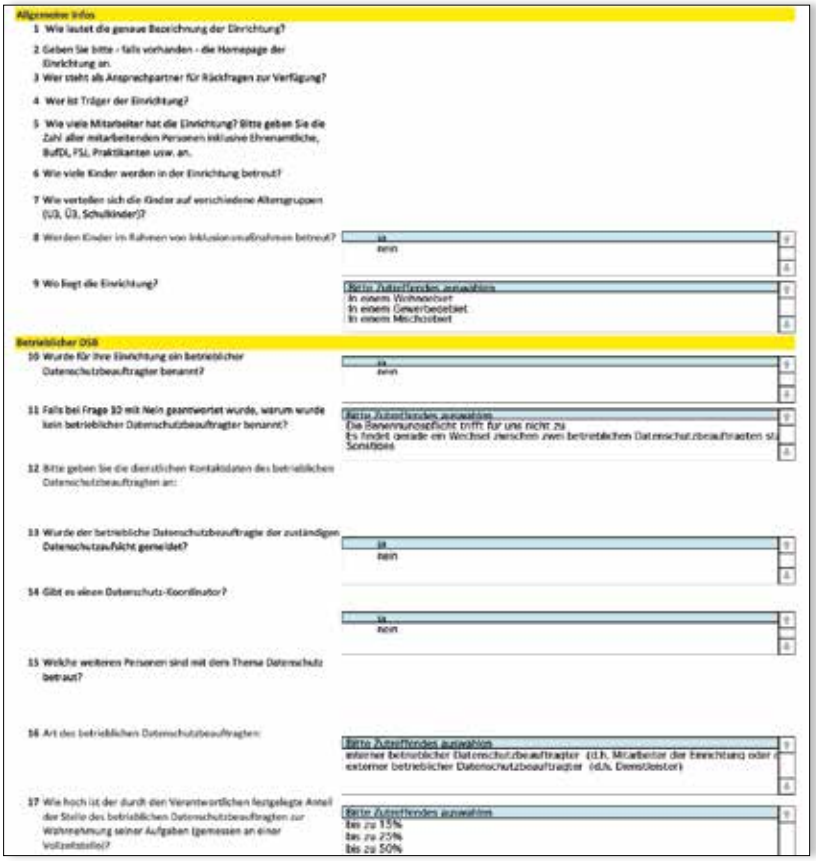
Hinweis:

Wir bitten um vollständige Beantwortung der in diesem Prüfkatalog gestellten Fragen und Zusendung der angeforderten Unterlagen bis spätestens innerhalb des im Anschreiben angegebenen Zeitraums.

Machen Sie sich bitte eine Kopie der ausgefüllten Excel Datei für Ihre Unterlagen.

Dieser Fragebogen ist zur Bearbeitung in Microsoft Excel optimiert. Es wird dringend empfohlen, den Fragebogen auf dem Computer auszufüllen. Für die Einträge von Freitexten können Sie die Zeilen-/Spaltengröße gerne verändern, die Auswahlelemente in anderen Zeilen sind an ihre Zelle gebunden. Sie können in den Formularelementen die Optionen Ihrer Wahl anklicken; sie sind dann blau markiert. Die Markierungen bleiben nach dem Speichern erhalten. Bitte fassen Sie sich bei Freitext-Antworten kurz, verweisen Sie -wo möglich- auf mitgelieferte Dokumente (bitte möglichst mit Kapitelnummer und/oder Seitenzahl). Bitte füllen Sie nur das erste Blatt "Fragebogen" aus, das zweite Blatt ist nur für die

...



Allgemeine Infos

1 Wie lautet die genaue Bezeichnung der Einrichtung?

2 Geben Sie bitte - falls vorhanden - die Homepage der Einrichtung an.

3 Wer steht als Ansprechpartner für Rückfragen zur Verfügung?

4 Wer ist Träger der Einrichtung?

5 Wie viele Mitarbeiter hat die Einrichtung? Bitte geben Sie die Zahl aller mitarbeitenden Personen inklusive Ehrenamtliche, BuFDi, FSJ, Praktikanten usw. an.

