Jahresbericht 2021

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Berichtszeitraum
01.01.–31.12.2021

Katholisches Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn
sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel.: 0231/13 89 85 – 0
Fax: 0231/13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Hinweis: Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt adäquate andere Formen gleichberechtigt ein.

Bildnachweis Titelmotiv: istockphoto.com | matejmo

6. Jahresbericht

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

für den Zeitraum 01.01.2021–31.12.2021

Redaktionsschluss: 30.09.2022

Inhaltsverzeichnis

Vorwort

Das Berichtsjahr 2021 war wie das Vorjahr geprägt durch die Corona-Pandemie.

Für die kirchlichen Einrichtungen und das Katholische Datenschutzzentrum bedeutete dies wie im Vorjahr, neue pandemiebedingte Fragestellungen zu klären oder Abläufe innerhalb der Einrichtungen pandemiebedingt anzupassen und diese dabei weiterhin auch datenschutzkonform zu organisieren.

Neben Corona sind andere Themen im Rückblick fast in Vergessenheit geraten. So erfolgten im ersten Halbjahr 2021 die finalen Schritte zum Brexit. Die datenschutzrechtlichen Folgen des Brexit konnten aber durch die schnelle Verabschiedung eines Angemessenheitsbeschlusses durch die EU-Kommission minimiert werden.

Auch die Umsetzung beziehungsweise Beachtung des Schrems II-Urteils wurde durch die pandemiebedingt verstärkte Nutzung von Kommunikationsdiensten aufgrund der faktischen Zwänge zur kurzfristigen Aufrechterhaltung z. B. des Schulunterrichts teilweise aufgeschoben. Hier muss aber eine dauerhaft tragfähige, datenschutzkonforme Lösung gefunden werden.

Im September 2021 konnten das Katholische Datenschutzzentrum und der von den fünf nordrhein-westfälischen (Erz-)Diözesen gemeinsam bestellte Diözesandatenschutzbeauftragte auf fünf Jahre Tätigkeit zurückblicken. Dieser wichtige und richtige Schritt zur besseren Umsetzung der kirchlichen Datenschutzaufsicht in den fünf (Erz-)Diözesen wurde von Wegbereitern und Wegbegleitern unseres Hauses im Rahmen unserer Veröffentlichung „Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung" als zweitem Band der Schriften zum kirchliche Datenschutz genutzt, um die Anfänge unseres Hauses und aktuelle Fragestellungen des kirchlichen Datenschutzes gesammelt zu dokumentieren. Für die Bereitschaft, an dieser Veröffentlichung mitzuarbeiten, darf ich mich nochmals bei allen Beteiligten bedanken.

Bedanken möchte ich mich auch bei den Kolleginnen und Kollegen des Katholischen Datenschutzzentrums, denn die Arbeit unseres Hauses lebt vom Engagement und dem Wissen der Mitarbeitenden. Ohne sie wäre die Arbeit nicht möglich.

Steffen Pau
Diözesan- und Verbandsdatenschutzbeauftragter
und Leiter des Katholischen Datenschutzzentrums (KdöR)

1 Entwicklungen im Datenschutzrecht

Die gesetzgeberischen oder regulatorischen Initiativen zur Weiterentwicklung des Datenschutzrechts auf europäischer, nationaler und kirchlicher Ebene waren auch in diesem Berichtszeitraum wieder zahlreich und werden im Folgenden auszugsweise dargestellt.

1.1 Gesetzgeberische Entwicklungen auf Ebene der Europäischen Union

Auf europäischer Ebene wurde im Berichtszeitraum unter anderem der Angemessenheitsbeschluss für das Vereinigte Königreich Großbritannien und Nordirland in Kraft gesetzt und über die neuen Standardvertragsklauseln entschieden. Nachfolgend sind einige aus Sicht des Katholischen Datenschutzzentrums (KDSZ) wichtige Vorhaben erläutert.

1.1.1 Brexit und der Angemessenheitsbeschluss der Europäischen Kommission zum Vereinigten Königreich Großbritannien und Nordirland

In einem Referendum hatten sich Mitte 2016 die Bürger des Vereinigten Königreichs Großbritannien und Nordirland für einen Austritt aus der Europäischen Union (EU) entschieden, den sog. „Brexit".

Als eine Folge dieser Entscheidung war die Europäische Datenschutz-Grundverordnung (DSGVO) auf den Datenaustausch zwischen den beteiligten Staaten nach Vollzug des Austritts aus der EU nicht mehr anwendbar.

