Kath. Datenschutzzentrum Frankfurt/M.

Tätigkeitsbericht 2020

2021

2022

2023

2024

2025

2026

Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht 2020

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

Titelmotiv: AdobeStock

Inhaltsverzeichnis

Vorwort 5

1 Aus der Datenschutzaufsicht 7

2 Gründung des Kath. Datenschutzzentrums Frankfurt/M. als KdöR 8
Nepomuk wird Schutzheiliger 13

3 Entwicklung des Datenschutzes 14
3.1 Ausgewählte Rechtsprechung staatlicher Gerichte 14
3.1.1 Neue Regeln für internationalen Datentransfer 14
3.1.2 Regelungen zur Bestandsdatenauskunft verfassungswidrig 14
3.1.3 Einwilligung per Cookie 15
3.2 Wichtige Entscheidungen des Interdiözesanen Datenschutzgerichts 16
3.2.1 Name der Küsterin auf Pfarrei-Homepage 16
3.2.2 Weitergabe von Bewerbungsunterlagen an Bistum 17
3.2.3 Spendenaufruf für Caritas-Sammlung 17
3.2.4 Kein teilweiser Kirchenaustritt durch Datenschutz 17
3.2.5 Juristische Person als Verantwortlicher 18

4 Schwerpunkte der Tätigkeiten im Berichtszeitraum 19
4.1 Datenschutzverletzungen 19
4.1.1 Bettelbrief und verbrannte Erde im Pfarrbüro 21
4.1.2 Schulserver verschlüsselt 21
4.1.3 Bilder auf Abwegen 21
4.2 Beschwerden 22
4.2.1 Virtuelle Klassenzimmer 22
4.2.2 Testung von Krankenhausbeschäftigten 22
4.2.3 Ignorierte Auskunftsersuchen 23
4.3 Anfragen 23
4.3.1 Corona wirft neue Fragen auf 23
4.3.2 Vernichten oder womöglich archivieren? 23
4.3.3 Datenschutz ist Opferschutz 24
4.4 Gerichtsverfahren 24
4.5 Prüfungen 25
4.5.1 Prüfung der Erfassung von Gottesdienstbesuchern 25
4.5.2 Anlassbezogene virtuelle Prüfung einer Kindertagesstätte 30

5 Veranstaltungen und Öffentlichkeitsarbeit 30

6 Meldungen von betrieblichen Datenschutzbeauftragten 31

7 Vernetzung mit anderen Datenschutzaufsichten 31

8 Orientierungshilfen des Kath. Datenschutzzentrums Frankfurt/M. 32
8.1 Online-Meeting-Tools 32
8.2 MAVO-Änderung – Videokonferenzen für Mitarbeitervertretungen 37
8.3 EuGH erkärt Privacy Shield für ungültig 38

9 Mitteilungen aus der Konferenz der Diözesandatenschutzbeauftragten 41
Mitteilung zum „Schrems II"-Urteil des EuGH vom 16. Juli 2020 41

10 Ausblick 43

11 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland 44

Aufsicht unter herausfordernden Bedingungen

Wie in allen Lebensbereichen war auch die Arbeit des Katholischen Datenschutzzentrums Frankfurt/M. im Jahr 2020 von der weltweiten Pandemie geprägt.

Zugute kam dem Datenschutzzentrum Frankfurt/M. in dieser Situation, dass die technische und organisatorische Ausstattung es erlaubte, in den verordneten Lockdown zu gehen und trotzdem arbeitsfähig zu bleiben. Diese für alle schwierige Situation haben die Mitarbeiterinnen und Mitarbeiter in der Datenschutzaufsicht mit großem Einsatz mitgetragen, wofür allen an dieser Stelle ein herzliches Dankeschön gilt.

Ob aus dem Schulbereich, der Kinderbetreuung, der Verkündigung oder der Seelsorge, die Anfragen, Beschwerden oder auch Meldungen von Datenschutzverletzungen brachten ganz neue Fragestellungen. Auch das Katholische Datenschutzzentrum Frankfurt/M. musste sich mit der Abwägung zwischen dem Recht auf körperliche Unversehrtheit und dem Recht auf Bildung, der Abgrenzung zwischen dem Recht auf informationelle Selbstbestimmung und der Religionsausübungsfreiheit, der Spannung zwischen Datenschutz und Elternrecht beschäftigen.

Beinahe zeitgleich mit dem Beginn der Pandemie in Deutschland konnte auch die Datenschutzaufsicht Veränderungen verzeichnen. Am 23. März 2020 veröffentlichte das Hessische Kultusministerium im Staatsanzeiger 13/2020 ab Seite 395 die Errichtung des Katholischen Datenschutzzentrums Frankfurt/M. als Körperschaft des öffentlichen Rechts. Durch die Gründung durch das Bistum Limburg und diese genannte Veröffentlichung entstand das Katholische Datenschutzzentrum Frankfurt/M. als Körperschaft des öffentlichen Rechts. Neben der Selbstständigkeit konnte vor allem die Unabhängigkeit der Behörde gestärkt werden.

Seit Juli 2020 wird der Datenschutz vor neue Herausforderungen gestellt. Denn mit der Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020, dem sogenannten Schrems II-Urteil, sind die Verantwortlichen – aber auch die Aufsichtsbehörden – mit neuen (alten) Fragen des Drittlandtransfers konfrontiert. Die Folgen dieses Urteils waren und sind auch im kirchlichen Bereich spürbar. Hier bleibt nur zu hoffen, dass diese Entscheidung einen Innovationsschub auch im europäischen Raum auslöst, der Abhängigkeiten von sogenannten Global Players zumindest ein Stück weit auflöst.

Manches, das sich das Katholische Datenschutzzentrum Frankfurt/M. für das Jahr 2020 vornahm, konnte coronabedingt nicht durchgeführt werden. Ein großer Teil der mit Dienstreisen verbundenen Veranstaltungen, wie Fortbildungen, Schulungen, auch

Vor-Ort-Prüfungen, konnte nicht wie geplant stattfinden. Aber für vieles war es dennoch möglich, andere passende Formate zu finden. Und es wurde immer wieder festgestellt, dass der Bedarf enorm hoch ist. Auch die Prüfungsformate wurden an die veränderte Situation angepasst, wenngleich diese eine Vor-Ort-Prüfung nicht vollständig ersetzen konnten.

Ursula Becker-Rathmair

Diözesandatenschutzbeauftragte und Leiterin des
Kath. Datenschutzzentrums Frankfurt/M.

1 Aus der Datenschutzaufsicht

Dieses in jeder Hinsicht außergewöhnliche Jahr 2020 brachte auch für das Kath. Datenschutzzentrum Frankfurt/M. höchst unterschiedliche Signale, zum einen in dieser pandemischen Situation immer wieder die Frage letztlich nach dem Selbstverständnis des Datenschutzes, wie die nach der vorrangigen Berücksichtigung des Gesundheitsschutzes oder der Bildungsinteressen, zum anderen aber auch das bereits im Vorwort erwähnte Urteil des Europäischen Gerichtshofs zum internationalen Datentransfer, das dem Datenschutz ganz erheblich mehr Bedeutung zumisst. In diesem Spannungsfeld musste auch die Datenschutzaufsicht ihre Arbeit fortsetzen und Antworten auf Fragen geben, die sich bis dahin noch niemand stellte.

In dieser für alle schwierigen Situation hat das Datenschutzzentrum Frankfurt/M. seine Aufbauarbeit fortgesetzt und neben einer weiteren Verwaltungskraft auch einen IT-Referenten gewonnen und in ihre Tätigkeiten einführen können. So kann die bislang gebundene externe Kompetenz schrittweise durch interne Kräfte ersetzt werden.

Diese Corona-Situation veränderte aber auch die Arbeitsweise der Datenschutzaufsicht in einem nicht zu vernachlässigenden Umfang. Die Menge aufgelaufener Anfragen bekam zum Teil einen anderen Charakter und war ebenfalls „pandemisch geprägt“. Deutlich wurde zudem, dass – gerade in dieser Pandemie – die Frage nach dem Datenschutz, das heißt nach dem Schutz des Einzelnen in seinem Recht auf informationelle Selbstbestimmung, immer drängender wurde. Das Kath. Datenschutzzentrum Frankfurt/M. hat auch im Berichtszeitraum nicht nachgelassen, den Belangen des Datenschutzes Geltung zu verschaffen, sei es durch stetige Beratung, Bearbeitung der Beschwerden oder auch die Verhängung von Sanktionen, soweit dies notwendig und unumgänglich war.

2 Gründung des Kath. Datenschutzzentrums Frankfurt/M. als KdöR

Die öffentlich-rechtliche Vereinbarung aus dem Jahre 2017 wurde jeweils in den Amtsblättern der sieben (Erz-)Bistümer veröffentlicht – exemplarisch: Amtsblatt des Bistums Limburg Nr. 11/2017, S. 206 ff. (Nr. 133)]

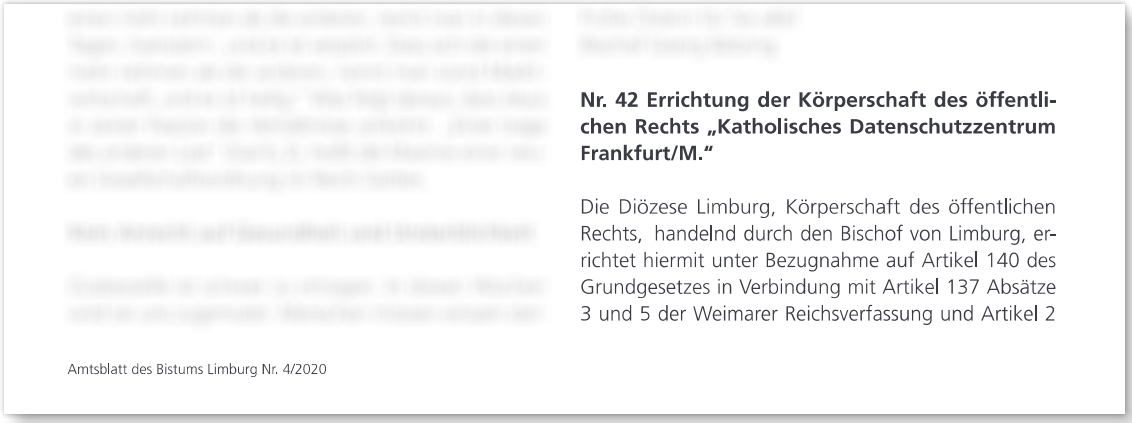
Bereits im Jahr 2016 fanden sich die sieben (Erz-)Bistümer der Region Mitte-Süd-West zusammen und gründeten die „Gemeinsame Datenschutzstelle für die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier“, die die aufsichtliche Tätigkeit ausüben soll. Hierzu schlossen sie im Jahr 2017 eine öffentlich-rechtliche Vereinbarung über die Errichtung der neuen Datenschutzbehörde.

Sehr bald nach Aufnahme der Tätigkeit der Diözesandatenschutzbeauftragten im Jahr 2018 wurde jedoch deutlich, dass eine größere Unabhängigkeit der Datenschutzaufsicht notwendig und von den (Erz-)Bistümern gewollt war. Daher nahmen das Kommissariat der Katholischen Bischöfe im Lande Hessen und das für den Standort Frankfurt am Main zuständige Belegenheitsbistum Limburg noch im Frühjahr 2018 Verhandlungen mit dem Hessischen Kultusministerium auf mit dem Ziel, eine Körperschaft des öffentlichen Rechts (KdöR) zu gründen. Da das Kath. Datenschutzzentrum Frankfurt/M. auch in den Bundesländern Baden-Württemberg, Rheinland-Pfalz, Saarland und im thüringischen Teil der Rhön Aufsicht ausüben können soll, wurden auch die dortigen zuständigen staatlichen Stellen in die Verhandlungen einbezogen. Nach einem langen Verhandlungsprozess – auch unter Einbeziehung der Expertise des Instituts für Staatskirchenrecht und der übrigen beteiligten Katholischen Büros – erfolgte im März 2020 neben der Gründung des Datenschutzzentrums Frankfurt/M. durch das Bistum Limburg im Juni 2019 und der Unterzeichnung und Veröffentlichung der Satzung durch die beteiligten (Erz-)Bistümer die Veröffentlichung der Gründungsurkunde und der Satzung durch das Hessische Kultusministerium im Hessischen Staatsanzeiger. An dieser Stelle sei allen, die an der Gründung des Kath. Datenschutzzentrums Frankfurt/M. beteiligt waren, sehr herzlich gedankt.

> „An dieser Stelle sei allen, die an der Gründung des Kath. Datenschutzzentrums Frankfurt/M. beteiligt waren, sehr herzlich gedankt.“

Die Körperschaft war gegründet und das Datenschutzzentrum Frankfurt/M. konnte seine Arbeit unter diesen veränderten Vorzeichen fortsetzen. Mit dieser Gründung war auch die organisatorische Selbstständigkeit erreicht.