6 Wie viele Kinder werden in der Einrichtung betreut?

7 Wie verteilen sich die Kinder auf verschiedene Altersgruppen (U3, Ü3, Schulkinder)?

8 Werden Kinder im Rahmen von Inklusionsmaßnahmen betreut? ja / nein

9 Wo liegt die Einrichtung? Bitte Zutreffendes auswählen: In einem Wohngebiet / In einem Gewerbegebiet / In einem Mischobjekt

Betrieblicher DSB

10 Wurde für Ihre Einrichtung ein betrieblicher Datenschutzbeauftragter benannt? ja / nein

11 Falls bei Frage 10 mit Nein geantwortet wurde, warum wurde kein betrieblicher Datenschutzbeauftragter benannt? Bitte Zutreffendes auswählen: Die Benennungspflicht trifft für uns nicht zu / Es findet gerade ein Wechsel zwischen zwei betrieblichen Datenschutzbeauftragten st... / Sonstiges

12 Bitte geben Sie die dienstlichen Kontaktdaten des betrieblichen Datenschutzbeauftragten an:

13 Wurde der betriebliche Datenschutzbeauftragte der zuständigen Datenschutzaufsicht gemeldet? ja / nein

14 Gibt es einen Datenschutz-Koordinator? ja / nein

15 Welche weiteren Personen sind mit dem Thema Datenschutz betraut?

16 Art des betrieblichen Datenschutzbeauftragten: Bitte Zutreffendes auswählen: interner betrieblicher Datenschutzbeauftragter (d.h. Mitarbeiter der Einrichtung oder ... / externer betrieblicher Datenschutzbeauftragter (d.h. Dienstleistor)

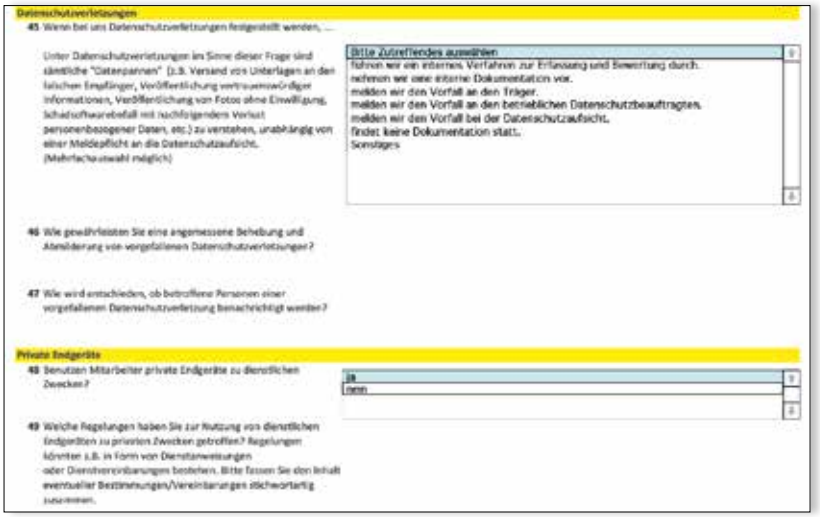
17 Wie hoch ist der durch den Verantwortlichen festgelegte Anteil der Stelle des betrieblichen Datenschutzbeauftragten zur Wahrnehmung seiner Aufgaben (gemessen an einer Vollzeitstelle)? Bitte Zutreffendes auswählen: bis zu 15% / bis zu 25% / bis zu 50%

Die anfängliche Zurückhaltung aufseiten der Einrichtungen legte sich zumeist schnell, wenn ersichtlich wurde, dass die Prüfung zum Ziel hat, kooperativ und konstruktiv den Datenschutz vor Ort voranzubringen und die Datenschutzaufsicht nur ihren gesetzlichen Verpflichtungen nachkommt.