Damit auch nach einem Austritt Großbritanniens aus der EU weiterhin die Datenschutzstandards der EU beim Austausch von personenbezogenen Daten zwischen der EU und dem Vereinigten Königreich sichergestellt werden können, verhandelten Vertreter beider Seiten über ein Handels- und Kooperationsabkommen. Darin verständigten sie sich für eine Übergangsfrist u. a. darauf, dass Transfers personenbezogener Daten zwischen der EU und dem Vereinigten Königreich für einen Übergangszeitraum nicht als Transfers in ein Drittland im Sinne von Art. 44 DSGVO angesehen werden sollten[1].

Noch gerade rechtzeitig vor dem endgültigen Ablauf der vereinbarten Übergangsfrist verabschiedete die Europäische Kommission am 26.06.2021 zwei Angemessenheitsbeschlüsse im Sinne von Art. 45 DSGVO, mit denen der Datenaustausch zwischen der EU und dem Vereinigten Königreich eine neue Grundlage erhielt. Dadurch konnte vermieden werden, das Vereinigte Königreich als ein Drittland im Sinne der DSGVO und des KDG (Gesetz über den Kirchlichen Datenschutz) ein-

[1] Vgl. Article FINPROV.10a: Interim provision for transmission of personal data to the United Kingdom.

zustufen. Dabei bezog sich ein Beschluss auf Datenübermittlungen im Anwendungsbereich der DSGVO und ein Beschluss auf Datenübermittlungen im Rahmen der JI-Richtlinie.

Mit diesen Angemessenheitsbeschlüssen stellte die Europäische Kommission fest, dass im Vereinigten Königreich auch nach dem „Brexit" ein Schutzniveau besteht, welches dem nach EU-Recht vorgegeben Schutzniveau grundsätzlich gleichwertig ist. Dadurch ermöglicht die Europäische Kommission den Austausch personenbezogener Daten ohne weitere Maßnahmen zwischen den am Datentransfer beteiligten Parteien.

„Das Vorliegen dieser Angemessenheitsbeschlüsse ist auch für den Bereich der katholischen Kirche von Bedeutung ..."

Das Vorliegen dieser Angemessenheitsbeschlüsse ist auch für den Bereich der katholischen Kirche von Bedeutung, da § 40 Abs. 1 KDG in diesen Fällen die Übermittlung in Drittländer oder an internationale Organisationen für zulässig erklärt.

Die Europäische Kommission kommt in den Beschlüssen zu dem Ergebnis, dass das Datenschutzsystem des Vereinigten Königreichs auch weiterhin auf denselben Regeln basiert, welche bereits Geltung hatten, als das Vereinigte Königreich noch ein Mitgliedstaat der EU war. Nach Auffassung der Europäischen Kommission hat das Vereinigte Königreich die Grundsätze, Rechte und Pflichten der DSGVO und der Richtlinie zum Datenschutz bei der Strafverfolgung hinreichend in sein heutiges, seit dem Brexit geltendes Rechtssystem übernommen.

Die Europäische Kommission führt weiter aus, dass das Vereinigte Königreich geeignete Garantien in Bezug auf den Zugriff auf personenbezogene Daten durch Behörden vorsieht. Hervorgehoben wird, dass die Datenerhebungen durch Nachrichtendienste einer vorherigen Genehmigung durch ein unabhängiges Rechtsorgan unterliegen. Darüber hinaus wird durch das britische Recht vorgegeben, dass sämtliche Maßnahmen notwendig und im Hinblick auf das verfolgte Ziel verhältnismäßig sein müssen.

Ferner wird darauf verwiesen, dass im Bedarfsfall Klage bei einem Gericht für Ermittlungsbefugnisse, dem Investigatory Powers Tribunal, eingereicht werden kann, wenn sich ein Betroffener unrechtmäßiger Überwachungsmaßnahmen ausgesetzt sehen sollte. Derzeit unterliegt das Vereinigte Königreich noch der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, der Europäischen Menschenrechtskonvention und dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Bei Letzterem handelt es sich um das einzige verbindliche internationale Übereinkommen auf dem Gebiet des Datenschutzes. Bei der Bewertung des Rechtsrahmens durch die Europäische Kommission haben diese völkerrechtlichen Verpflichtungen eine wesentliche Bedeutung gehabt.