Veröffentlichung der Gründungsurkunde zur Errichtung der Körperschaft des öffentlichen Rechts „Katholisches Datenschutzzentrum Frankfurt/M.“



Nr. 42 Errichtung der Körperschaft des öffentlichen Rechts „Katholisches Datenschutzzentrum Frankfurt/M.“

Die Diözese Limburg, Körperschaft des öffentlichen Rechts, handelnd durch den Bischof von Limburg, errichtet hiermit unter Bezugnahme auf Artikel 140 des Grundgesetzes in Verbindung mit Artikel 137 Absätze 3 und 5 der Weimarer Reichsverfassung und Artikel 2

Amtsblatt des Bistums Limburg Nr. 4/2020

aus: Amtsblatt des Bistums Limburg Nr. 4/2020, S. 46 f. (Nr. 42)

Absatz 2 Satz 1 des Vertrages zur Ergänzung des Vertrages des Landes Hessen mit den Katholischen Bistümern in Hessen vom 29. März 1974 die Körperschaft des öffentlichen Rechts

„Katholisches Datenschutzzentrum Frankfurt/M."

nach Maßgabe der Satzung des Katholischen Datenschutzzentrums Frankfurt/M., die Bestandteil dieser Urkunde ist.

Limburg, 27. Juni 2019 + Dr. Georg Bätzing
Az. 555B/60419/19/04/4 Bischof von Limburg

Nr. 43 Satzung des Katholischen Datenschutzzentrums Frankfurt/M. der/des gemeinsamen Diözesandatenschutzbeauftragten für die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier

Präambel

Das verfassungsrechtlich garantierte Recht der Kirche, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten, umfasst auch das Recht zur autonomen Regelung des Datenschutzes im kirchlichen Bereich, wie es in Art. 91 Datenschutzgrundverordnung (DSGVO) verankert ist. Die deutschen (Erz-)Bischöfe möchten im Rahmen ihres kirchlichen Selbstbestimmungsrechtes ein hohes Datenschutzniveau garantieren. Im Hinblick auf die EU-Datenschutz-Grundverordnung, welche am 25.05.2018 in Kraft trat, soll der kirchliche Datenschutz der (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier neu geordnet werden, um den kirchlichen Datenschutz dem staatlichen Recht gegenüber wirkungsgleich gewährleisten zu können. Damit wird die Unabhängigkeit der Datenschutzbeauftragten garantiert und der kirchliche Datenschutz gegenüber dem staatlichen Recht auf gleichem Niveau ausgestaltet.

Dementsprechend haben die (Erz-) Bischöfe der (Erz-) Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier für ihren Zuständigkeitsbereich umfassende datenschutzrechtliche Regelungen getroffen und sich darauf verständigt, die Datenschutzaufsicht in einem überdiözesanen Katholisches Datenschutzzentrum Frankfurt/M. zu organisieren und in Form einer Körperschaft des öffentlichen Rechts zu errichten. Die Belegenheitsdiözese Limburg wird mit der Errichtung dieser Körperschaft betraut.

§ 1 Rechtsform, Name, Sitz, Rechtsanwendung

(1) Das Katholische Datenschutzzentrum ist eine rechtlich selbstständige kirchliche Einrichtung in der Rechtsform einer Körperschaft des öffentlichen Rechts (KdöR) gemäß Artikel 140 Grundgesetz in Verbindung mit Artikel 137 Absatz 5 Weimarer Reichsverfassung.

(2) Es führt den Namen „Katholisches Datenschutzzentrum Frankfurt/M." und ein eigenes Siegel mit der Umschrift „Kath. Datenschutzzentrum Frankfurt/M. KdöR".

(3) Sitz des Katholischen Datenschutzzentrums ist Frankfurt am Main.

(4) Für das Katholische Datenschutzzentrum Frankfurt/M. gilt die Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse in ihrer jeweils geltenden, vom Bischof der für den Sitz des Datenschutzzentrums zuständigen Diözese Limburg in Kraft gesetzten Fassung.

(5) Für das Katholische Datenschutzzentrum Frankfurt/M. gilt das diözesane Datenschutzrecht der Belegenheitsdiözese. Es wendet in den einzelnen Diözesen das jeweilige diözesane Datenschutzrecht, insbesondere das Gesetz über den kirchlichen Datenschutz (im Folgenden: KDG) in der jeweils gültigen Fassung an.

§ 2 Mitgliedschaft

(1) Die Körperschaft wird vom Bistum Limburg errichtet. Mit der Unterzeichnung erklären die in der Präambel genannten (Erz-)Diözesen ihre Mitgliedschaft in der neuen Körperschaft.

(2) Weitere (Erz-) Diözesen können der Körperschaft unter den in dieser Satzung festgelegten Voraussetzungen als Mitglieder beitreten.

(3) Mitglieder können unter den in dieser Satzung festgelegten Voraussetzungen aus der Körperschaft austreten. Ein Austritt ist nur zulässig, wenn die diözesanen Aufsichtsstrukturen ein gleichwertiges Schutzniveau garantieren.

§ 3 Zweckbestimmung

(1) Zweck des Katholischen Datenschutzzentrums Frankfurt/M. ist die Wahrnehmung der kirchli-

Veröffentlichung der Satzung des Katholischen Datenschutzzentrums Frankfurt/M. der/des gemeinsamen Diözesandatenschutzbeauftragten für die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier

Amtsblatt des Erzbistums Freiburg Nr. 14/2020, S. 331 ff. (Nr. 224); Amtsblatt des Bistums Fulda Stück III/2020, S. 43 ff. (Nr. 37); Amtsblatt des Bistums Limburg Nr. 4/2020, S. 47 ff. (Nr. 43); Amtsblatt des Bistums Mainz Nr. 5/2020, S. 45 ff. (Nr. 32); Amtsblatt des Bistums Rottenburg-Stuttgart Nr. 6/2020, S. 163 ff. (Nr. 1953); Amtsblatt des Bistums Speyer Nr. 7/2019, S. 1271 ff. (Nr. 326); Amtsblatt des Bistums Trier Nr. 5/2020, S. 121 ff. (Nr. 93)

chen Datenschutzaufsicht auf der Grundlage der für die Mitgliedsdiözesen geltenden kirchlichen Datenschutzregelungen, insbesondere des Gesetzes über den kirchlichen Datenschutz (KDG) in der für die Mitgliedsdiözesen jeweils geltenden Fassung. Mit der Wahrnehmung der kirchlichen Datenschutzaufsicht wird zugleich sichergestellt, dass bei den kirchlichen verantwortlichen Stellen im Sinne des KDG ausreichende Maßnahmen zum Datenschutz getroffen werden.

(2) Die Datenschutzaufsicht erstreckt sich auf die Bereiche der Mitgliedsdiözesen gemäß § 3 KDG.

(3) Das Katholische Datenschutzzentrum Frankfurt/M. ist Anstellungsträger der/des von den Mitgliedsdiözesen nach § 42 Absatz 1 KDG bestellten gemeinsamen Diözesandatenschutzbeauftragten und der dort Mitarbeitenden.

§ 4 Organe

Organe des Katholischen Datenschutzzentrums Frankfurt/M. sind
- die/der gemeinsame Diözesandatenschutzbeauftragte und
- der Verwaltungsrat.

§ 5 Gemeinsame/r Diözesandatenschutzbeauftragte/r

(1) Gesetzliche Vertretung des Katholischen Datenschutzzentrums Frankfurt/M. ist die/der von den (Erz-) Bischöfen der Mitgliedsdiözesen bestellte gemeinsame Diözesandatenschutzbeauftragte Diese Person ist für die Mitgliedsdiözesen und ggf. weiteren kirchlichen Rechtsträger, die dem Datenschutzzentrum aufgrund besonderer rechtlicher Regelungen unterstellt werden, die/der gemeinsame Diözesandatenschutzbeauftragte gemäß den jeweils geltenden Bestimmungen des KDG. Sie vertritt das Katholische Datenschutzzentrum Frankfurt/M. gerichtlich und außergerichtlich und führt dessen Geschäfte. Vertreter/in ist die/der jeweilige Stellvertreter/in des/der gemeinsamen Diözesandatenschutzbeauftragten. Die/Der gemeinsame Diözesandatenschutzbeauftragte und die/der Stellvertreter/in sind jeweils einzeln zur Vertretung berechtigt. Entsprechende Erklärungen sind unter Bedrückung des Siegels des Katholischen Datenschutzzentrums Frankfurt/M. abzugeben. Im Falle von Beschlüssen nach § 7 j) vertritt die/der Vorsitzende bzw. ihr/sein Stellvertreter das Datenschutzzentrum.

(2) Die Rechtsstellung, der Rahmen für die Dauer der Bestellung und die Aufgaben der/des gemeinsamen Diözesandatenschutzbeauftragten ergeben sich aus dem KDG in der für den Sitz des Katholischen Datenschutzzentrums Frankfurt/M. jeweils geltenden Fassung.

(3) Zur Erledigung ihrer/seiner Aufgaben steht der/dem gemeinsamen Diözesandatenschutzbeauftragten eine Geschäftsstelle mit der erforderlichen Personal- und Sachausstattung zur Seite. Der Umfang der Ausstattung ist nach Maßgabe des § 43 Absatz 4 KDG festzulegen und im Haushalts- oder Wirtschaftsplan des Datenschutzzentrums zu veröffentlichen.

§ 6 Zusammensetzung des Verwaltungsrates, Vertretung

(1) Die (Erz-) Bischöfe der Mitgliedsdiözesen bilden den Verwaltungsrat des Katholischen Datenschutzzentrums Frankfurt/M. Sie können eine von ihnen bevollmächtigte Vertretung in den Verwaltungsrat entsenden. Im Falle der Sedisvakanz werden die Aufgaben gemäß den kirchenrechtlichen Bestimmungen wahrgenommen.

(2) Wird das Katholische Datenschutzzentrum Frankfurt/M. um weitere Mitgliedsdiözesen erweitert oder scheiden Mitgliedsdiözesen aus, ändert sich die Zusammensetzung des Verwaltungsrates entsprechend. Jede Mitgliedsdiözese hat einen Sitz im Verwaltungsrat.

(3) Der Verwaltungsrat wählt für eine Amtszeit von jeweils fünf Jahren aus seiner Mitte eine/n Vorsitzende/n und eine/n stellvertretende/n Vorsitzende/n. Wiederwahl ist zulässig.

(4) Der Verwaltungsrat kann auf Vorschlag der/des Vorsitzenden eine Person mit der Geschäftsführung des Verwaltungsrates beauftragen, der insbesondere die Vor- und Nachbereitung der Sitzungen (einschl. Anfertigung der Niederschrift) übertragen werden kann. Diese Person muss nicht Mitglied des Verwaltungsrates sein.

(5) Soweit der Verwaltungsrat nicht im Einzelfall etwas anderes beschließt, nimmt die/der gemeinsame Diözesandatenschutzbeauftragte, im Verhinderungsfall seine Vertretung, an den Sitzungen des Verwaltungsrates beratend teil.

§ 7 Aufgaben des Verwaltungsrates

(1) Unter Wahrung der den (Erz-) Bischöfen kirchenrechtlich vorbehaltenen Zuständigkeiten und unter Wahrung der in § 43 Abs. 1 KDG festgelegten Unabhängigkeit der/des gemeinsamen Diözesandatenschutzbeauftragten nimmt der Verwaltungsrat die Rechtsaufsicht wahr und es kommen ihm insbesondere die nachfolgend genannten Aufgaben zu:
   a) Entscheidung über die der/dem Diözesandatenschutzbeauftragten zukommende Personal- und Sachausstattung nach Maßgabe der bestehenden rechtlichen Verpflichtungen und der hierfür durch die Mitgliedsdiözesen zur Verfügung gestellten Mittel,
   b) Entgegennahme des gemäß den Vorgaben des KDG regelmäßig zu erstattenden Berichtes der/des gemeinsamen Diözesandatenschutzbeauftragten,
   c) Erlass einer Geschäftsordnung für den Verwaltungsrat,
   d) Beratung vor der Einstellung von Mitarbeitenden,
   e) Entscheidungsvorschlag zur Bestellung der/des gemeinsamen Diözesandatenschutzbeauftragten,
   f) Entscheidungsvorschlag zur Herstellung des Einvernehmens für die Bestellung der Vertretung der/des gemeinsamen Diözesandatenschutzbeauftragten,
   g) Entscheidungsvorschlag zum Widerruf der Bestellung zur/zum gemeinsamen Diözesandatenschutzbeauftragten,
   h) Entscheidung über die Übernahme der Datenschutzaufsicht über sonstige, nicht über die Mitgliedschaft der (Erz-)Diözesen erfasste kirchliche Rechtsträger,
   i) Entscheidung über Satzungsänderungen des Katholischen Datenschutzzentrums Frankfurt/M,
   j) Entscheidung bei allen Rechtsgeschäften und Rechtsstreitigkeiten gegenüber dem gemeinsamen Datenschutzbeauftragten.