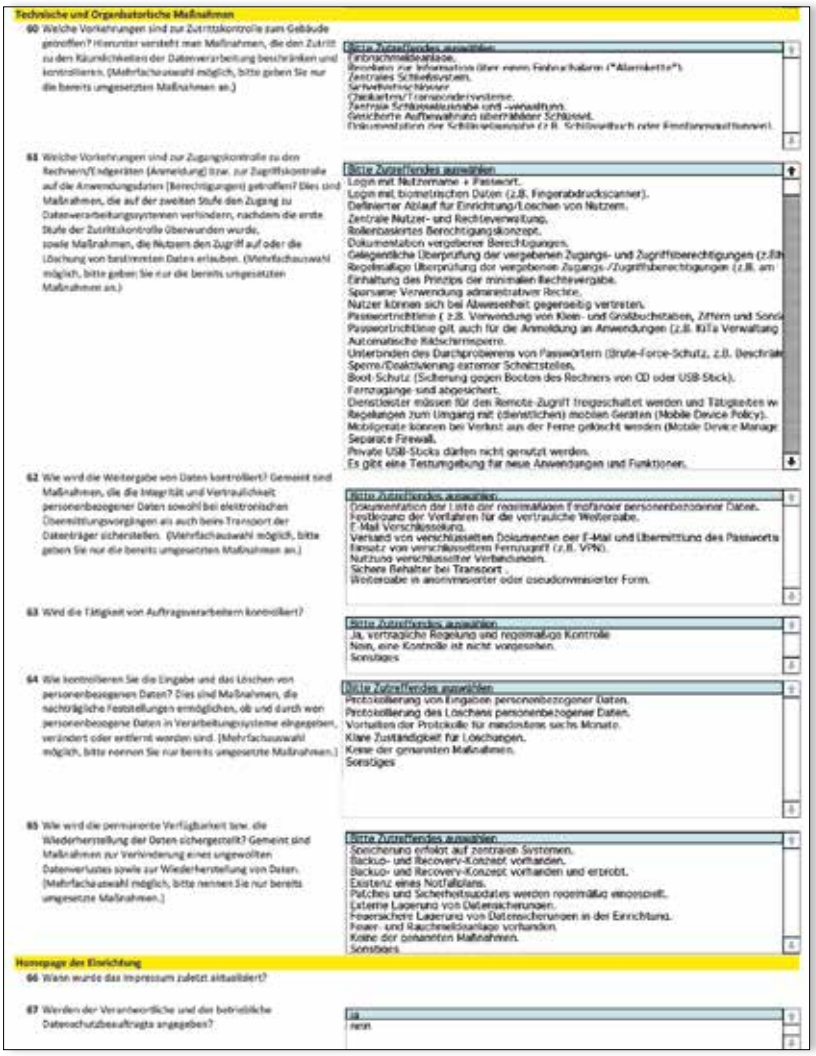
Wie sich rasch zeigte, war oft gleich zu Beginn die große Herausforderung, die rechtlichen Beziehungen zwischen den Beteiligten zu klären. Oft übernehmen andere Verwaltungsstellen des jeweiligen (Erz-)Bistums zentrale Aufgaben von den Kirchengemeinden als Trägerinnen der Einrichtungen, um diese von einigen Aufgaben beim Betrieb von Kitas zu entlasten.

Als Zwischenfazit kann an dieser Stelle festgehalten werden, dass die Einrichtungen in der Regel sorgsam mit personenbezogenen Daten umgehen und dank der betrieblichen Datenschutzbeauftragten, die in den (Erz-) Bistümern zur Unterstützung der Kirchengemeinden eingesetzt sind, im Datenschutz

gut aufgestellt sind. Optimierungsmöglichkeiten sehen die verschiedenen Prüfteams noch bei den Dokumentationspflichten und bei der regelmäßigen Schulung der Mitarbeiterinnen und Mitarbeiter im Datenschutz.



...



...

3 Veranstaltungen und Öffentlichkeitsarbeit

Schulungs- und Fortbildungsveranstaltungen konnten im Berichtszeitraum angeboten werden, die allerdings aufgrund der Pandemie wie schon im Jahr zuvor virtuell per Videokonferenztechnik stattfinden mussten.

So lud das Kath. Datenschutzzentrum Frankfurt/M. beispielsweise in der zweiten Jahreshälfte 2021 die betrieblichen Datenschutzbeauftragten der Bischöflichen Ordinariate und der Caritasverbände an zwei Terminen zum Austausch über datenschutzrechtlich relevante und interessierende Fragen ein. Bei dieser Gelegenheit wurden die Teilnehmenden auch eingehend in das KDM, das Kirchliche Datenschutzmodell, eingeführt. Bei einer Veranstaltung der Arbeitsgemeinschaften katholischer Krankenhäuser Rheinland-Pfalz und Saarland zum Datenschutz in Krankenhäusern bot sich ebenfalls die Möglichkeit, umfassend zu diesem aktuellen Thema zu referieren. Auch einer Einladung des DiCV Stuttgart zu einem digitalen Datenschutzforum folgte die Datenschutzaufsicht gerne und beteiligte sich unter anderem mit einem Vortrag zu datenschutzrechtlichen Aspekten des Faxversands.

Die Mitarbeiterinnen und Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. bildeten sich ihrerseits fort, beispielsweise in einem Live-Webinar zum Standard-Datenschutzmodell, in Veranstaltungen zum Datenschutz in der Pandemie und auch im Digitalunterricht oder nahmen an der 45. DAFTA teil.