Zu beachten ist, dass erstmalig bei einem Angemessenheitsbeschluss eine Verfallsklausel eingefügt worden ist. Die Angemessenheitsbeschlüsse bezüglich des Vereinigten Königreichs sind auf vier Jahre ab ihrem Inkrafttreten befristet. Danach besteht die Möglichkeit, dass sie erneuert werden können, sofern das Vereinigte Königreich auch weiterhin ein nach Ansicht der Europäischen Kommission angemessenes Datenschutzniveau sicherstellt. Die Europäische Kommission hat ange-

kündigt, dass sie im weiteren zeitlichen Verlauf die Entwicklung der Rechtslage im Vereinigten Königreich beobachten und gegebenenfalls eingreifen wird, falls dort vom derzeit bestehenden Datenschutzniveau in Richtung einer Schwächung des Datenschutzes abgewichen werden sollte.

Schon kurz nach der Annahme der Angemessenheitsbeschlüsse durch die Europäische Kommission hat die britische Regierung angekündigt, dass das Vereinigte Königreich Großbritannien und Nordirland sein Datenschutzrecht überarbeiten werde. Dabei hat sie auch darauf hingewiesen, dass beabsichtigt sei, sich von einigen aus der DSGVO übernommenen Regelungen zu lösen. Dies dürfte zur Folge haben, dass die Europäische Kommission überprüfen muss, ob das künftige britische Datenschutzrecht die Anforderungen der DSGVO und die entsprechenden Voraussetzungen für ein gleichwertiges Schutzniveau noch erfüllen wird.

In einer ersten Reaktion der Europäischen Kommission wies ein Sprecher darauf hin, dass die Angemessenheitsbeschlüsse unter dem Vorbehalt stehen, dass das Datenschutzniveau des Vereinigten Königreichs auf einem vergleichbaren Level mit dem EU-Recht liegt. Sollte das Datenschutzniveau jedoch absinken, bestünde die Möglichkeit, die Beschlüsse zu verändern, auszusetzen oder zu beenden.

Sofern bei einer konkreten Prüfung der künftigen Gesetzesänderungen durch die Europäische Kommission festgestellt würde, dass das aus Sicht der EU gewünschte Datenschutzniveau im Vereinigten Königreich nicht mehr erreicht werden sollte, hätte dies voraussichtlich zur Folge, dass die Beschlüsse mindestens ausgesetzt werden würden. In diesem Fall müssten betroffene Unternehmen in der EU weitere Maßnahmen im Sinne von Art. 46 Abs. 1 DSGVO ergreifen, um die Rechtmäßigkeit eines Datentransfers in das Vereinigte Königreich zu gewährleisten.

Auswirkungen auf kirchliche Einrichtungen

Auch wenn mit der Verabschiedung der Angemessenheitsbeschlüsse durch die Europäische Kommission derzeit rechtssichere Grundlagen geschaffen worden sind, die in Erfüllung der Vorgaben von § 29 Abs. 11 KDG auch für die kirchlichen Einrichtungen einen rechtssicheren Datenaustausch mit Stellen im Vereinigten Königreich sowie die Verwendung von Produkten und Dienstleistungen von Anbietern aus dem Vereinigten Königreich ermöglichen, sollten die kirchlichen Stellen und Einrichtungen weiterhin die Entwicklungen genau beobachten.

Verantwortliche sollten für die Zukunft rechtzeitig vor Ablauf der Fristen der Verfallsklauseln die Entscheidungen der Europäischen Kommission beobachten und prüfen, ob auch weiterhin geeignete Rechtsgrundlagen für die eigenen Bedürfnisse zur Verfügung stehen.

Auch vor Ablauf der vierjährigen Geltungsdauer der Angemessenheitsbeschlüsse könnte sich Handlungsbedarf ergeben, wenn die Pläne der britischen Regierung zu substantiellen Änderungen an den britischen Datenschutzbestimmungen umgesetzt werden und damit die mit den Angemessenheitsbeschlüssen festgestellte vergleichbare Rechtslage im Vereinigten Königreich nicht mehr bestehen würde.

Das Katholische Datenschutzzentrum beobachtet die Entwicklungen zu den Angemessenheitsbeschlüssen, um im Fall der erforderlichen Beratung anfragender kirchlicher Stellen vorbereitet zu sein.