(2) Beschlüsse zu Buchstaben e) bis j) müssen mit einer Mehrheit von zwei Dritteln der Stimmen aller Verwaltungsratsmitglieder erfolgen. Enthaltungen sind nicht zulässig.

(3) Die/Der Vorsitzende des Verwaltungsrates ist Dienstvorgesetzte/r der/des Diözesandatenschutzbeauftragten, wobei deren/dessen Unabhängigkeit nach den jeweils geltenden Regelungen des KDG zu wahren ist. Entsprechendes gilt für die Stellvertretung in Ausübung der Vertretung.

§ 8 Arbeitsweise des Verwaltungsrates

(1) Der Verwaltungsrat ist beschlussfähig, wenn wenigstens die Hälfte seiner Mitglieder, darunter die/der Vorsitzende oder die/der stellvertretende Vorsitzende, anwesend sind.

(2) Sitzungen des Verwaltungsrates finden mindestens einmal jährlich, darüber hinaus nach Bedarf, statt. Zu diesen Sitzungen ist in Textform (Brief, Telefax, E-Mail) mit einer Frist von mindestens vier Wochen unter Angabe der Beratungspunkte einzuladen. Der Verwaltungsrat ist von der/dem Vorsitzenden einzuberufen, wenn es mindestens zwei Mitglieder unter Angabe der Beratungspunkte schriftlich verlangen.

(3) Soweit in dieser Satzung nicht ausdrücklich etwas anderes bestimmt ist, entscheidet der Verwaltungsrat mit der Mehrheit der Stimmen der anwesenden Mitglieder. Der Verwaltungsrat kann Beschlüsse im Einzelfall auch im schriftlichen oder im elektronischen Umlaufverfahren fassen, wenn alle Verwaltungsratsmitglieder bzw. Vertreter dieser Form der Beschlussfassung zustimmen.

(4) Über die Sitzungen des Verwaltungsrates ist eine Niederschrift anzufertigen.

(5) Die Mitglieder des Verwaltungsrates sind ohne besondere Vergütung tätig.

(6) Weitere Einzelheiten zur Arbeitsweise des Verwaltungsrates können in einer Geschäftsordnung geregelt werden.

§ 9 Beitritt weiterer Mitgliedsdiözesen

Weitere (Erz-) Diözesen (Körperschaften des öffentlichen Rechts) können der Körperschaft als Mitglieder beitreten, wenn der Verwaltungsrat dem Beitrittsgesuch mit den Stimmen aller seiner Mitglieder zustimmt. Die näheren Einzelheiten sind in einer Beitrittsvereinbarung zu regeln.

§ 10 Austritt von Mitgliedsdiözesen

Mitgliedsdiözesen können mit einer Frist von einem Jahr zum Jahresende ihren Austritt aus der Körperschaft er-

klären. Die näheren Einzelheiten sind in einer Austrittsvereinbarung mit den verbleibenden Mitgliedsdiözesen zu regeln.

§ 11 Auflösung der Körperschaft

Über die Auflösung der Körperschaft entscheidet der Verwaltungsrat nach Anhörung der/des Diözesandatenschutzbeauftragten. Die Auflösung kann nur mit den Stimmen aller Mitglieder des Verwaltungsrates beschlossen werden.

§ 12 Vermögensanfall

Bei Auflösung der Körperschaft fällt das vorhandene Vermögen zu gleichen Teilen an die Mitglieder der Körperschaft.

§ 13 Inkrafttreten/Ausfertigungen

Diese Satzung tritt am Tage nach der Unterzeichnung durch alle beteiligten (Erz-)Bischöfe in Kraft. Jede (Erz-)Diözese erhält eine Ausfertigung. Sie ist in den Amtsblättern der beteiligten (Erz-)Diözesen bekannt zu machen.

Limburg, 27. Juni 2019 Az. 555B/60419/19/04/4	+ Dr. Georg Bätzing Bischof von Limburg
Freiburg, 8. Juli 2019	+ Stephan Burger Erzbischof von Freiburg
Fulda, 11. Juli 2019	+ Dr. Michael Gerber Bischof von Fulda
Mainz, 13 Juli 2019	+ Prof. Dr. Peter Kohlgraf Bischof von Mainz
Rottenburg-Stuttgart, 20. Juli 2019	+ Dr. Gebhard Fürst Bischof von Rottenburg-Stuttgart
Speyer, 5. August 2019	+ Dr. Karl-Heinz Wiesemann Bischof von Speyer
Trier, 9. August 2019	+ Dr. Stephan Ackermann Bischof von Trier

Nepomuk wird Schutzheiliger

Mit dieser Körperschaftsgründung verbunden war auch die Berechtigung zur Siegelführung, von der das Kath. Datenschutzzentrum Frankfurt/M. Gebrauch gemacht hat. In dieses Siegel Eingang gefunden hat der Schutzpatron des Datenschutzzentrums Frankfurt/M. – der Heilige Johann Nepomuk. Dieser Heilige wurde zum Schutzheiligen gewählt, da er in verschiedener Weise mit dem Datenschutz im Weiteren verbunden ist.

Geboren wurde Johann (von) Pomuk, der als sogenannter Brückenheiliger etliche Brücken ziert, irgendwann zwischen 1340 und 1350 in dem Ort Pomuk in der Nähe von Pilsen. Die bekannteste Darstellung ist wahrscheinlich die in Prag auf der Brücke über die Moldau. Die Legende des Heiligen besagt, dass er sich nach dem Studium der Theologie und der Juristerei, in beiden Disziplinen promovierte er, zunächst den Ruf eines gern gehörten Predigers erwarb, der sich insbesondere für die Belange der armen Bevölkerung einsetzte. Vom damaligen Prager Erzbischof Johann von Jenstein zum Generalvikar und Domkapitular berufen, zog er sich den Unmut von König Wenzel zu, da er von diesem angebotene Vergünstigungen ausschlug und vor allem keine als Beichtvater der Königin erlangte Informationen aus der Beichte preisgab. Dies erzürnte den König derart, dass er Johann Nepomuk foltern und anschließend mit einem Keil im Mund in der Moldau ertränken ließ. Die Zunge des zunächst an einem anderen Ort beigesetzten und sodann in den Prager Dom überführten Leichnams blieb unverwest und wird seitdem in einem gesonderten Reliquiar aufbewahrt.

Die Tatsache, dass Johannes Nepomuk auch unter grausamer Folter das Beichtgeheimnis nicht preisgab, bedingt, dass er gelegentlich mit einem Finger an den Lippen dargestellt wird, die Darstellung, die auch das Kath. Datenschutzzentrum Frankfurt/M. für sein Siegel wählte.

Möge dieser Schutzheilige das Kath. Datenschutzzentrum Frankfurt/M. und seine Arbeit begleiten und hier den Blick dafür öffnen, wann man reden und wann man vielleicht besser schweigen sollte.

3 Entwicklung des Datenschutzes

3.1 Ausgewählte Rechtsprechung staatlicher Gerichte

3.1.1 Neue Regeln für internationalen Datentransfer

Mit der in diesem Tätigkeitsbericht bereits genannten Schrems II-Entscheidung hat der Europäische Gerichtshof (EuGH) den sogenannten EU-US-Privacy-Shield für unwirksam erklärt (Urteil vom 16. Juli 2020, Az.: C-311/18). Das Abkommen war bis zu diesem Zeitpunkt Grundlage des Datentransfers zwischen der EU und den USA. Hintergrund ist, dass jede Übermittlung von personenbezogenen Daten in Länder außerhalb der EU einer besonderen rechtlichen Absicherung bedarf. Der EuGH hat im Sommer 2020 jedoch entschieden, dass das Abkommen kein der EU-Datenschutzgrundverordnung (DSGVO) vergleichbares Datenschutzniveau bietet. Das Gericht verweist in seiner Entscheidung darauf, dass Zugriffe der US-Sicherheitsbehörden auf diese in die USA übermittelten Daten von EU-Bürgern dennoch möglich seien. Klar ist, dass seit diesem Urteil eine Berufung auf den Privacy Shield mangels Übergangsfrist nicht mehr zulässig ist. Grundsätzlich möglich sind nach der Entscheidung aber noch Datentransfers auf Basis von Standardvertragsklauseln. Wie mit diesen ein angemessenes Datenschutzniveau sichergestellt werden kann, mit welchen Maßnahmen und Garantien, ließ der EuGH jedoch offen.

Der konkrete Umgang mit dem Schrems II-Urteil stellt alle noch vor große Herausforderungen. Verhandlungen über ein drittes Abkommen beziehungsweise neue Standardvertragsklauseln laufen bereits seit einiger Zeit im Hintergrund.

Eine Mitteilung der Konferenz der Diözesandatenschutzbeauftragten zu diesem wichtigen Urteil des EuGH findet sich weiter hinten im Tätigkeitsbericht (siehe unter Ziffer 9). Das Kath. Datenschutzzentrum Frankfurt/M. hat dazu auch eine Orientierungshilfe auf seiner Homepage veröffentlicht, die ebenfalls in diesem Bericht abgedruckt ist (siehe unter Ziffer 8).

3.1.2 Regelungen zur Bestandsdatenauskunft verfassungswidrig

Ebenfalls im Jahr 2020 hat das Bundesverfassungsgericht (BVerfG) eine wichtige Entscheidung zur Bestandsdatenauskunft gefällt (Beschluss vom 27. Mai 2020, Az.: 1 BvR 1873/13, 1 BvR 2618/13). Mit seinem Beschluss hat es § 113 des Telekommunikationsgesetzes (TKG) und mehrere Fachgesetze des Bundes, die die manuelle Bestandsdatenauskunft regeln, für verfassungswidrig erklärt, weil diese die Inhaber von Telefon- und Internetanschlüssen in ihren Grundrechten auf informationelle Selbstbestimmung sowie auf Wahrung des Telekommunikationsgeheimnisses, Art. 10 Abs. 1 des Grundgesetzes (GG) verletzten.

Die manuelle Bestandsdatenauskunft ermöglicht es Sicherheitsbehörden, von Telekommunikationsunternehmen Auskunft insbesondere über den Anschlussinhaber eines Telefonanschlusses oder einer zu einem bestimmten Zeitpunkt zugewiesenen IP-Adresse zu erlangen. Mitgeteilt werden personenbezogene Daten der Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen (Bestandsdaten). Nicht mitgeteilt werden dagegen Daten, die sich auf die Nutzung von Telekommunikationsdiensten (Verkehrsdaten) oder den Inhalt von Kommunikationsvorgängen beziehen.

Die Erteilung einer Auskunft über Bestandsdaten sei grundsätzlich verfassungsrechtlich zulässig. Der Gesetzgeber müsse aber nach dem Bild einer Doppeltür sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils die Verhältnismäßigkeit regelnde Rechtsgrundlagen schaffen, so das BVerfG. Übermittlungs- und Abrufregelungen müssten die Verwendungszwecke der Daten hinreichend begrenzen, indem sie insbesondere tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz vorsehen.

Der Senat hat klargestellt, dass den allgemeinen Befugnissen zur Übermittlung und zum Abruf von Bestandsdaten trotz ihres eher mäßigen Eingriffsgewichts für die Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht zugrunde liegen müssen. Findet eine Zuordnung dynamischer IP-Adressen statt, müsse diese im Hinblick auf ihr erhöhtes Eingriffsgewicht darüber hinaus auch dem Schutz von Rechtsgütern von zumindest hervorgehobenem Gewicht dienen. Bleiben die Eingriffsschwellen im Bereich der Gefahrenabwehr oder der nachrichtendienstlichen Tätigkeit hinter dem Erfordernis einer konkreten Gefahr zurück, seien im Gegenzug erhöhte Anforderungen an das Gewicht der zu schützenden Rechtsgüter vorzusehen. Diese Voraussetzungen seien von den angegriffenen Vorschriften nicht erfüllt worden.

Unzulässig ist es dagegen, so die Richter in ihrer Begründung, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt.

3.1.3 Einwilligung per Cookie

Der Bundesgerichtshof (BGH) hat in seinem viel beachteten Planet49-Urteil entschieden, dass eine ausdrückliche Einwilligung zum Setzen von Cookies erforderlich ist (Urteil vom 28. Mai 2020, Az.: I ZR 7/16). In dem zugrunde liegenden Sachverhalt hatte die Firma Planet49 ein Gewinnspiel im Internet veranstaltet, bei dem das Häkchen bei der Einwil-

> Der Bundesgerichtshof hat in seinem viel beachteten Planet49-Urteil entschieden, dass eine ausdrückliche Einwilligung zum Setzen von Cookies erforderlich ist.

ligung in Werbung bereits gesetzt war (sogenanntes Opt-out-Verfahren). Nach diesem Richterspruch ist nunmehr beim Setzen von Cookies – um beispielsweise Nutzerprofile zu Werbezwecken zu erstellen – zwingend eine Einwilligung des Users einzuholen und dieser vorher transparent zu informieren. Ausnahmen davon soll es nur für sogenannte funktionale Cookies geben.