4 Vernetzung mit anderen Datenschutzaufsichten

Die Vernetzung mit anderen Datenschutzaufsichten, ob kirchlich oder staatlich, ist ein wichtiges Mittel, um sachgerechte und möglichst einheitliche Lösungen für datenschutzrechtliche Herausforderungen in der betrieblichen Praxis zu finden. Hierzu dienen vor allem die regelmäßigen Konferenzen der fünf Diözesandatenschutzbeauftragten der Katholischen Kirche, in denen ein enger fachlicher Austausch stattfindet und einheitliche Leitlinien zu zentralen Themenstellungen besprochen werden.

Nachdem bereits im Jahr 2020 ein intensiver Austausch mit den staatlichen Aufsichtsbehörden in Baden-Württemberg und Rheinland-Pfalz stattgefunden hatte, folgten im Berichtszeitraum spannende und aufschlussreiche virtuelle Treffen mit der saarländischen Beauftragten für Datenschutz und Informationsfreiheit Monika Grethel und ihrem hessischen Kollegen Prof. Dr. Alexander Roßnagel, der das Amt des hessischen Beauftragten für Datenschutz und Informationsfreiheit am 1. März 2021 angetreten hat. Auch bei diesen beiden Begegnungen wurde am Ende von allen Seiten der Wunsch geäußert, den Austausch fortzusetzen.

> **„Da in vielen Bereichen, sei es im Krankenhaus-, im Kindertagesstätten- oder im Bildungsbereich ähnliche Fragen sowohl für evangelische wie auch für katholische Einrichtungen zu lösen sind, ist dieser Austausch auch sehr wichtig.“**

Mit den evangelischen Kolleginnen und Kollegen befindet sich das Kath. Datenschutzzentrum Frankfurt/M. ebenfalls auf verschiedenen Ebenen und zu ganz unterschiedlichen Themen in einem regelmäßigen und regen Austausch zu datenschutzrechtlichen Fragestellungen. So wurde zum Beispiel auf dem ökumenischen Datenschutztag der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche und der Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland, der im April 2021 stattgefunden hat, das Kirchliche Datenschutzmodell verabschiedet. Da in vielen Bereichen, sei es im Krankenhaus-, im Kindertagesstätten- oder im Bildungsbereich ähnliche Fragen sowohl für evangelische wie auch für katholische Einrichtungen zu lösen sind, ist dieser Austausch auch sehr wichtig.

5 Hinweise des Kath. Datenschutzzentrums Frankfurt/M.

Im Berichtsjahr 2021 hat das Kath. Datenschutzzentrum Frankfurt/M. seinen Einrichtungen im Zuständigkeitsbereich auch wieder praktische Hinweise zu aktuellen Datenschutzthemen auf Veranstaltungen und der Homepage gegeben.

5.1 Problematischer Fax-Versand

Im Jahr 2021 haben verschiedene staatliche Aufsichten Bedenken geäußert, dass der Versand von Fax-Nachrichten noch datenschutzkonform durchgeführt werden kann. Interessanterweise wäre der „klassische“ Fax-Versand über eine analoge Telefonleitung, innerhalb der durch das Telekommunikationsgesetz garantierten Sicherheit im Fernmeldewesen, eine sichere Verbindung. Die Unsicherheit kam in diesem Falle mit der Digitalisierung. Durch die digitale Übertragung gemäß dem TCP/IP-Protokoll, in dem Verschlüsselung nicht vorgesehen ist, wird der Kommunikationsweg unsicher. Die gesamten Daten werden hier in einzelne Pakete zerlegt, die über zum Teil zahlreiche Internetknoten ihren Weg zum Adressaten finden müssen. Insbesondere ist nicht vorhersagbar, welchen Weg die Pakete nehmen: Die Pakete eines digitalen Faxes, dessen Sender und Empfänger in Deutschland ansässig sind, könnten ohne Weiteres über Knoten im Ausland „geroutet“ werden, bevor sie beim Adressaten ankommen. Jeder dieser Knoten sei ein potenzieller Punkt, an dem die Daten mitgelesen werden könnten, zumal deren Betreiber oftmals kommerzielle Interessen hätten.

Aus diesen Gründen wird mittlerweile allgemein davon abgeraten, personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, per Fax zu übertragen, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind. Solche Schutzmaßnahmen sind möglich, gelten aber als aufwändig und teuer.

5.2 Gefährliche Schwachstelle in Microsoft Exchange

Am 2. März 2021 stellte der Hersteller Microsoft Software-Aktualisierungen („Patches“) für Microsoft Exchange zur Verfügung und machte auf aktuelle Beobachtungen von Ausnutzungen zuvor bekannt gewordener Schwachstellen aufmerksam. Es wurde von Microsoft dringend empfohlen, die Software-Aktualisierung sofort durchzuführen.