1.1.2 Europäische Kommission verabschiedet neue EU-Standardvertragsklauseln

Die Europäische Kommission hatte bereits in den zurückliegenden Jahren zur Ermöglichung von Datentransfers und später auch zur Erfüllung der Vorgaben aus Art. 46 Abs. 2 lit. c) DSGVO Standardvertragsklauseln erlassen. Diese entsprechend ihrer englischen Bezeichnung auch als Standard Contractual Clauses oder abgekürzt als SCC bezeichneten Klauseln zählen zu den geeigneten Garantien im Sinne von Art. 46 DSGVO. Das Bestehen geeigneter Garantien ist Vorbedingung für die Übermittlung von Daten an ein Drittland oder eine internationale Organisation, falls kein Beschluss nach Art. 45 Abs. 3 DSGVO vorliegt (sog. Angemessenheitsbeschluss).

Im Berichtsjahr 2021 hat die Europäische Kommission am 04.06.2021 eine Neufassung der „Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates“ veröffentlicht. Eine Novellierung der Klauseln war erforderlich geworden, um neuere Entwicklungen zu berücksichtigen, insbesondere in der Gesetzgebung durch die DSGVO und in der Rechtsprechung, vor allem durch die Entscheidungen des Europäischen Gerichtshofs (EuGH).

So hatte der EuGH in seiner als „Schrems II“ bekannt gewordenen Entscheidung in der Rechtssache C-311/18 die Möglichkeit der Übermittlung von Daten in die USA unter Verwendung der Standardvertragsklauseln weiterhin für zulässig erachtet, auch wenn das Gericht in der gleichen Entscheidung das Privacy Shield für unanwendbar erklärte. Die weitere Anwendung der SCC hat der EuGH jedoch mit weiteren Anforderungen verbunden. Der Verantwortliche muss sich bei Verwendung der Standardvertragsklauseln überzeugen, dass sein Vertragspartner auch in der Lage ist, die Bedingungen der Klauseln einzuhalten und deren Beachtung sicherzustellen. Dazu gehört auch die Prüfung, ob die Rechtslage im Herkunftsland des Vertragspartners einer Umsetzung der Klauseln entgegensteht und somit die Gewährung eines im Wesentlichen gleichen Datenschutzniveaus mittels der Verwendung der Standardvertragsklauseln nicht sichergestellt werden kann. Dem Verantwortlichen obliegen als Datenexporteur die Verantwortung sowie die Verpflichtungen für die Prüfung der Zulässigkeit der jeweiligen Übermittlungen.

Die neuen Klauseln sind im Unterschied zu ihren Vorgängern modular aufgebaut und beinhalten passende Module für Datenübermittlungen von Verantwortlichen zu Verantwortlichen, von Verantwortlichen zu Auftragsverarbeitern, von Auftragsverarbeitern zu Auftragsverarbeitern sowie von Auftragsverarbeitern zu Verantwortlichen. Die Verwender müssen darunter die für sie und die beabsichtigten Datentransfers geeigneten Klauseln auswählen.

„Die neuen Klauseln sind im Unterschied zu ihren Vorgängern modular aufgebaut …“

Die Verwender von Vertragsklauseln müssen dabei beachten, dass die Vertragsklauseln grundsätzlich nur in der von der Europäischen Kommission verabschiedeten Fassung eine rechtlich zulässige Möglichkeit darstellen, eine Grundlage für den Datentransfer zu bieten, ohne dass es einer zusätzlichen Überprüfung durch eine Datenschutzaufsichtsbehörde bedarf. Nach dem Willen der Kommission dürfen zwar weitere Klauseln und zusätzliche Garantien in die Vertragsvereinbarungen aufgenommen werden. Diese dürfen jedoch nicht zu einer Absenkung des durch die Klauseln angestrebten Schutzniveaus führen und dabei weder mittelbar noch unmittelbar im Widerspruch zu den Standardvertragsklauseln stehen. Ferner dürfen sie nicht die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden.

Der Durchführungsbeschluss der Europäischen Kommission und die neuen Vertragswerke sind am 07.06.2021 im Amtsblatt der Europäischen Union veröffentlicht worden.[2]

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2021:199:TOC
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

Auswirkungen auf kirchliche Einrichtungen

Die bisher geltenden Klauseln durften noch für eine Übergangszeit in Verträgen verwendet werden, sofern diese bis zum 27.09.2021 abgeschlossen wurden. Danach sind nur noch die neuen Standardvertragsklauseln zulässig. Zu beachten ist ferner, dass bis zum 27.09.2022 alle Verträge auf die neuen Versionen der Standardvertragsklauseln umzustellen sind.