Das höchste deutsche Zivilgericht hatte die Frage bereits vorher dem EuGH vorgelegt und dieser hatte ebenfalls eine aktive Einwilligung nach der DSGVO gefordert – das Opt-in-Verfahren. Über das Ersuchen des BGH um die Auslegung des Unionsrechts über den Schutz der Privatsphäre in der elektronischen Kommunikation und dem daraufhin erfolgten Urteil des EuGH (Urteil vom 1. Oktober 2019, Az.: C-673/17) berichtete das Kath. Datenschutzzentrum Frankfurt/M. in seinem Tätigkeitsbericht 2019.

3.2 Wichtige Entscheidungen des Interdiözesanen Datenschutzgerichts

3.2.1 Name der Küsterin auf Pfarrei-Homepage

Im ersten im Jahr 2020 veröffentlichten Rechtsstreit hatte sich das Interdiözesane Datenschutzgericht (IDSG) mit dem Antrag einer Küsterin zu beschäftigen, die sich gegen die Nennung ihres Namens auf der Internetseite der Pfarrei wandte. Dort war ihre personalisierte dienstliche E-Mail-Adresse vorname.nachname@xxx.de aufgeführt. Sie forderte dagegen die Einrichtung einer Funktionsadresse für sie im Sinne von kuesterin@xxx.de.

Die Klage der Küsterin blieb ebenso erfolglos wie ihre zuvor erhobene Beschwerde.

Nach der Entscheidung des Gerichts verletzt die Veröffentlichung der mit dem Namen und Vornamen gebildeten dienstlichen E-Mail-Anschrift eines Mitarbeiters mit Außenkontakten wie im vorliegenden Fall auf der Homepage der Pfarrgemeinde keine kirchlichen Datenschutzrechte (Beschluss vom 22. April 2020, Az.: IDSG 03/2019).

Die Pfarrgemeinde habe ein legitimes Interesse daran, dass die bei Taufen und Trauungen betroffenen Gläubigen eine unmittelbare Kommunikationsmöglichkeit mit der Küsterin hätten, um die Vorbereitung, Durchführung und Nachbereitung dieser Feiern besprechen zu können. Zudem mache die namentliche Benennung der Küsterin, so das IDSG in seiner Begründung, „die kirchliche Dienstleistungsstruktur transparent“ und senke „die Zugangsschwellen für die betroffenen Gläubigen“. Nach alledem sei der Eingriff in das Recht der Antragstellerin auf informationelle Selbstbestimmung verhältnismäßig.

3.2.2 Weitergabe von Bewerbungsunterlagen an Bistum

In einer weiteren Entscheidung ging es um die Weiterleitung von Unterlagen eines Bewerbers durch den Generalvikar an dessen früheres Bistum, obwohl das Schreiben den Hinweis auf eine diskrete Behandlung enthielt (Beschluss vom 5. Mai 2020, Az.: IDSG 02/2018).

Der Antragsteller war von der römisch-katholischen in die alt-katholische Kirche übergetreten und war dort als Priester tätig. Er fragte beim Generalvikar an, ob eine Rückkehr und ein Einsatz als Priester möglich sei. Dieser leitete die Anfrage an den früheren Arbeitgeber weiter, um weitere Informationen zu erlangen. Die Richter sahen darin eine unzulässige Verarbeitung personenbezogener Daten.

Die Anfrage hätte der Generalvikar selbst beantworten können, ohne das Bistum zu involvieren, so das IDSG. Es konnte keinen legitimen Zweck in der Weitergabe der personenbezogenen Daten des Antragstellers an das Bistum erkennen – „die Befriedigung einer gewissen Neugier über das Vorleben des Antragstellers ist kein solcher", schreibt das Gericht in seinem Beschluss.

3.2.3 Spendenaufruf für Caritas-Sammlung

Am 18. Juni 2020 hat das Gericht entschieden, dass eine Pfarrei, die in ihrer Meldedatenbank gespeicherte Namen und Anschriften der Pfarrangehörigen zu Spendenaufrufen für Caritas-Sammlungen nutzt – zu deren Durchführung die Pfarreien durch bischöfliche Anordnung verpflichtet sind – und diese in die Briefkästen der Pfarrangehörigen einwerfen lässt, eine nach dem kirchlichen Datenschutzrecht zulässige Verarbeitung personenbezogener Daten vornimmt (Az.: IDSG 02/2019).

Die genannte bischöfliche Anordnung als Rechtsgrundlage lautete im Amtsblatt unter anderem zu einer Caritas-Herbstsammlung: „Die Haus- bzw. Briefsammlung ist in allen Pfarreien durchzuführen."

3.2.4 Kein teilweiser Kirchenaustritt durch Datenschutz

Im Berichtszeitraum hatte sich das IDSG auch mit dem Fall eines Kirchenaustritts zu beschäftigen (Beschluss vom 9. Dezember 2020, Az.: IDSG 05/2019). Der Antragsteller erklärte auf dem Standesamt seinen Austritt aus der römisch-katholischen Kirche als Körperschaft des öffentlichen Rechts. Den daraufhin erfolgten Eintrag im Taufbuch („Austritt am … in XX.") wollte er korrigiert haben in: „Austritt aus der Katholischen Kirche, Körperschaft des öffentlichen Rechts, am … in XX". Der Eintrag ohne „Körperschaft des öffentlichen Rechts" sei unrichtig im Sinne des § 18 KDG. Dieser Begründung folgten die Richter nicht.

Der Eintrag sei formell richtig erfolgt. Ob er auch inhaltlich richtig ist, sei im datenschutzrechtlichen Verfahren nicht zu überprüfen.

Der Antragsteller habe damit im Ergebnis erreichen wollen, dass sich sein Austritt auf das Ausscheiden aus der öffentlich-rechtlichen Körperschaft beschränkt und keine innerkirchlichen Wirkungen hat. Eine statusrechtliche Prüfung der Kirchenmitgliedschaft liege jedoch außerhalb seiner Kompetenz, so das IDSG. Gegen diesen Beschluss wurde Rechtsmittel zum Datenschutzgericht der Deutschen Bischofskonferenz eingelegt (Az.: DSG-DBK 05/2020).

3.2.5 Juristische Person als Verantwortlicher

Mitten in der Adventszeit 2020 hat das Datenschutzgericht schließlich noch eine wichtige Entscheidung verkündet (Beschluss vom 14. Dezember 2020, Az.: IDSG 01/2020): Werden personenbezogene Daten im Bereich einer juristischen Person verarbeitet, ist grundsätzlich die juristische Person als Rechtsträger der betroffenen Einrichtung oder des betroffenen Unternehmens Verantwortlicher und nicht die jeweils handelnde natürliche Person.

Auf Mitarbeiter des Rechtsträgers könnte nach ausdrücklicher Aussage der Richter in dem Beschluss ausnahmsweise nur abzustellen sein, „wenn ein Mitarbeiter entgegen der Weisung des Rechtsträgers mit der Datenverarbeitung eigene Zwecke verfolgt (Mitarbeiterexzess) oder wenn ein Mitarbeiter aufgrund seiner besonderen rechtlichen Stellung unabhängig von Weisungen des Rechtsträgers – etwa als Betriebsrat, Mitarbeitervertretung oder Personalrat – ist“.

Die vorgestellten Entscheidungen hat das IDSG auch auf seiner Homepage veröffentlicht.

4 Schwerpunkte der Tätigkeiten im Berichtszeitraum

4.1 Datenschutzverletzungen

Im Berichtszeitraum wurden wieder zahlreiche Datenschutzverletzungen von Verantwortlichen sowie betrieblichen Datenschutzbeauftragten und -koordinatoren gemeldet. Die Meldungen bewegten sich fast auf Vorjahresniveau und haben lediglich im mittleren einstelligen Prozentbereich zugenommen.

Die häufigsten Datenpannen betrafen diesmal die falsche Übermittlung und Weitergabe von besonderen Kategorien personenbezogener Daten – allein aus dem Gesundheitsbereich kamen hierzu weit über 50 Meldungen. Die Dunkelziffer dürfte gerade in diesem Bereich dennoch aufgrund der unzähligen herumzureichenden Gesundheitsunterlagen wie beispielsweise Arztbriefe oder Röntgenbilder und fehlerbehafteten Übertragungswegen enorm sein.

Knapp hinter dem Falschversand von Gesundheitsdaten folgten die sogenannten BCC-Fälle. Aus Versehen per offenem Verteiler versandt wurden dabei von Einrichtungen ganz überwiegend lediglich „harmlose“ Newsletter oder Info-Schreiben ohne personenbezogene Inhalte an zahlreiche Adressaten, die dadurch jedoch untereinander die E-Mail-Adressen einsehen konnten.

> „Bei einigen besonders gravierenden Datenschutzverletzungen kam das Kath. Datenschutzzentrum Frankfurt/M. nicht umhin, neben Beanstandungen und Anordnungen zur Wiederherstellung von rechtmäßigen Zuständen in Einzelfällen auch zusätzlich Bußgelder [...] zu verhängen.“

Gravierender war dagegen die von einem Schulleiter dem Kath. Datenschutzzentrum Frankfurt/M. gemeldete Datenschutzverletzung. Eine seiner Lehrkräfte hatte statt einer allgemeinen Information das Protokoll zur virtuellen pädagogischen Konferenz, in dem explizit das Sozialverhalten und die Leistungsstände einzelner Schüler einer Klasse aufgeführt waren und eigentlich nur für die Schulleitung bestimmt war, an die komplette Elternschaft dieser Klasse geschickt.

Der Leiter einer anderen Schule meldete auch eine für alle Beteiligten bittere Datenpanne. Eine Lehrerin hatte die Einladung zu einem Elterngespräch mit der Schulleitung wegen des drohenden Schulausschlusses des Kindes versehentlich an den 26 Eltern umfassenden Klassenverteiler statt nur an die Eltern des Schülers versandt.

In einem anderen Fall hatte sich der Absender einer E-Mail in einer Klinik bei der Auswahl des Empfängers ebenfalls verklickt und das Schreiben statt an die Mitarbeitervertretung an einen internen Verteiler mit rund 150 Adressen von Mitarbeiterinnen und Mitarbeitern geschickt. Aufgeführt waren in der E-Mail Daten über arbeitsrechtliche Rechtsverhält-

nisse wie zum Beispiel Arbeitszeiten, Befristungen, Gehaltsinformationen oder Fortbildungen von Beschäftigten. Nur aufgrund der intensiven Bemühungen des Verantwortlichen zur Behebung der Mängel und der Folgen der Datenschutzverletzung hat das Kath. Datenschutzzentrum Frankfurt/M. vorliegend von einschneidenderen Maßnahmen abgesehen.

Diese Beispiele machen wieder einmal deutlich, dass das Versenden einer E-Mail an einen großen Empfängerkreis zwar praktisch und unkompliziert, nach dem Drücken des Senden-Buttons das Zurückholen quasi unmöglich ist, gegebenenfalls das genaue Gegenteil bewirkt wird.

Sehr häufig gingen im Jahr 2020 Meldungen zu Datenschutzverletzungen auch einher mit gestohlenen und verlorenen mobilen Geräten wie Laptops, Smartphones, Tablet-PCs, Digitalkameras, externen Festplatten und nach wie vor USB-Sticks, die gerne einmal in den Fotodruckern bei dm, Rossmann & Co. stecken gelassen werden. Unter den verloren gegangenen Geräten befand sich sogar das Mobilteil eines Festnetztelefons mit zahlreichen darauf befindlichen personenbezogenen Daten, das unauffindbar aus einer Einrichtung offensichtlich weit in ein angrenzendes Feld geworfen wurde.

Höherwertige elektronische Geräte sind oft der Grund für Einbrüche – bevorzugt am Wochenende in Einrichtungen wie Kindertagesstätten. Es zeigt sich dabei immer wieder aufs Neue, dass es noch viel zu häufig an der Verschlüsselung von Festplatten mangelt und die SD-Karten nach wie vor oft in den Kameras belassen und nicht separat gelagert werden. Hier könnte mit einfachen Mitteln noch viel für den Schutz personenbezogener Daten getan werden.

Auffällig sind nach dem Eindruck der Datenschutzaufsicht, die sich häufenden Meldungen zum Verlust von Dokumenten auf dem Postweg. Da es sich dabei des Öfteren um arbeitsrechtliche Vertragsunterlagen handelt, die in der Regel noch auf dem herkömmlichen Weg verschickt werden, ist der Inhalt gemäß der Durchführungsverordnung zum KDG (KDG-DVO) häufig der höchsten Datenschutzklasse III zuzuordnen.

Gleich zu Beginn des Berichtszeitraums gingen bereits in kurzer Folge zahlreiche Meldungen von – teils vermuteten – Datenschutzverletzungen zu einer Citrix-Sicherheitslücke ein.

Bei einigen besonders gravierenden Datenschutzverletzungen kam das Kath. Datenschutzzentrum Frankfurt/M. nicht umhin, neben Beanstandungen und Anordnungen zur Wiederherstellung von rechtmäßigen Zuständen in Einzelfällen auch zusätzlich Bußgelder, teils in fünfstelliger Höhe, zu verhängen.