In den darauffolgenden Tagen erreichten das Kath. Datenschutzzentrum Frankfurt/M. tatsächlich zahlreiche Meldungen von Datenschutzverletzungen gemäß § 33 KDG, in denen es um die Kompromittierung von Microsoft Exchange Servern durch die Ausnutzung eben dieser Schwachstelle ging. Die nachfolgenden Untersuchungen der gemeldeten Fälle ergaben zumeist, dass die Verantwortlichen und ihre Dienstleiter oft mehrere Tage verstreichen ließen, bevor sie die bereit gestellten Patches installierten. Darüber hinaus

wurde beobachtet, dass oftmals keine definierten Prozesse für die Informationen über neue Software-Aktualisierungen und deren Installation existierten.

Gemäß § 26 KDG sind die Verantwortlichen verpflichtet, technische und organisatorische Maßnahmen zu treffen und regelmäßig zu überprüfen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Insbesondere ist der Verantwortliche nach § 16 Abs. 3 KDG-DVO verpflichtet, geeignete Maßnahmen gegen Angriffe und Schadsoftwarebefall zu treffen, wie beispielsweise ein Patch-Management. Die Datenschutzverletzungen wurden überwiegend mit Bescheid beanstandet und zum Teil mit Anordnungen zur Verbesserung der technischen und organisatorischen Maßnahmen erlassen.

5.3 Kirchliches Datenschutzmodell gibt Hilfestellung

Im April 2021 wurde als Ergebnis eines ökumenischen Projekts das Kirchliche Datenschutzmodell (KDM) veröffentlicht. Es überträgt die Methodik des staatlichen Standard-Datenschutzmodells (SDM), die nachvollziehbare Ableitung von technischen und organisatorischen Datenschutzmaßnahmen aus den gesetzlichen Anforderungen zu erleichtern, in das rechtliche Umfeld der Kirchen. Drei Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. haben sich in den Arbeitsgruppen „Risikoanalyse und Risikobehandlung“, „Referenzmaßnahmen Bausteine“ und „Kita-Fallbeispiel“ engagiert und an den darin erstellten Dokumenten mitgewirkt.

Im Herbst 2021 hat die Datenschutzaufsicht darüber hinaus in vier Workshops betriebliche Datenschutzbeauftragte und Verantwortliche aus ihrem Zuständigkeitsbereich in die Thematik des KDM eingeführt und Hinweise auf die Anwendung des KDM gegeben.

Weitere aktuelle Informationen zum Kirchlichen Datenschutzmodell sind unter folgendem Link zusammengestellt:
https://www.kirchliches-datenschutzmodell.de

6 Beschlüsse und Empfehlungen der Konferenz der Diözesandatenschutzbeauftragten

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche erörtert aktuelle Themen aus dem Bereich des kirchlichen Datenschutzes, fasst Beschlüsse und gibt auch von Zeit zu Zeit Empfehlungen zu wichtigen Themen, beispielsweise im Jahr 2021 zum datensparsamen Einsatz von Windows 10.

6.1 Beschluss betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG vom 4. Januar 2021

Geltungszeitraum des Beschlusses: 01.01.2021 bis längstens 30.04.2021

▶ **Zum Download**
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Beschluss-GB-29-Abs.-11-KDG-20210104.pdf

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands beschließt

- vor dem Hintergrund der speziellen Anforderungen des Kirchlichen Datenschutzgesetzes der (Erz-)Diözesen (KDG) aus § 29 Abs. 11 KDG,
- auf Grund des Endes der Übergangsphase zum 31.12.2020 zum Austritt des Vereinigten Königreiches von Großbritannien und Nordirland aus der Europäischen Union,
- auf der Basis des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich vom 24.12.2020 („TRADE AND COOPERATION AGREEMENT BETWEEN THE EUROPEAN UNION AND THE EUROPEAN ATOMIC ENERGY COMMUNITY, OF THE ONE PART, AND THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, OF THE OTHER PART", nachfolgend „Handelsabkommen"), vorläufig in Kraft getreten zum 01.01.2021,
- vorbehaltlich der Ablehnung oder etwaiger Änderungen des oben genannten Handelsabkommens durch das Europäische Parlament zur noch erforderlichen Genehmigung des Handelsabkommens,
- zur Vermeidung von Nachteilen katholischer Einrichtungen gegenüber außerkirchlichen Einrichtungen durch die Formulierung des § 29 Abs. 11 KDG,
- betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG im Geltungsbereich des Handelsabkommens, dass sie durch das Handelsabkommen, Abschnitt FINPROV.10A,
- für den Zeitraum vom 01.01.2021 bis zur Wirksamkeit einer Entscheidung der Europäischen Kommission nach Artikel 45 Abs. 3 DSGVO (Verordnung (EU) 2016/679) bezüglich des Vereinigten Königreichs von Großbritannien und Nordirland oder bis zum 30.04.2021, je nachdem, welches Ereignis eher eintritt und
- soweit und solange die in Abschnitt FINPROV.10A des Handelsabkommens aufgestellten Voraussetzungen erfüllt werden, ▶

für Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland die Voraussetzungen des § 29 Abs. 11 KDG durch das Handelsabkommen als erfüllt ansieht.