Kirchliche Verantwortliche, in deren Verantwortungsbereich Datentransfers in Drittländer fallen, die nicht den Regelungen der DSGVO unterliegen oder für die ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, müssen sich mit den Möglichkeiten und Vorgaben der Standardvertragsklauseln befassen. Dabei ist sorgfältig zu prüfen, ob die Anforderungen der Klauseln durch den jeweiligen Datenempfänger erfüllt werden können.

1.1.3 Gesetzgebungsverfahren zur e-Privacy-Verordnung schreitet voran

Die e-Privacy-Verordnung („Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)") sollte eigentlich schon parallel zur DSGVO im Mai 2018 in Kraft treten.[3] Damit sollten die Regelungen zur elektronischen Kommunikation an die DSGVO angeglichen werden.

Der Gesetzgebungsprozess ist jedoch immer noch nicht abgeschlossen. Am 10.02.2021 wurde die Position des Rates der Europäischen Union verabschiedet, sodass mit den sogenannten Trilog-Verhandlungen begonnen werden konnte.[4] Während der Trilog-Verhandlungen werden Parlament, Rat und Kommission versuchen ihre Verordnungsentwürfe aufeinander abzustimmen. Wann mit einem Abschluss der Verhandlungen zu rechnen ist, lässt sich zum jetzigen Zeitpunkt noch nicht absehen. Eine Einigung könnte länger auf sich warten lassen, da sich die Entwürfe von Rat und Parlament in einigen Grundsatzfragen unterscheiden.[5]

Welche Auswirkungen die Verordnung auf die verschiedenen Formen der Datenverarbeitung durch kirchliche Stellen haben wird, ist erst nach einem Abschluss der Trilog-Verhandlungen beurteilbar.

[3] Siehe hierzu auch Abschnitt 1.1.1 des Jahresberichts 2019.

[4] Der Entwurf kann in der Pressemitteilung abgerufen werden: https://www.consilium.europa.eu/de/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

[5] So z. B. in der Frage der Vorratsdatenspeicherung. Diese lässt sich im Entwurf des Rates in Erwägungsgrund 25 und Art. 7 Abs. 4 finden, während das Parlament diese explizit aus ihrem Entwurf gestrichen hat.

Im Berichtszeitraum hat die Bundesregierung noch am 01.12.2021 mit dem TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) Bestimmungen aus der Vorgängernorm Richtlinie 2002/58/EG umgesetzt.[6]

1.1.4 Vorratsdatenspeicherung

Im Berichtszeitraum war die bundesdeutsche Speicherung von Kommunikationsdaten erneut Gegenstand einer Untersuchung und Bewertung auf europäischer Ebene. Zwar hat der Gerichtshof der Europäischen Union seine zugehörige Entscheidung erst im Jahr 2022 getroffen, jedoch hatte der EuGH-Generalanwalt Manuel Campos Sánchez-Bordona sein Votum im Jahr 2021 veröffentlicht.

In den zurückliegenden Jahren hatte der EuGH bereits mehrfach Entscheidungen zur Vorratsdatenspeicherung getroffen. Darauf nahm der Generalanwalt in seinem Votum Bezug, als er u. a. anklingen ließ, dass die bisherigen Urteile des EuGH die den aktuellen Verfahren zugrunde liegenden Fragestellungen inhaltlich bereits abdecken und Anhaltspunkte für die Beantwortung der Fragen zur Verfügung stellen würden. Dazu betont er die aus seiner Sicht detaillierten Entscheidungsgründe in den zurückliegenden Urteilen des EuGH, die eine hinreichende Klarheit bezüglich der Auffassung des Gerichts beinhalten würden. Nicht überraschend folgt der Generalanwalt in seinem aktuellen Gutachten der durch die vorangegangenen Entscheidungen vorgegebenen Linie.

Den Schlussanträgen des Generalanwalts lagen Rechtssachen aus Deutschland, Frankreich und Irland zugrunde. In der deutschen Rechtssache wurde die Frage gestellt, ob die im Telekommunikationsgesetz (TKG) geregelte Vorratsdatenspeicherung, insbesondere §§ 113a, 113b TKG, gegen europäisches Recht verstoßen würde. Die Frage resultierte aus Begehren von Anbietern von Telekommunikationsdienstleistungen, gerichtlich feststellen zu lassen, dass sie nicht dazu verpflichtet seien, bestimmte Verkehrsdaten auf Vorrat speichern zu müssen.