4.1.1 Bettelbrief und verbrannte Erde im Pfarrbüro

Weshalb die KDG-DVO die dienstliche Nutzung privater IT-Systeme untersagt, zeigt folgende Datenpanne in einem Pfarrbüro. Die Pfarrsekretärin nutzte viele Jahre ihren privaten E-Mail-Account zur dienstlichen Korrespondenz. Im Berichtszeitraum wurde dieser jedoch gehackt. Der Eindringling versandte einen Bettelbrief an die rund 400 im Adressbuch befindlichen Kontakte und löschte im Anschluss sämtliche – auch seelsorgerischen – Inhalte des Postfachs unwiederbringlich. Die private und dienstliche Korrespondenz der Pfarrsekretärin von zwölf Jahren war damit für immer verloren und sie musste sich im weiteren Verlauf zudem noch mit Fragen von Empfängern „ihres“ Bettelbriefs herumschlagen. Der erzwungene Anschauungsunterricht zum Thema der notwendigen Trennung von dienstlichen und privaten E-Mails zeigte zumindest in diesem Fall durchschlagenden Erfolg und führte zur prompten Aktivierung des dienstlichen Accounts.

4.1.2 Schulserver verschlüsselt

Andere Cyberkriminelle verschlüsselten per Trojaner den Server einer Bildungseinrichtung und hinterlegten virtuell gut sichtbar ein Erpresserschreiben. Die von der Datenschutzaufsicht empfohlene komplette Löschung des Systems mit anschließender erneuter Einrichtung war für die IT der Schule keine große Herausforderung. Eine ältere Sicherungskopie half schließlich beim Wiederaufbau des Datenbestands. Allerdings war das verwendete Backup mit den Daten nicht mehr taufrisch. Denn pandemiebedingt blieb der Vorfall lange Zeit unentdeckt und in der Folge sind auch die Backups überschrieben worden.

4.1.3 Bilder auf Abwegen

Wie schnell ein Bild sich verbreitet und wie wichtig deshalb Einwilligungen der abgebildeten Menschen sind, zeigte die Geschichte hinter einer Datenschutzverletzung in einer Kindertagesstätte. Diese stellte dem örtlichen Bürgermeister Fotos mit spielenden Kindern zur Verfügung, welche dieser wiederum an die Redakteure seiner (kommunalen) Facebook-Seite zur Veröffentlichung weiterleitete. Nach einer Beschwerde aus der Elternschaft musste die Einrichtung feststellen, dass keine Einwilligungen von den Eltern der erkennbar abgebildeten Kinder vorlagen. Aufgrund der sofortigen Maßnahmen des Verantwortlichen zur Beseitigung des datenschutzwidrigen Zustands und dessen nachdrücklichem Hinweis an die Mitarbeiterinnen und Mitarbeiter auf die einzuhaltenden Vorschriften und ihre Verantwortung in diesem Zusammenhang wurde vorliegend auf weitergehende Maßnahmen über eine Beanstandung hinaus verzichtet.

4.2 Beschwerden

Die Beschwerden sind im Berichtszeitraum insgesamt leicht zurückgegangen. Das ist ein erfreuliches Zeichen und lässt den vorsichtigen Schluss zu, dass vor Ort in den Einrichtungen sorgsamer mit Daten umgegangen wird und der Datenschutz zunehmend ins Bewusstsein rückt.

4.2.1 Virtuelle Klassenzimmer

Ein Schwerpunkt im Jahr 2020 war sicherlich der Datenschutz an Schulen im Rahmen des Einsatzes von Videokonferenztools. Beschwerden erreichten die Datenschutzaufsicht beispielsweise von Eltern, die den Einsatz datenschutzrechtlich problematischer Lösungen für den Distanzunterricht bemängelten. Nachfragen bei den Schulen und deren Trägern zeigte oft, dass der Datenschutz bis zur Pandemie doch eher stiefmütterlich behandelt wurde – teilweise war vor Ort überhaupt kein Ansprechpartner für den Datenschutz vorhanden. Man merkte, dass die Schulen in der Pandemie und unter dem Druck, den Unterrichtsbetrieb irgendwie aufrechterhalten zu müssen, an ihre Grenzen kamen. Neben der vernehmlich murrenden Elternschaft kam nun auch noch die Datenschutzbaustelle hinzu. Das eine oder andere Mal erschien dem Kath. Datenschutzzentrum Frankfurt/M. vor allem zu Beginn der Umgang mit ihm als Behörde fast ablehnend – wobei die Datenschutzaufsicht von Beginn an den konstruktiven Dialog mit den Verantwortlichen gesucht hat. Das Datenschutzzentrum Frankfurt/M. war und ist in dieser herausfordernden und nie dagewesenen Lage immer bemüht, die Gesamtsituation im Blick zu haben, und sich gleichzeitig mit den kirchlichen und staatlichen Datenschutzbehörden zu dieser heiklen Thematik auszutauschen. Zusätzliche Hilfestellung sollte Verantwortlichen auch die 2020 veröffentlichte Orientierungshilfe zu Online-Meeting-Tools geben.

4.2.2 Testung von Krankenhausbeschäftigten

Eine weitere Beschwerde war ebenfalls eine Nebenwirkung der Pandemie. Ein Krankenhaus ließ seine Mitarbeiterinnen und Mitarbeiter vom eigenen Betriebsarzt auf das Coronavirus testen. Dieser fragte die Beschäftigten unter anderem auch nach Vorerkrankungen, Allergien und Ähnlichem. Die auf diese Weise gewonnenen Daten flossen im Anschluss in das allgemeine Krankenhausinformationssystem (KIS), auf die die Krankenhausmitarbeitenden zugreifen konnten. Diese Vermischung von Patienten- und Betriebsarztdaten ging dem Beschwerdeführer deutlich zu weit. Er forderte von seinem Dienstgeber die Löschung sämtlicher im Rahmen der Testung erhobenen und verarbeiteten Daten aus dem KIS. Nach dem Einschalten der Datenschutzaufsicht erklärte sich der Verantwortliche zu einer Trennung der aufgeführten Daten im IT-System und zur Vornahme weiterer Datenschutzmaßnahmen bereit.

4.2.3 Ignorierte Auskunftsersuchen

Andere Petentinnen und Petenten beschwerten sich über Verantwortliche von kirchlichen Einrichtungen, die ihrer Ansicht nach überhaupt nicht beziehungsweise nicht ausreichend ihren Auskunftsersuchen nachkamen. An diesen Beschwerden über mangelnde Auskünfte zeigt sich einmal wieder, dass der Umfang des Auskunftsrechts über die verarbeiteten personenbezogenen Daten umstritten bleibt und deshalb oft zu Konflikten führt.

4.3 Anfragen

Enorm angestiegen ist die Anzahl der Anfragen. Dies kann schlicht daran liegen, dass deren Erfassung im Berichtszeitraum noch konsequenter vorgenommen wurde oder auch, dass das Wirken der Datenschutzaufsicht mehr in den Fokus der Verantwortlichen und Einrichtungen gerückt ist und deren Expertise nachgefragt wird. Eine Möglichkeit ist sicher auch, dass sich pandemiebedingt gänzlich neue Fragen gestellt haben – vor allem im Gesundheits-, aber auch im Betreuungsbereich, in den Schulen und den Kirchengemeinden, bei deren Beantwortung das Kath. Datenschutzzentrum Frankfurt/M. in einem bereits sehr frühen Stadium zu Rate gezogen wurde.

„Pandemiebedingt haben sich gänzlich neue Fragen gestellt – vor allem im Gesundheits-, aber auch im Betreuungsbereich, in den Schulen und den Kirchengemeinden, bei deren Beantwortung das Datenschutzzentrum Frankfurt/M. in einem bereits sehr frühen Stadium zu Rate gezogen wurde.“

4.3.1 Corona wirft neue Fragen auf

Pandemiebedingt erreichten die Datenschutzaufsicht auch zahlreiche Anfragen zur Datenweitergabe an Gesundheitsämter, zum Homeoffice, zum Einsatz von Microsoft beziehungsweise Office 365, zur Einführung von Google Workspace (G-Suite) oder Zoom in kirchlichen Einrichtungen. Einige Anfragen betrafen auch die Anfertigung und Verwendung von Fotos in Kinderbetreuungseinrichtungen. Immer wieder gestellt wurden ebenfalls knifflige Fragen zur Zuständigkeit der staatlichen oder kirchlichen Datenschutzaufsicht, die auch Verantwortliche das eine oder andere Mal zum Grübeln über ihre Zugehörigkeit brachten.

4.3.2 Vernichten oder womöglich archivieren?

Weitere Anfragen erreichten das Kath. Datenschutzzentrum Frankfurt/M. von Einrichtungen zum Umfang und der Stelle für die Erfüllung von Informationspflichten und zu Aufbewahrungsfristen von Unterlagen. Zum letztgenannten Punkt werden Verantwortliche zeitnah überlegen müssen, wie sie künftig hinsichtlich der Archivierungspflicht mit der zunehmenden Menge an nur noch in elektronischer Form vorliegenden Dokumenten

umgehen wollen – und müssen. Es empfiehlt sich an dieser Stelle regelmäßig, frühzeitig den Kontakt zum zuständigen (Erz-)Bistum zu suchen. Denn möglicherweise unterfällt eine kirchliche Einrichtung hinsichtlich der Frage nach den Aufbewahrungsfristen auch der Kirchlichen Archivordnung der Katholischen Kirche und deren Regeln. Die Archivordnung geht als besondere kirchliche Rechtsvorschrift dem KDG vor und gilt beispielsweise auch für den Caritas-Bereich. Eine Archivierung würde dann die Vernichtung der Unterlagen gegebenenfalls ersetzen.

4.3.3 Datenschutz ist Opferschutz

Die Datenschutzaufsicht wurde auch zu datenschutzrechtlichen Fragestellungen im Rahmen der Aufarbeitung von Missbrauchsfällen konsultiert sowie zu einem Folgeprojekt zur Erkennung systemischer Risiken, das aus der sogenannten MHG-Studie hervorgegangen ist.

4.4 Gerichtsverfahren

Im Tätigkeitsbericht für das Jahr 2019 berichtete das Kath. Datenschutzzentrum Frankfurt/M., dass Klagen vor dem IDSG gegen seine Entscheidungen nicht lange auf sich warten ließen und es eine bereits in die zweite Instanz geschafft hatte. Diese Klage wegen angeblicher Untätigkeit der Datenschutzaufsicht blieb letztlich auch vor dem Datenschutzgericht der Deutschen Bischofskonferenz erfolglos (Az.: DSG-DBK 01/2019).

Im Berichtszeitraum 2020 gesellten sich sechs Klagen gegen das Datenschutzzentrum Frankfurt/M. (und zum Teil weitere Antragsgegner) dazu. In einem Verfahren ging es wieder einmal um eine angebliche Untätigkeit und in weiteren Verfahren um die verweigerte Erteilung von Auskünften zu personenbezogenen Daten durch Verantwortliche. Einigen dieser Klagen lagen sehr komplexe und zudem heikle Sachverhalte zugrunde, denn die Kläger begehrten unter anderem die Preisgabe von Daten im Rahmen einer Heimunterbringung eines minderjährigen Kindes und in einem anderen Fall die Herausgabe sämtlicher Daten einer angestellten Person im Hochschulbereich.

Eine in 2020 erhobene Klage ließ das IDSG gleich an der Zulässigkeit scheitern: Es zweifelte an der wahren Identität des Antragstellers. In einem weiteren Fall wollten der Antragsteller und sein Rechtsbeistand nicht wahrhaben, dass im katholisch-kirchlichen Bereich das KDG und nicht die DSGVO Anwendung findet. Von deren Warte aus konsequent wurde Klage gegen das Kath. Datenschutzzentrum Frankfurt/M. beim staatlichen Verwaltungsgericht eingereicht. Die drei Richter der Verwaltungsgerichtskammer fanden dafür deutliche Worte und stellten klar, dass für gerichtliche Rechtsbehelfe gegen Entscheidungen der katholischen Datenschutzaufsicht nun einmal gemäß § 49 Abs. 3 KDG das IDSG zuständig ist. Eine verwaltungsgerichtliche Überprüfung kommt laut Beschluss

nur und zudem eingeschränkt in Betracht, „sofern der innerkirchlich vorgegebene Rechtsweg ausgeschöpft ist“. Denn aufgrund der verfassungsrechtlich geschuldeten Rücksichtnahme auf das Selbstbestimmungsrecht der Religionsgesellschaften gebühre der innerkirchlichen Gerichtsbarkeit der Vorrang vor der subsidiären Anrufung staatlicher Gerichte.