Begründung

Das Gesetz über den Kirchlichen Datenschutz (KDG) sieht in § 29 Abs. 11 Satz 1 KDG eine Voraussetzung für die Verarbeitung personenbezogener Daten durch Auftragsverarbeiter katholischer Einrichtungen vor, die die DSGVO nicht kennt.

> ***§ 29 Abs. 11 KDG:***
> *Der Auftragsverarbeiter darf die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten. Abweichend von Satz 1 ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Absatz 1 vorliegt oder wenn die Datenschutzaufsicht selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.*

Mit dem Austritt des Vereinigten Königreichs von Großbritannien und Nordirland aus der Europäischen Union und dem Europäischen Wirtschaftsraum (EWR) und dem Ende der Übergangsphase zum 31.12.2020 liegen die Voraussetzungen des § 29 Abs. 11 KDG nicht mehr vor, da (noch) kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

Zwar sieht das Handelsabkommen in Abschnitt FINPROV.10A, Zf. 1 vor, dass Datenübermittlungen aus der Europäischen Union in das Vereinigte Königreich von Großbritannien und Nordirland für den dort genannten Zeitraum und unter den dort genannten Voraussetzungen nicht als Drittlandtransfers von Daten gelten sollen. Diese Regelung kann aber auf Grund der spezifischen Formulierung des § 29 Abs. 11 KDG von den kirchlichen Einrichtungen bzw. deren Auftragsverarbeitern nicht direkt herangezogen werden.

Zur Vermeidung von Nachteilen der katholischen Einrichtungen trifft die Konferenz der Diözesandatenschutzbeauftragten in den obigen Beschluss, so dass für den im Handelsabkommen in Abschnitt FINPROV.10A genannten Zeitraum und unter den dort aufgestellten Bedingungen eine Datenverarbeitung durch Auftragsverarbeiter im Vereinigten Königreich von Großbritannien und Nordirland für die katholischen Einrichtungen in Deutschland erfolgen kann. ■

6.2 Verlängerung des Beschlusses betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG vom 22. April 2021

▶ Zum Download
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Verlängerung-Beschluss-GB-29-Abs.-11-KDG.pdf

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, den Geltungszeitraum des Beschlusses der Konferenz vom 04.01.2021 zur Übermittlung von Daten an das Vereinigte Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG bis zum 30.06.2021 zu verlängern, solange und soweit die im Beschluss genannten Bedingungen erfüllt sind.

6.3 Beschluss zur Beurteilung von Messenger- und anderen Social Media-Diensten (ersetzt den Beschluss der Konferenz vom 27.06.2018) vom 15. September 2021

▶ Zum Download
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/2021-09-15-Beschluss-zu-Messenger-Diensten.pdf

Die Konferenz der Diözesandatenschutzbeauftragten beschließt, die Kriterienliste aus dem Beschluss vom 26. Juli 2018 wie folgt zu aktualisieren:

Kriterien zur Beurteilung von Messenger- und anderen Social Media-Diensten

Vorbemerkung

Die katholischen Datenschutzaufsichten haben nachfolgend die aus ihrer Sicht relevanten Kriterien für die Bewertung und die Auswahl eines geeigneten Messenger-Produktes unter Datenschutz-Gesichtspunkten zusammengestellt. Neben diesen können aber auch andere Kriterien eine Rolle spielen, deren Erfüllung für die legale Verbreitung im kirchlichen Raum förderlich ist.

Kriterien, die ein Dienst aus Sicht des Datenschutzes erfüllen muss

Serverstandort: Wo verarbeitet der Dienst-Anbieter die Nutzerdaten? Hält der Provider die Drittlandbestimmungen ein, d. h. keine Datenspeicherung außerhalb der EU bzw. nur in Ländern, deren Datenschutzniveau durch die EU anerkannt ist?