Inhaltlich führt der Generalanwalt aus, dass eine allgemeine Speicherung von Daten innerhalb eines Landes auch dann nicht gerechtfertigt sei, wenn es darum gehe, schwere Straftaten zu verfolgen. Auch die im Berichtszeitraum aktuelle deutsche Vorratsdatenspeicherung sei mit EU-Recht nicht vereinbar. Die Speicherung würde zu allgemein und zu unterschiedslos vorgenommen werden können. Dies sei nach Auffassung des Generalanwalts nach derzeit geltendem Unionsrecht nicht zulässig. Zugriffe auf die Daten aus einer solchen Vorratsdatenspeicherung würden regelmäßig einen schweren Eingriff in den personenbezogenen Datenschutz darstellen. Ausnahmen könnten nur im Fall einer ernsten Bedrohung für die nationale Sicherheit in Betracht kommen. Selbst im Gesetz vorgesehene zeitliche Begrenzungen könnten nicht zu einem anderen Ergebnis führen.

Auch wenn die Schlussanträge des Generalanwalts für den EuGH nicht bindend sind, zeigen dessen Darlegungen, insbesondere unter Beach-

[6] Siehe dazu auch den Abschnitt 1.2.1 in diesem Jahresbericht.

tung der bisherigen Rechtsprechung des EuGH zum Thema der Vorratsdatenspeicherung, welche Tendenz für die Entscheidung des EuGH zu erwarten ist.

1.2 Gesetzgeberische Entwicklungen in der Bundesrepublik Deutschland

Auch auf nationaler Ebene gab es mehrere, datenschutzrechtlich relevante Gesetzgebungsvorhaben, von denen einige hier erwähnt werden sollen.

1.2.1 Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien tritt in Kraft

Das Telekommunikation-Telemedien-Datenschutz-Gesetz ist am 01.12.2021 in Kraft getreten. Es führt dabei die datenschutzrechtlichen Regelungen des Telekommunikationsgesetzes und des Telemediengesetzes (TMG) zusammen, wobei diese Gesetze mit den nicht datenschutzrechtlichen relevanten Regelungen fortbestehen. Außerdem wurden nun mit dem TTDSG Vorgaben aus der Richtlinie 2002/58/EG (ePrivacy-Richtlinie) umgesetzt.

Das TTDSG enthält datenschutzrechtliche Bestimmungen in den Bereichen der Telekommunikation und Telemedien. Der Schutzzweck des TTDSG umfasst dabei insbesondere das Endgerät des Benutzers. Durch die Regelungen des TTDSG werden alle Anbieter von Telemedien und Telekommunikation gebunden.

Anbieter von Telemedien i. S. d. TTDSG ist gem. § 2 Abs. 2 Nr. 1 jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt. Also z. B. Betreiber und Anbieter von Webseiten, Apps oder Speichermöglichkeiten im Netz. Gemäß § 3 Nr. 61 TKG sind Anbieter von Telekommunikation die Anbieter von Festnetz- und Mobilfunk. Auch Anbieter von Internetanschlüssen zählen zu den Telekommunikationsanbietern.

Auch die katholische Kirche und ihre Stellen fallen in den Anwendungsbereich des TTDSG, sofern sie Anbieter von Telemedien oder Telekommunikation sind. Daher sind die neuen (insbesondere datenschutzrechtlichen) Anforderungen des Gesetzes von den kirchlichen Verantwortlichen zu beachten.

In den §§ 19–24 TTDSG finden sich die Datenschutzbestimmungen bezüglich der Erbringung von Telemediendienstleistungen. Die Regelungen entsprechen im Wesentlichen den Vorgaben der DSGVO beziehungsweise dem KDG und ergänzen diese nur bedingt. Hervorzuheben ist aber das Verbot der kommerziellen Nutzung der Daten Minderjähriger in § 20 TTDSG.

Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Das ist z. B. bei dem Einsatz von Cookies oder anderen Leistungen von Drittanbietern der Fall. Diese Einwilligungserfordernis ist in § 25 Abs. 1 TTDSG normiert.

Grundsätzlich müssen Einwilligungen im Rahmen des § 25 Abs. 1 TTDSG am Maßstab der allgemeinen datenschutzrechtlichen Vorgaben für eine Einwilligung gemessen werden. Die Einwilligung muss daher die Maßstäbe der § 6 Abs. 1 und § 8 KDG erfüllen.

Ausnahmen von der Einwilligungserfordernis sind nunmehr abschließend in § 25 Abs. 2 TTDSG zu finden. Lediglich technisch notwendige Cookies und/oder Dienste sind von der Ausnahme erfasst.