4.5 Prüfungen

Das Kath. Datenschutzzentrum Frankfurt/M. konnte die bereits im Jahr 2019 begonnenen umfangreichen Prüfungen von Websites kirchlicher Einrichtungen und hier speziell der sieben (Erz-)Bistümer im Zuständigkeitsbereich auf Datenschutzkonformität im Berichtszeitraum abschließen. Auf die gute und konstruktive Zusammenarbeit mit den Ordinariaten der (Erz-)Diözesen ist an dieser Stelle ausdrücklich hinzuweisen. Es wurden zahlreiche technische Anpassungen wie beispielsweise bei der Verwendung von Cookies und externen Inhalten vorgenommen und insbesondere die für die Nutzerinnen und Nutzer so wichtigen Datenschutzerklärungen auf aktuellen Stand gebracht. Gleichwohl bestanden auch bei einer Nachprüfung noch Auffälligkeiten, die von den Verantwortlichen in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen sind. Da eine Internetseite „lebt“ und ständigen Änderungen unterworfen ist, sind regelmäßige Kontrollen und gegebenenfalls Überarbeitungen im Hinblick auf den Datenschutz durch den Verantwortlichen ohnehin angezeigt.

Die auch in 2019 begonnenen Website-Prüfungen der verschiedenen Caritasverbände und -zentren wurden im Berichtszeitraum fortgesetzt und führten erfreulicherweise ebenfalls bereits zu deutlichen Verbesserungen beim Datenschutz und der Datensicherheit. Aufgrund der auch im technischen Bereich bestehenden komplexen Zusammenhänge im Caritas-Bereich dauern die Vorgänge noch an und werden von einem Austausch sowohl auf technischer als auch juristischer Ebene begleitet.

Bei einigen Caritasverbänden zeigte sich durch Verweise auf die nicht einschlägige DSGVO in der Datenschutzerklärung auf der Internetseite, dass nach wie vor die eigenen Datenschutzregeln der Katholischen Kirche nicht allgemein bekannt sind.

4.5.1 Prüfung der Erfassung von Gottesdienstbesuchern

Im letzten Quartal 2020 prüfte das Kath. Datenschutzzentrum Frankfurt/M. unter anderem auch die Erfassung der Gottesdienstbesucher im Rahmen der Nachverfolgung von möglichen Infektionsketten während der Covid-19-Pandemie unter Datenschutzaspekten.

Um es gleich vorweg zu sagen: Die Ergebnisse waren äußerst positiv. Es gab nur in ganz wenigen Fällen unstimmige Selbstauskünfte durch Kirchengemeinden, die jedoch im Gespräch mit der Datenschutzaufsicht geklärt werden konnten.

Die Datenschutzaufsicht ist verpflichtet, über die Einhaltung der datenschutzrechtlichen Vorschriften zu wachen und sich hiervon gegebenenfalls durch Prüfungen vor Ort zu überzeugen. Aus diesem Grund hat die Datenschutzaufsicht einen Fragebogen (siehe unten) entwickelt, um den für die Kirchengemeinden und die Gläubigen so wesentlichen Be-

Muster-Fragebogen für Kirchengemeinden zum datenschutzkonformen Umgang mit personenbezogenen Daten von Gottesdienstbesuchern während der Pandemie

Katholisches Datenschutzzentrum
Frankfurt/M. KdöR

Bitte zurücksenden bis zum 05.11.2020 **Az.: .....**

An das
Kath. Datenschutzzentrum Frankfurt/M.
Domplatz 3, Haus am Dom
60311 Frankfurt

Fragebogen

Datenschutzkonformer Umgang mit personenbezogenen Daten von Gottesdienstbesuchern während „Corona-Zeiten".

Mehrfachnennungen sind bei allen Fragen außer 1. und 3. möglich.

1. **Werden in Ihrer Kirchengemeinde personenbezogene Daten von Gottesdienstbesuchern erfasst?**

   ☐ Ja

   ☐ Nein

   Wenn ja, weiter bei Frage 2.

   Wenn nein, kann die Beantwortung der weiteren Fragen unterbleiben.

2. **Welche Daten erfassen Sie?**

   ☐ Name

   ☐ Vorname

   ☐ Anschrift

   ☐ Geburtsdatum

   ☐ E-Mail-Adresse

   ☐ Tel.-Nr. (Festnetz)

   ☐ Tel.-Nr. (Mobil)

   ☐ Sonstige:

   _____

Kath. Kirchengemeinde Straße Ort

standteil des gemeindlichen Lebens wie den Gottesdienstbesuch zu Pandemiezeiten beziehungsweise dessen Begleitumstände auf Datenschutzkonformität hin zu überprüfen.

Die Besucherinnen und Besucher von Gottesdiensten sollten der Kirchengemeinde ihre Daten „mit einem guten Gefühl“ überlassen, das heißt in dem Wissen, dass die Kirchen-

3. Werden zusätzlich Daten zum gesundheitlichen Zustand der Gottesdienst-Besucher erfasst?

- ☐ Ja
- ☐ Nein

4. Worauf werden die Gottesdienstbesucher bei ihrer Anmeldung hingewiesen?

- ☐ Zweck der Verarbeitung
- ☐ Rechtsgrundlagen der Verarbeitung
- ☐ mögliche Empfänger der Daten
- ☐ Löschfristen
- ☐ keine Hinweise

5. Wann erfolgt die Anmeldung?

- ☐ vor dem Gottesdienst
- ☐ im Rahmen der unmittelbaren Teilnahme am Gottesdienst

6. In welcher Form erfolgt die Anmeldung?

- ☐ in Papierform (Anmeldeformular)
- ☐ in Papierform (Teilnehmerliste)
- ☐ telefonisch
- ☐ auf der Homepage
- ☐ per E-Mail-Nachricht
- ☐ per Mobilfunkanwendung (u. a. App)

7. In welcher Form werden die personenbezogenen Daten nach der Anmeldung verarbeitet (Speicherung, Übermittlung o. ä)?

- ☐ in Papierform
- ☐ elektronisch

Kath. Kirchengemeinde Straße Ort

gemeinde sorgsam, sparsam und datenschutzkonform mit ihren Daten umgeht und diese Daten nur zu dem Zweck verwendet, für den sie erhoben wurden beziehungsweise die Daten auch nur an denjenigen herausgibt, der gesetzlich zur Verarbeitung verpflichtet ist.

8. Wer ist an der Verarbeitung der personenbezogenen Anmeldedaten Ihrer Kirchengemeinde beteiligt?

- ☐ hauptamtliche Mitarbeiter (z. B. Pfarrer, Diakon, Gemeindereferenten)
- ☐ ehrenamtliche Mitarbeiter (z. B. Pfarrgemeinderat, Gemeindemitglieder)
- ☐ externe Dienstleister (z. B. bei der Anmeldung per App)

9. Wo werden die personenbezogenen Daten der Gottesdienstbesucher (Listen) aufbewahrt? Mehrfachnennungen sind möglich.

- ☐ während des Gottesdienstes: beim zuständigen Ansprechpartner
- ☐ während des Gottesdienstes: liegen im Eingangsbereich aus
- ☐ während des Gottesdienstes: in der Sakristei
- ☐ vor und nach dem Gottesdienst: im Pfarrbüro
- ☐ in einem verschlossenen Schrank oder Behältnis
- ☐ bei elektronischer Erfassung in einem Ordner mit besonderer Zugriffsberechtigung
- ☐ Sonstiges:

_____

10. Wann werden die erhobenen Daten nach dem Gottesdienst gelöscht?

- ☐ unmittelbar nach dem Gottesdienst
- ☐ spätestens nach 1 Woche
- ☐ spätestens nach 1 Monat
- ☐ spätestens nach 12 Wochen
- ☐ gar nicht

11. Wie erfolgt die Löschung der Daten in Papierform?

- ☐ über den Hausmüll/Papiertonne
- ☐ durch Schreddern der Liste
- ☐ über zertifizierte Entsorgungsunternehmen

Kath. Kirchengemeinde Straße Ort

Für die Überprüfung wurden aus allen sieben (Erz-)Diözesen jeweils gleich viele Pfarreien per Zufallsgenerator als Prüfkandidaten ausgewählt. Der Rücklauf erfolgte zügig, so dass der Prüfvorgang noch im selben Jahr abgeschlossen werden konnte.

12. Wie erfolgt die Löschung der Daten in elektronischer Form?

- ☐ vollständiges Löschen der Anmelde-E-Mails im E-Mail-Postfach
- ☐ vollständiges Löschen der erstellten Teilnehmerlisten
- ☐ automatisierte Löschung
- ☐ manuelle Löschung
- ☐ Löschen über den externen Dienstleister

13. An welche Dritte wurden die Daten bereits weitergegeben?

- ☐ Gesundheitsamt
- ☐ Polizeibehörden
- ☐ keine
- ☐ Sonstige:

_____

14. Auf welcher Rechtsgrundlage erfolgt die Datenerfassung?

- ☐ kirchliche Regelung (Maßgaben des Bistums)
- ☐ Landesregelung
- ☐ kommunale Regelung

15. Besteht die Möglichkeit zur spontanen Teilnahme am Gottesdienst?

- ☐ Nein
- ☐ Ja, durch persönliches Eintragen in eine Teilnehmerliste vor Ort
- ☐ Ja, durch Registrierung beim zuständigen Ansprechpartner vor Ort

16. Erfolgt ein Abgleich der angemeldeten Besucher mit den tatsächlichen Gottesdienstbesuchern vor Ort?

- ☐ Nein
- ☐ Ja, durch persönliches Eintragen in eine Teilnehmerliste vor Ort
- ☐ Ja, durch Abgleich durch den zuständigen Ansprechpartner vor Ort

Kath. Kirchengemeinde Straße Ort

Die betrieblichen Datenschutzbeauftragten der (Erz-)Bistümer wurden im Übrigen über die Prüfung informiert und ihnen der Fragebogen an die Kirchengemeinden zur Information übersandt. Sofern also möglicherweise einzelne Kirchengemeinden Fragen im Zusammenhang mit der Bearbeitung des Fragebogens an den betrieblichen Datenschutzbeauftragten herangetragen haben, konnte dieser gegebenenfalls bereits kurzfristig weiterhelfen.

4.5.2 Anlassbezogene virtuelle Prüfung einer Kindertagesstätte

Das Kath. Datenschutzzentrum Frankfurt/M. stellte bereits im letzten Tätigkeitsbericht eine drastische Datenschutzverletzung vor, die sich in einem Kindergarten zugetragen hatte. Dort wurde eine Digitalkamera gestohlen, auf deren Speicherkarte sich Fotos von teils unbekleideten Kindern im Rahmen eines Rollenspiels befunden haben. Die Vorgeschichte und die weitreichenden Konsequenzen sind im Bericht für das Jahr 2019 nachzulesen.

Der gesamte Vorgang gab Anlass zu einer Prüfung, die auch beispielsweise die Begutachtung der Verfahrensverzeichnisse und weiterer Unterlagen nach sich zog und ihren Abschluss in einem ausführlichen Gespräch – pandemiebedingt in Form einer Videokonferenz – mit allen Beteiligten gefunden hat.

5 Veranstaltungen und Öffentlichkeitsarbeit

Dienstreisen konnten im Berichtszeitraum aufgrund der Corona-Beschränkungen kaum unternommen werden. Das hat das Kath. Datenschutzzentrum Frankfurt/M. aber nicht davon abgehalten, Schulungs- und Fortbildungsmaßnahmen in den virtuellen Raum zu verlegen, um Unterstützung zu leisten und sich fachlich auszutauschen. Im Jahr 2020 wurden zum Beispiel Videokonferenzen zu datenschutzrechtlichen Themen mit den betrieblichen Datenschutzbeauftragten der (Erz-)Bistumsordinariate veranstaltet sowie mit Schulleiterinnen und Schulleitern katholischer Schulen. Ein reger Austausch fand ebenfalls auf einer Infoveranstaltung des Diözesancaritasverbands Stuttgart statt als auch zum technischen Datenschutz mit katholischen Krankenhäusern.

Die Diözesandatenschutzbeauftragte sowie die Referenten des Kath. Datenschutzzentrums Frankfurt/M. für Recht und Informationstechnologie nahmen ihrerseits an mehreren Fortbildungsveranstaltungen teil – beispielsweise am Europäischen Datenschutztag in Berlin, am evangelischen Datenschutztag in Hannover, an der 44. DAFTA im November oder an Seminaren zu Datensicherheit im Gesundheitswesen und zu internationalen Datentransfers.

6 Meldungen von betrieblichen Datenschutzbeauftragten

Das Kirchliche Datenschutzgesetz schreibt kirchlichen Stellen vor, einen betrieblichen Datenschutzbeauftragten zu benennen und ihn der Datenschutzaufsicht zu melden. Hier zeigt sich eine erfreuliche Tendenz. Die Meldungen von betrieblichen Datenschützern haben im Berichtszeitraum 2020 deutlich zugenommen. Einige (Erz-)Diözesen haben sich ein Beispiel am Bistum Trier genommen, das im Jahr 2019 einen Großteil seiner Datenschutzbeauftragten gemeldet hat.

> „Die Meldungen von betrieblichen Datenschützern haben im Berichtszeitraum 2020 deutlich zugenommen."