Aus §§ 39-41 KDG ergibt sich, dass eine Verarbeitung personenbezogener Daten nur dann in einem Drittland, also außerhalb der EU, stattfinden darf, wenn besondere Bedingungen erfüllt sind. Das können ein Angemessenheitsbeschluss der Europäischen Kommission, geeignete Garantien (§ 40 KDG) oder eine explizite Einwilligung der betroffenen Person (§ 41 Abs. 1 KDG) sein.

Der Verantwortliche muss sich also überzeugen, dass die Rechtmäßigkeit der Verarbeitung durch Vorliegen mindestens einer dieser Bedingungen gegeben ist. Die Überprüfung der Rechtmäßigkeit der Verarbeitung in einem Drittland führt dabei in jedem Fall zu einem deutlich größeren Aufwand bei der Einrichtung des ▶

Verfahrens im Vergleich zu einem Betrieb in einem EU-Mitgliedsland. Schon aus diesem Grund sowie wegen des permanenten Risikos, dass die Rechtmäßigkeit durch Änderung z. B. der Gesetzeslage im Drittland oder Änderung der Anerkennungssituation entfällt, raten wir grundsätzlich von der dauerhaften Verarbeitung in einem Drittland ab, selbst wenn formal die Rechtmäßigkeit der Verarbeitung zum aktuellen Zeitpunkt gegeben wäre.

Sicherer Datentransport: Werden die Inhalte der Kommunikation Ende-zu-Ende verschlüsselt, also z.B. auch bei der Zwischenpufferung auf dem Server des Providers?

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. Als geeignete Maßnahme wird unter anderem die Verschlüsselung personenbezogener Daten ausdrücklich genannt. Auch in § 6 Abs. 1 lit. b) KDG-DVO wird Verschlüsselung als geeignete Maßnahme zum Schutz personenbezogener Daten bei deren Übertragung aufgeführt und in § 12 Abs. 2 lit. e) KDG-DVO für Daten der DSK II explizit gefordert. § 27 KDG fordert überdies, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Verschlüsselung darf deshalb nicht „optional zuschaltbar“ sein, sondern sollte per Default 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, durch eine sichere Datenhaltung in der Applikation, die die Daten z. B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt. Dem aktuellen Stand der Technik (im Jahr 2020) entsprechen Transport- und Inhaltsverschlüsselungen nach den Standards TLS mindestens in der Version 1.2 idealerweise mit Perfect Forward Secrecy[1] oder AES 128 und größer, idealerweise mit der Betriebsart GCM bzw. bei der Verwendung von EC-Verfahren eine Schlüssellänge von mindestens 250 Bit[2].

Falls vorhanden, sollten Zertifizierungen des Produktes oder des Anbieters durch unabhängige Institutionen in die Bewertung einfließen.

Datenminimierung: Werden höchstens Metadaten der Verbindung über das Verbindungsende hinaus gespeichert und auch diese so bald wie möglich gelöscht?

Eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß an personenbezogenen Daten wird in § 7 Abs.1 lit. c) KDG gefordert. Die Beschränkung gilt für die Menge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist

zu fordern, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten Kommunikation, sobald wie möglich gelöscht werden. Eine Speicherung von Inhalten der Kommunikation auf dem zentralen Server ist – genau wie ein Mitlesen durch den Serviceprovider – nicht akzeptabel.

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.

Respektierung der Rechte Dritter: Werden nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet und behält der Anwender die Kontrolle über die auf seinem Gerät hinterlegten personenbezogenen Daten Dritter, wird also z.B. das komplette Telefonbuch an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt?

Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden. (§ 7 Abs. 1 KDG). Der Betroffene hat nach den §§ 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 allzu neugierige Applikationen. Manche Anbieter versuchen über die AGB, die Verantwortung für die Einholung einer Einwilligung der Dritten in die Weitergabe ihrer Daten dem Nutzer aufzubürden, was dieser in der Praxis aber nie leisten kann.

Weitere Kriterien

Zu dem erweiterten Kriterienkreis gehören zum einen die Kosten: Der Entscheider sollte prüfen, ob die Nutzung des Produktes idealerweise für den privaten Nutzer kostenfrei und für die nicht-private Nutzung, also z. B. durch eine kirchliche Einrichtung, relativ erschwinglich ist. Bei einer Beurteilung einer Messenger-Lösung ist ferner die Verfügbarkeit des Quellcodes (Open Source) zu berücksichtigen und ggf. positiv zu bewerten. Der Quellcode erlaubt es unabhängigen Experten, einerseits die Korrektheit von Herstellerangaben zu verifizieren und eröffnet diesen andererseits die Möglichkeit, Schwachstellen im Programmcode zu identifizieren.