Alle Verantwortlichen müssen prüfen, ob z. B. auf ihren Webseiten oder in ihren Apps Cookies oder Drittdienste ohne eine wirksame Einwilligung eingesetzt werden. Falls dies der Fall ist, muss weiter überprüft werden, ob es sich um Cookies oder Dienste handelt, für die die Ausnahmeregelung gemäß § 25 Abs. 2 Nr. 2 TTDSG greift. Sollte diese Frage nicht geklärt werden können, ist zu raten, die Cookies oder den Dienst vorläufig abzustellen oder vorsichtshalber Cookie-Banner für die Einwilligung einzurichten.

Zu prüfen ist ferner, ob durch die Verwendung von Cookies oder Drittdiensten personenbezogene Daten an Drittländer übertragen werden. Dies ist insbesondere aufgrund der Schrems II (C-311/18) Entscheidung des EuGH für Datenübertragungen in die USA zu bedenken. Ferner hat die Gestaltung der Cookie-Banner TTDSG-konform zu erfolgen.

Umstritten ist noch, ob Arbeitgeber Pflichten als Telekommunikationsdienstleister treffen, wenn sie Angestellten betriebliche Kommunikation auch zur privaten Nutzung zur Verfügung stellen. Unterschiedlich wurde dabei in der Vergangenheit die Frage der Bindung des Arbeitgebers an das Fernmeldegeheimnis beurteilt. Es bleibt abzuwarten, wie die Gerichte diese Frage entscheiden werden. Um Konflikten mit dem Fernmeldegeheimnis aus dem Weg zu gehen, ist Arbeitgebern zu raten, eine private Nutzung von betrieblichen Kommunikationsmitteln zu untersagen.

Verstöße gegen das TTDSG stellen eine Ordnungswidrigkeit dar und können gem. § 28 TTDSG mit einem Bußgeld geahndet werden.

Für die Einhaltung datenschutzrechtlicher Vorgaben im Bereich der katholischen Kirche und ihrer Einrichtungen in den Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandes der Diözesen Deutschlands (VDD) mit den angeschlossenen Einrichtungen ist das Katholische Datenschutzzentrum die zuständige Aufsichtsbehörde. In den §§ 29 und 30 TTDSG sind im Bereich der Telekommunikation Sonderzuständigkeiten für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und die Bundesnetzagentur festgelegt.

Abzuwarten bleibt die Auswirkung von „Personal Information Management Services“ (PIMS) in § 26 TTDSG. Unter PIMS werden Dienste verstanden, die es Nutzern ermöglichen sollen, ihre Präferenzen bezüglich der Handhabung von Cookies einmalig festzulegen, um dann Cookie-Anfragen automatisch zu verarbeiten. Eine konkrete praktische Umsetzung dieser Systeme bedarf allerdings noch einer Rechtsverordnung durch den Bundesgesetzgeber.

Für eine DSGVO- beziehungsweise KDG-konforme Gestaltung von Cookie-Bannern und Einwilligungen kann die Orientierungshilfe (OH) zum TTDSG der DSK (Datenschutzkonferenz) herangezogen werden.[7]

1.2.2 Neue Anforderungen im technischen Datenschutz für kleinere Krankenhäuser (§ 75c SGB V)

Bislang wurden die IT-Sicherheit in Krankenhäusern und die daran gestellten Anforderungen maßgeblich durch § 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geprägt. Diese Vorgaben gelten jedoch nur für Betreiber sogenannter „Kritischer Infrastrukturen“ (KRITIS). Welche Einrichtungen, Anlagen und Teile zu diesen Kritischen Infrastrukturen zählen, wird in § 2 Abs. 10 BSIG i. V. m. der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) festgelegt. Aus § 6 Abs. 4 BSI-KritisV „Sektor Gesundheit“ i. V. m. dem Anhang 5 Teil 3 ergibt sich, dass nur solche Krankenhäuser im Bereich der stationären medizinischen Versorgung zu den Kritischen Infrastrukturen in diesem Sinne zählen, die den Schwellenwert von 30.000 bei der vollstationären Fallzahl/Jahr erreichen oder überschreiten. Kleinere Krankenhäuser – die diesen Schwellenwert nicht erreichen – sind von den Vorgaben somit nicht betroffen.