7 Vernetzung mit anderen Datenschutzaufsichten

Trotz erschwerter Bedingungen waren die fünf katholischen Datenschutzaufsichten um einen regelmäßigen Austausch zu den zentralen aktuellen Themen im Datenschutz bemüht. Da die Anfragen aus den deutschen (Erz-)Bistümern zu Corona und Datenschutz landauf, landab ganz ähnlich gelagert waren, bot sich diesbezüglich eine enge Zusammenarbeit geradezu an und ist im Übrigen ausdrücklich im Kirchlichen Datenschutzgesetz auch so vorgesehen.

Die Pandemie hat aber nicht nur die katholischen Datenschutzaufsichten enger zusammenrücken lassen. Auch mit den staatlichen Aufsichtsbehörden in Baden-Württemberg und in Rheinland-Pfalz fand ein intensiver Austausch statt. In Videokonferenzen mit den Datenschutzbeauftragten der beiden genannten Bundesländer, Dr. Stefan Brink und Prof. Dr. Dieter Kugelmann, wurde beispielsweise über den Datentransfer in die USA nach dem Ende des Privacy Shield diskutiert, über den Einsatz von Microsoft beziehungsweise Office 365 mit seinen zahlreichen Tools an Schulen oder über den Gesundheitsdatenschutz in Krankenhäusern.

8 Orientierungshilfen des Kath. Datenschutzzentrums Frankfurt/M.

Im Berichtszeitraum hat das Kath. Datenschutzzentrum Frankfurt/M. für Einrichtungen in seinem Zuständigkeitsbereich auch einige Orientierungshilfen zu aktuellen Themen erstellt, die auf der Website der gemeinsamen Datenschutzstelle der (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier abrufbar sind.

8.1 Online-Meeting-Tools

▶ Zum Download
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Online-Meeting-Tools-04-2020-KDSZ-FFM.pdf

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

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

Vorab ist darauf hinzuweisen, dass zuerst geprüft werden sollte, ob das virtuelle Treffen als Video- oder als Telefonkonferenz erfolgen muss bzw. kann. Im Sinne von Datensparsamkeit und Datenminimierung ist immer der Telefonkonferenz der Vorzug zu geben.

1. Welche Beurteilungskriterien sollten bei der Auswahl eines Online-Meeting-Tools herangezogen werden? Zunächst gilt es bei der Auswahl des Online-Meeting-Services festzulegen, welche Kriterien dafür relevant sind.

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

1.2. In welchem Land befindet sich der Serverstandort?
1.2.1 Serverstandort Deutschland/ EU
Wenn möglich, sind Online-Meeting-Services aus Deutschland oder der EU bzw. dem EWR zu bevorzugen, da diese unmittelbar den Vorgaben der DSGVO (bzw. des KDG) unterliegen und somit ein angemessenes Schutzniveau gewährleistet ist.

1.2.2 Serverstandort Drittland

Nach § 40 Abs. 1 KDG ist die Datenübermittlung an oder in ein Drittland oder an eine internationale Organisation zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt und dieser Beschluss wichtigen kirchlichen Interessen nicht entgegensteht.

Liegt nach § 40 Abs. 1 KDG kein Angemessenheitsbeschluss vor, dann kann die Datenübermittlung zulässig sein, wenn in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind (§ 40 Abs. 2 Nr. 1 KDG) oder der Verantwortliche oder der Auftragsverarbeiter nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, davon ausgehen kann, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen (§ 40 Abs. 2 Nr. 2 KDG).

Liegen die Voraussetzungen des § 40 KDG nicht vor, so kann unter den Voraussetzungen des § 41 KDG in Ausnahmefällen eine Datenverarbeitung in einem Drittland zulässig sein.

1.3 Auftragsverarbeitung

Als Auftragsverarbeiter werden Dienstleister bezeichnet, die personenbezogene Daten ihrer Kunden oder Mitarbeiter entsprechend deren Weisungen verarbeiten. Auch Anbieter von Video- und Online-Konferenzdiensten sind grundsätzlich als Auftragsverarbeiter anzusehen, sodass die Maßgaben der §§ 29 ff. KDG zu beachten sind. Ferner müssen die Angaben zu technischen und organisatorischen Maßnahmen sowie zu eingesetzten Subunternehmern geprüft werden.

1.4 Werden Daten verschlüsselt versendet?

Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Hier ist insbesondere die Verschlüsselung der Daten relevant. § 27 KDG fordert, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Eine Verschlüsselung darf deshalb nicht „optional zuschaltbar“ sein, sondern sollte vorgegeben werden. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind. Dies kann durch eine sichere Datenhaltung in der Applikation, die die Daten z. B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt, gewährleistet sein.

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

Es gilt im Einzelfall zu bestimmen, welche Art von Verschlüsselung benötigt wird. Dies hängt letztlich von der Art der Daten ab, die verarbeitet werden.

1.5 Werden übermittelte Dateien, aufgezeichnete Videomitschnitte oder Fotos nach einem festgelegten Zeitraum gelöscht?

§ 7 Abs. 1 lit. c) KDG fordert eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß. Die Beschränkung gilt für die Datenmenge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist darauf zu achten, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden. Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende-Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z. B. durch staatliche Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server ins Leere.

1.6 Werden weitere Daten versendet?

Weiter ist zu klären, ob nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet werden und ob der Anwender die Kontrolle über die bei ihm hinterlegten Kontaktdaten Anderer behält. Bei einigen gängigen Online-Meeting-Services wird z. B. die komplette Kontaktliste an den Provider übermittelt und die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt. Dies gilt es zu vermeiden. Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden (§ 7 Abs. 1 lit. a) KDG). Der Betroffene hat nach §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch Online-Meeting-Services.

1.7 Ist es notwendig eine Business-Version zu verwenden?

Für die Verwendung in Einrichtungen eignen sich in der Regel keine Tools, die für den privaten Einsatz gedacht sind. Sollten Sie sich trotzdem für eine private Version entscheiden, gilt es darauf zu achten, dass die geschäftliche Nutzung erlaubt ist (da datenschutzrechtliche Zusicherungen auf Geschäftskunden beschränkt sein können).

In jedem Fall sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt werden. Von Anbietern wird teilweise die nicht-private Nutzung der privaten Versionen untersagt, teilweise wird lediglich die kommerzielle Anwendung untersagt. Das bedeutet, dass die Nutzung des Produkts durch ehrenamtliche Non-Profit-Organisationen möglich ist, für eine kommerzielle Nutzung aber der Erwerb einer Business-Version erforderlich ist.

Sollten auch Jugendliche an einer Telekonferenz teilnehmen müssen, ist darauf zu achten, dass ein Mindestalter entsprechend geregelt ist. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren.

Weiter sollte man vorab überprüfen, wie viele Personen in der Regel bei den Telekonferenzen teilnehmen und die Lizenzvereinbarungen dahingehend überprüfen, ob diese Menge von der Lizenz mitumfasst ist.

Zuletzt ist auch auf eine örtliche Begrenzung des Dienstes zu achten. Manche Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

1.8 Werden Logfiles (Protokolldateien) erstellt?
Logfiles sollten nur erstellt werden, soweit diese erforderlich sind. Diese können auch für die Fehlerbehebung durch den Dienstleister notwendig sein. Logfiles sind dann nur zu diesem Zweck zu verwenden und nach Wegfall des Zwecks wieder zu löschen.

1.9 Wie lange werden personenbezogene Daten gespeichert?
Hier ist sicherzustellen, dass Dateien und personenbezogene Daten nur für den benötigten Zeitraum zur Verfügung stehen und danach automatisch gelöscht werden. Bei der Telekonferenz dürfte dies nach Ende des Meetings der Fall sein. Werden Dateien ausgetauscht, kann z. B. ein Zeitraum von wenigen Stunden oder einem Tag gewählt werden, innerhalb dessen die Teilnehmer Zeit haben, die Daten herunterzuladen und anderweitig abzulegen. Ergänzend sollte als organisatorische Maßnahme geregelt werden, welche Arten von Dokumenten (nicht) über den Online-Meeting-Service geteilt werden dürfen. Dies kann sowohl als Blackoder als Whitelist ausgestaltet werden.

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

2. Welche technischen und organisatorischen Maßnahmen sind bei der Verwendung des gewählten Tools zu berücksichtigen?
Nach der Entscheidung für den Anbieter muss noch geprüft werden, welche technischen und organisatorischen Maßnahmen anzuwenden sind. Welche insbesondere hierfür relevant erscheinen, finden Sie untenstehend.

2.1 Können die Datenschutzeinstellung innerhalb des Online-Meeting-Services manuell angepasst werden?
Bei vielen Tools ist es notwendig, die Datenschutzeinstellungen richtig zu konfigurieren, um einer möglichen unzulässigen Datenverarbeitung vorzubeugen. Hier sollte insbesondere im Hinblick auf die Datensparsamkeit ein besonderes Augenmerk liegen.

2.2 Wer nimmt an der Telekonferenz teil?
Einladungen sollten nur an Personen vergeben werden, die für die behandelten Themen die nötige Freigabe haben. Dies kann durch die Einrichtung von Zugangsbeschränkungen (z. B. über Login-Daten) oder durch die einzufordernde Zustimmung des Organisators bei der Teilnahme von Gästen geschehen.

2.3 Auf was muss beim ScreenSharing geachtet werden?
Es ist unbedingt darauf zu achten, dass nur für das Online-Meeting relevante Informationen zu sehen sind. Es empfiehlt sich, unnötige Inhalte und Fenster zu schließen und einen separaten Desktop einzurichten, auf dem keine Dateien oder Verknüpfungen zu sehen sind.

2.4 Was ist im Hintergrund der Teilnehmer zu sehen?
Es muss darauf geachtet werden, dass keine Informationen im Hintergrund der Teilnehmer zu sehen sind, die nicht für die anderen Teilnehmer der Konferenz bestimmt sind.

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

2.6 Darf die Telekonferenz aufgezeichnet werden?
Viele Tools bieten mittlerweile die Möglichkeit, die Videokonferenz aufzunehmen. Dies ist in den meisten Fällen nur mit einer Einwilligung aller Teilnehmer zulässig. Daher sollte das Tool so eingestellt werden können, dass vor Start der Aufnahme bei allen Teilnehmern eine Nachricht mit den nötigen Informationen erscheint sowie die Option besteht, zuzustimmen oder abzulehnen.

2.7 Wie kann Datenverstößen vorgebeugt werden?
Vor allem sind die Teilnehmer entsprechend zu informieren und zu sensibilisieren, welche Daten über das Tool (vor allem auch mit Externen) geteilt werden dürfen.

3. Weitere Hinweise

Ob und ggf. welche arbeitsrechtlichen vor allem mitarbeitervertretungsrechtlichen Aspekte bei der Nutzung von Online-Meeting-Tools bzw. Online-Meeting-Services zu beachten sind, unterliegt nicht datenschutzrechtlicher Beurteilung. Es wird hierzu eine eigene Prüfung empfohlen.

4. Fazit

Aufgrund der Menge an Online-Meeting-Services ist es nicht möglich, eine allgemeinverbindliche Lösung anzubieten. Dieses Dokument soll daher als Entscheidungshilfe dienen, sich – in Abhängigkeit der jeweils vorliegenden Situation – für einen passenden Anbieter zu entscheiden. ■

8.2 MAVO-Änderung – Videokonferenzen für Mitarbeitervertretungen

Videokonferenzen jetzt auch für MAVen möglich

Corona sei Dank. Mitarbeitervertretungen können nun auch virtuell Beschlüsse fassen. Die Präsenzpflicht für Mitglieder der betrieblichen Interessenvertretung bei Sitzungen wurde im Zuge der Pandemie aufgehoben.

Um auch ohne die physische Anwesenheit der MAV-Mitglieder wirksam Beschlüsse fassen zu können, wurde § 14 Abs. 4 der Mitarbeitervertretungsordnung (MAVO) um folgende Sätze ergänzt: „Kann die Sitzung der Mitarbeitervertretung wegen eines unabwendbaren Ereignisses nicht durch die körperliche Anwesenheit eines oder mehrerer Mitglieder durchgeführt werden, kann die Teilnahme einzelner oder aller Mitglieder an der Sitzung auch mittels neuer Informations- und Kommunikationstechnologien erfolgen, wenn sichergestellt ist, dass Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können. Im Hinblick auf die Beschlussfähigkeit gelten die an der virtuellen Sitzung teilnehmenden Mitglieder als anwesend im Sinne des Abs. 5 S. 1.“

Neue Technologien im Einsatz

Mittlerweile haben alle sieben Bistümer im Zuständigkeitsbereich des Katholischen Datenschutzzentrums Frankfurt/M. – die (Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier – diese Gesetzesänderung in Kraft gesetzt und in ihren Amtsblättern veröffentlicht.

Damit durch diese durchaus heikle Änderung der Datenschutz auch in virtuellen MAV-Sitzungen weiterhin eine hohe Priorität genießt, wurde ausdrücklich die Formulierung aufgenommen, dass die oben genannten Technologien in diesem ▶

▶ **Zum Download**
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/MAVO-Aenderung-Pandemie-05-2020.pdf

Zusammenhang nur eingesetzt werden dürfen, wenn „Dritte vom Inhalt der Sitzung keine Kenntnis nehmen können“.