Darüber hinaus sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt werden. Manche Anbieter untersagen die nicht-private Nutzung, andere untersagen lediglich die kommerzielle Anwendung. Während das Produkt im ersten Fall auch durch ehrenamtliche Non-Profit-Organisationen nicht genutzt werden darf, können diese im zweiten Fall – abhängig von den Formulierungen der AGB – doch von einer bestimmungsgemäßen Nutzung ausgehen. Nicht-privaten ▶

Nutzern wird manchmal eine spezielle „Business-Lösung“ angeboten, die aber oft mit höheren Lizenzkosten verbunden ist als die Privat-Anwendung.

Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren, andere Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

Jeder Entscheider muss sich also ausführlich und umfassend über die Lizenzbedingungen der Produkte informieren. ■

1 Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR--02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 -Verwendung von Transport Layer Security (TLS), Version: 2021--01, Seite 7 ff, Kapitel 3.3

2 Bundesamt für Sicherheit in der Informationstechnik, BSI -Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR--02102-1), Version: 2021-01, Seite 28, Tabelle 3.1

6.4 Technische Empfehlungen zu Windows 10

▶ **Zum Download**
Sechs Arbeitshilfen erhältlich über https://www.kath-datenschutzzentrum-ffm.de/technische-hinweise

Der Arbeitskreis (AK) Technik der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland hat im Jahre 2021 eine sechsteilige Reihe von Arbeitshilfen für Administratoren von Windows-Netzwerken erarbeitet. Die IT-Referenten des KDSZ Frankfurt/M. haben zu dieser Reihe das Dokument „Technische Hinweise für Windows 10 – Webbrowser (Edge)“ beigesteuert und die Erstellung der übrigen Dokumente beratend begleitet.

Mit diesen Dokumenten erhalten Administratoren in kirchlichen Einrichtungen Hinweise über technische Hilfsmittel, um den Einsatz von Windows 10 datensparsam zu gestalten, unabhängig von der datenschutzrechtlichen Frage, unter welchen Voraussetzungen eine Nutzung von Windows 10 datenschutzkonform erfolgen kann.

Technische Hinweise für Windows 10:

1. Manteldokument /datensparsamer Betrieb von Windows 10
2. Windows 10 Installation
3. Entfernung von automatisch installierten Applikationen
4. Windows 10 Suchfunktion
5. Online-Spracherkennung
6. Webbrowser (Edge)

7 Ausblick

Auch das Jahr 2021 war noch durch die Pandemie geprägt. Es war aber schon deutlich zu spüren, dass die durch den Corona-Schock um sich greifende Ohnmacht sich mit zunehmenden Impferfolgen allmählich legte und auch das Kath. Datenschutzzentrum Frankfurt/M. zu einer gewissen Routine zurückkehren konnte. So war es im Berichtsjahr 2021 neben dem Tagesgeschäft, der Bearbeitung datenschutzrechtlicher Fragestellungen und den zahlreichen Beratungsleistungen insbesondere möglich, den Prüfbetrieb wieder verstärkt aufzunehmen und häufigere Schulungen im Datenschutz durchzuführen. Die Vernetzung mit anderen kirchlichen und staatlichen Datenschutzstellen ging ebenfalls mit großen Schritten voran.

Dies alles zeigt, dass für das Kath. Datenschutzzentrum Frankfurt/M. der Schutz der personenbezogenen Daten in den vielen kleinen und großen katholischen Einrichtungen im Zuständigkeitsbereich auch unter widrigen Umständen immer im Mittelpunkt steht und immer stehen wird und die Dienststelle im Herzen Europas nach Jahren der Aufbauarbeit nunmehr ihren festen Platz im Datenschutzgefüge eingenommen hat und angenommen wird.

8 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland

Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28195 Bremen
Diözesandatenschutzbeauftragter:
Andreas Mündelein

Katholisches Datenschutzzentrum (KdöR)

Brackeler Hellweg 144
44309 Dortmund
Diözesandatenschutzbeauftragter:
Steffen Pau

Kath. Datenschutzzentrum Frankfurt/M. KdöR

Haus am Dom, Domplatz 3
60311 Frankfurt am Main
Diözesandatenschutzbeauftragte:
Ursula Becker-Rathmair

Diözesandatenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs

Im Badepark 4
39218 Schönebeck
Diözesandatenschutzbeauftragter:
Matthias Ullrich

Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen

Kapellenstraße 4
80333 München
Diözesandatenschutzbeauftragter:
Jupp Joachimski

Quelle: https://www.katholisches-datenschutzzentrum.de

Kath. Datenschutzzentrum
Frankfurt/M.
Tätigkeitsbericht 2021