Schweigepflicht gilt auch bei mobiler Arbeit
Nicht zu vergessen ist auch in außergewöhnlichen Pandemie-Zeiten, dass MAV-Mitglieder gemäß § 20 MAVO der Schweigepflicht unterliegen. Danach haben sie „über dienstliche Angelegenheiten oder Tatsachen, die ihnen aufgrund ihrer Zugehörigkeit zur Mitarbeitervertretung bekanntgeworden sind und Verschwiegenheit erfordern, Stillschweigen zu bewahren“. Da es sich in der Regel um sensible Daten der Schutzklasse III gemäß § 13 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) handelt, sind diese Informationen – auch im Homeoffice – besonders zu schützen.

Orientierungshilfe bietet Unterstützung
Unterstützung bei der Auswahl von datenschutzkonformer Video- und Telefonkonferenz-Software bietet unsere aktuelle Datenschutz-Orientierungshilfe allen interessierten Einrichtungen und Mitarbeitervertretungen. Das Infoblatt mit Auswahlkriterien für Online-Meeting-Tools steht auf der Homepage in der Infothek unter „Arbeitshilfen“ zum Download bereit. ■

8.3 EuGH erkärt Privacy Shield für ungültig

EuGH kippt Datenschutzabkommen mit USA
Mit seinem Urteil vom 16. Juli 2020 – C-311/18 (sog. „Schrems II-Urteil“) stellt der Europäische Gerichtshof (EuGH) fest, dass der Beschluss der EU-Kommission zur Angemessenheit des Datenschutzniveaus in den Vereinigten Staaten von Amerika (USA) ungültig ist. Denn die amerikanischen Behörden können nach dortigem Recht auf aus der EU übermittelte personenbezogene Daten zugreifen. Ein wirksamer Rechtsschutz ist zudem in den USA nicht vorhanden. Damit ist eine Übermittlung personenbezogener Daten aus der Europäischen Union (EU) in die USA auf der Grundlage des EU-US-Datenschutzschilds (sog. Privacy Shield) nicht zulässig.

Die Gültigkeit der dazu von der EU-Kommission beschlossenen Standardvertragsklauseln wird hingegen bestätigt. Allerdings stellt der EuGH fest, dass bei einer Übermittlung auf der Grundlage von Standarddatenschutzklauseln, insbesondere den Standardvertragsklauseln, für die Rechte Betroffener ein Schutzniveau gewährleistet sein muss, das dem in der EU gleichwertig ist. Es obliegt dem Verantwortlichen bzw. seinem Auftragsverarbeiter in jedem Einzelfall zu prüfen, ob das Recht des Bestimmungslandes einen angemessenen Schutz gewährleistet.

▶ **Zum Download**
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/EuGH-kippt-Datenschutzabkommen-mit-USA-KDSZ-FFM.pdf

Auswirkungen des EuGH-Urteils auf Verantwortliche und Auftragsverarbeiter im Sinne des KDG

Das EuGH-Urteil betrifft nicht nur die Übermittlung personenbezogener Daten in die USA, sondern Übermittlungen allgemein an und in Drittländer oder internationale Organisationen. Verantwortliche und ihre innerhalb der EU ansässigen Auftragsverarbeiter, die eine solche Übermittlung durchführen, müssen umgehend prüfen, ob die bisherige rechtliche Grundlage der Übermittlung noch Bestand hat. Da mit dem EuGH-Urteil eine Übermittlung personenbezogener Daten auf der Grundlage des EU-USDatenschutzschilds rechtswidrig ist, steht § 40 Abs. 1 KDG nicht mehr als Grundlage für eine Datenübermittlung in die USA zur Verfügung. Ob und inwieweit die Regelungen des § 41 KDG zur Anwendung gelangen, ist ggf. zu prüfen. Der Anwendungsbereich des § 41 KDG ist jedoch auf Ausnahmetatbestände beschränkt.

Standarddatenschutzklauseln (Standardvertragsklauseln)

Da der EuGH feststellt, dass eine Übermittlung personenbezogener Daten auf der Grundlage von Standarddatenschutzklauseln unter bestimmten Bedingungen weiterhin zulässig ist, kommen die von der EU-Kommission beschlossenen Standardvertragsklauseln (Beschluss 2010/87/EU) als Rechtsgrundlage in Betracht. Verantwortliche und ggf. Auftragsverarbeiter müssen jedoch auf Grundlage des EuGH-Urteils prüfen, ob das Recht des Bestimmungslandes einen angemessenen Schutz der zu übermittelnden personenbezogenen Daten bietet und erforderlichenfalls über die Standarddatenschutzklauseln hinausgehende Garantien gewährleisten. Kann auch mit über die Standarddatenschutzklauseln hinausgehenden Garantien kein angemessener Schutz der zu übermittelnden personenbezogenen Daten erreicht werden, ist die Übermittlung auszusetzen oder zu beenden.

Beispielsweise können Gesetze im Bestimmungsland dem Empfänger der zu übermittelnden Daten Pflichten auferlegen, die es ihm unmöglich machen, die vertraglichen Vereinbarungen mit dem Verantwortlichen zu befolgen. Eine Übermittlung ist in diesem Fall nicht zulässig. Das EuGH-Urteil betont in diesem Zusammenhang insbesondere die Zugriffsmöglichkeit auf personenbezogene Daten durch Behörden im Bestimmungsland. Im Falle der USA führt es ebenfalls einen fehlenden Rechtsschutz für betroffene Personen vor staatlichen Überwachungsprogrammen an. Solche Überwachungsprogramme greifen ggf. bereits während der Übertragung und bevor die zu übermittelnden Daten in den USA ankommen. Es ist also höchst fraglich, ob im Fall der USA überhaupt geeignete Garantien gegeben werden können.

Prüfung durch Verantwortliche und Auftragsverarbeiter

Verantwortliche und ihre innerhalb der EU ansässigen Auftragsverarbeiter müssen prüfen, ob sie eine durch das EuGH-Urteil betroffene Übermittlung personenbezogener Daten durchführen oder planen. Ist dies der Fall, muss die Rechts- ▶

grundlage der Übermittlung nach der Maßgabe der Gerichtsentscheidung geprüft und ggf. neu bewertet werden. Ist die Rechtsgrundlage durch das Urteil entfallen und kann auch keine neue Rechtsgrundlage geschaffen werden, ist die Übermittlung zu unterbinden oder zu beenden.

Bei der Analyse von Übermittlungen personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums (EWR) ist es hilfreich, zwischen Daten, die zwingend im Bestimmungsland verarbeitet werden müssen (beispielsweise beim Versand einer E-Mail an einen Empfänger außerhalb des EWR), und Daten, die auch (etwa durch einen anderen Auftragsverarbeiter) innerhalb des EWR verarbeitet werden könnten, zu unterscheiden.

Auswirkungen des EuGH-Urteils auf Betroffene im Sinne des KDG
Durch das EuGH-Urteil entstehen keine neuen Pflichten für Betroffene.

Fazit
Verantwortliche und Auftragsverarbeiter, die personenbezogene Daten in Länder außerhalb des EWR übermitteln, müssen in Folge des EuGH-Urteils sofort handeln. Da keine Übergangsfrist vorgesehen ist, sind Verarbeitungen mit entfallener Rechtsgrundlage unmittelbar unzulässig. ■

Weiterführende Hinweise:

- EuGH-Urteil vom 16.07.2020 im Volltext: C-311/18 – Facebook Ireland und Schrems
- EuGH-Pressemitteilung Nr. 91/20 vom 16.07.2020: Der Gerichtshof erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig

▶ **EuGH-Urteil vom 16.07.2020**
https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18

▶ **Pressemitteilung Nr. 91/20**
https://curia.europa.eu/jcms/jcms/p1_3117872/de/

9 Mitteilungen aus der Konferenz der Diözesandatenschutzbeauftragten

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche erörtert aktuelle Themen aus dem Bereich des kirchlichen Datenschutzes, erarbeitet dazu gemeinsame Empfehlungen und gibt diese in Form von Beschlüssen bekannt. Daneben veröffentlichen die in der Konferenz zusammengeschlossenen fünf Diözesandatenschutzbeauftragten auch Mitteilungen zu speziellen datenschutzrechtlichen Fragestellungen – so geschehen zum Schrems II-Urteil des EuGH (siehe unter Ziffer 3) und den möglichen Folgen.

Mitteilung zum „Schrems II"-Urteil des EuGH vom 16. Juli 2020

EuGH erklärt EU-US-Privacy-Shield für ungültig

In dem am Donnerstag, 16. Juli 2020, verkündeten Urteil des EuGH („Schrems II") erklärt der Gerichtshof den „Privacy Shield" für ungültig. Zur Urteilsbegründung führt der Gerichtshof aus, dass das Datenschutzniveau der EU und damit der durch die DS-GVO festgelegte und geforderte Schutz für personenbezogene Daten bei einer Übermittlung in die USA durch das Datenschutzabkommen („Privacy Shield") nicht gewährt werden kann.

In den Fällen, in denen Verantwortliche die Datenübermittlungen in die USA auf das nun nicht mehr gültige Datenschutzabkommen zwischen der EU und den USA gestützt haben, müssen diese nun handeln, da sie andernfalls personenbezogene Daten ohne Rechtsgrundlage in ein Drittland transferieren. Nicht für generell ungültig erklärt wurden die Standarddatenschutzklauseln der EU-Kommission nach Art. 46 Abs. 2 lit. c) und d) DS-GVO.

Bei der Verwendung von Standarddatenschutzklauseln müssen die Einrichtungen jedoch künftig bei der Übermittlung personenbezogener Daten in ein Drittland überprüfen, ob dort -evtl. auch durch zusätzliche vertragliche Vereinbarungen- ein angemessenes Datenschutzniveau hergestellt werden kann und diese Vereinbarungen eingehalten werden können. Nur in diesem Fall können die Standarddatenschutzklauseln eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in ein Drittland darstellen. Daher obliegt den Verantwortlichen in den kirchlichen Einrichtungen eine Rechtsprüfung, inwiefern das Datenschutzniveau im jeweiligen Drittland dem der DS-GVO entspricht bzw. dort von den Vertragspartnern eingehalten werden kann.

Das Urteil betrifft für die Anwendung der Standarddatenschutzklauseln alle Datenübertragungen in Drittländer, die keinem Angemessenheitsbeschluss nach ▶

▶ **Zum Download**
https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Mitteilung-Konferenz-20200723.pdf

Art. 45 DS-GVO unterfallen. Durch den Wegfall des „Privacy Shield“ fehlt ein solcher Beschluss jetzt auch für die USA. Nach den Ausführungen des EuGH (insbesondere Rn. 185/197) ist für die USA auch der Einsatz von Standarddatenschutzklauseln nicht mehr möglich.

Der EuGH hat auch die Erwartung geäußert, dass die europäischen Datenschutzaufsichten eine einheitliche Auslegung unter den Aufsichtsbehörden herbeiführen.

Die Datenschutzaufsichten arbeiten derzeit noch intensiv an dieser einheitlichen Auslegung und stimmen sich ab. Sofern bisher vorgenommene Übermittlungen personenbezogener Daten in die USA nun nicht mehr auf eine gültige Rechtsgrundlage gestützt werden können, werden die Diözesandatenschutzbeauftragten die Vorgaben des Urteils umsetzen; das erfordert aber intensive Untersuchungen zu der Frage, wie – ohne Gefährdung des laufenden Betriebs – ein Ausstieg möglich ist. ■

10 Ausblick

Das Jahr 2020 befand sich fest im Griff der Pandemie. Auch dem Datenschutz drohte in mancher Situation die Luft auszugehen. Nicht selten wurde der Datenschutz zum „Buhmann“ in der Pandemiebekämpfung und zum angeblichen Blockierer im Kampf gegen die Seuche. Dass das Recht auf informationelle Selbstbestimmung ein Grundrecht ist, das es genauso zu schützen gilt, wie andere von der Verfassung gewährleistete Rechte von Bürgerinnen und Bürgern, ging wohl zeitweise im – auch medialen – Getöse unter. Dabei ist der Datenschutz bei dem Ganzen nicht das Problem. Er bringt im Gegenteil Ordnung in manch chaotisches Vorgehen.

Nicht zuletzt die zahlreichen gemeldeten Datenpannen im Zuge der Pandemie zeigen die Notwendigkeit, auch in Krisenzeiten genau auf den Datenschutz zu achten. Fortschritt braucht Vertrauen. Und nachhaltiges Vertrauen braucht einen verlässlichen am Hier und Jetzt ausgerichteten Datenschutz. Er hilft dabei, die gesellschaftlichen Herausforderungen erfolgreich zu meistern.

Die nunmehr wieder hörbareren besonneneren Stimmen zum Ausklang der Pandemie lassen hoffen, dass der Datenschutz durchaus gestärkt aus dieser Situation hervorgeht – und sogar unverhofft für bleibende Verbesserungen sorgt.

11 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 2020