Im September 2020 wurde der § 75c neu in das Sozialgesetzbuch 5 (SGB V) aufgenommen. Durch diesen sind auch Krankenhäuser, die bisher nicht die Regelungen zum Schutz kritischer Infrastrukturen nach § 8a BSIG anwenden mussten, seit dem 01.01.2022 gemäß § 75c Abs. 1 SGB V verpflichtet, „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind“. Die IT-Systeme sind gemäß dieser Regelung spätestens alle zwei Jahre dem aktuellen Stand der Technik anzupassen. Eine Nachweispflicht gegenüber dem BSI (Bundesamt für Sicherheit in der Informationstechnik) – wie sie für KRITIS-Krankenhäuser besteht – gibt es hingegen nicht.

„Krankenhäusern, die ohnehin schon den KRITIS-Regelungen nach § 8a BSIG unterfallen, werden durch die Norm keine neuen Verpflichtungen auferlegt …“

Krankenhäusern, die ohnehin schon den KRITIS-Regelungen nach § 8a BSIG unterfallen, werden durch die Norm keine neuen Verpflichtungen auferlegt (vgl. § 75c Abs. 3 SGB V).

Die neu erfassten und nunmehr ebenfalls verpflichteten – kleineren – Krankenhäuser können die an sie gestellten Anforderungen

[7] Abrufbar unter: https://datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

gemäß § 75c Abs. 2 SGB V insbesondere dadurch erfüllen, dass sie einen branchenspezifischen Sicherheitsstandard (B3S) für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung umsetzen, dessen Eignung vom BSI nach § 8a Abs. 2 des BSIG festgestellt wurde. Ein solcher Maßstab beschreibt informationssicherheitstechnische Prozesse und Maßnahmen, anhand derer ein angemessenes Schutzniveau bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen erreicht werden kann.

Ein solcher B3S-Sicherheitsstandard wurde durch die Deutsche Krankenhausgesellschaft zur Unterstützung der Krankenhäuser entwickelt und vom BSI im Oktober 2019 anerkannt (Ablauf der Eignungsfeststellung August 2021). Dieser legt die Mindestanforderungen für die Krankenhäuser fest. Alternativ können gleichwertige Managementsysteme für Informationssicherheit (ISMS) zur Erfüllung der Nachweispflicht verwendet werden. Der B3S-Standard für Krankenhäuser wird derzeit überarbeitet.

Die Neuregelung in § 75c SGB V hat auch Auswirkungen auf die Beurteilung des technisch-organisatorischen Datenschutzes von Krankenhäusern. Wenn § 26 KDG unter den dort genannten Bedingungen fordert, „geeignete technische und organisatorische Maßnahmen zu treffen", dann legt der Gesetzgeber mit § 75c SGB V fest, welche Maßnahmen geeignet sind.

Den gleichen Effekt hat die Erwähnung der geeigneten technischen und organisatorischen Maßnahmen (TOM) in § 11 Abs. 4 KDG für die Verarbeitung besonderer Kategorien personenbezogener Daten, hier also z. B. Gesundheitsdaten im Sinne des § 4 Nr. 17 KDG. Auch hier werden die durch § 75c SGB V aufgestellten Vorgaben zukünftig zu berücksichtigen sein.

Die Deutsche Krankenhausgesellschaft stellt auf ihrer Internetseite ein „Starter-Paket" mit Erläuterungen und Handlungsempfehlungen zu § 75c SGB V zur Verfügung.[8]

1.2.3 Datenschutzrechtliche Aspekte der Corona-Gesetzgebung im Jahr 2021

Im Berichtsjahr haben sowohl der Bundesgesetzgeber – insbesondere mit Änderungen des Infektionsschutzgesetzes (IfSG)durch die Novellierungen des „Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" – wie auch der nordrhein-westfälische Landesgesetzgeber in der „Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 (Coronaschutzverordnung – Corona SchVO)" und weiteren begleitenden Verordnungen versucht, die notwendigen gesetzlichen Rahmenbedingungen zum Umgang und der weiteren Bekämpfung der Pandemie in der sich dynamisch entwickelnden Pandemielage zu setzen.

[8] Abrufbar unter: https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/

Die gesetzlichen Vorgaben waren auch von den kirchlichen Einrichtungen zu beachten. Dazu gehörten z. B. die Verpflichtungen zur Erstellung und zum Einsatz von Hygienekonzepten in Einrichtungen mit Publikumsverkehr und die Verarbeitungen von Kontaktdaten zur Nachverfolgung von Infektionsketten. Diese Verarbeitungen hatten den Anforderungen des Datenschutzes zu entsprechen. Besondere Vorgaben bestanden für Schulen und Kindertageseinrichtungen, insbesondere zur regelmäßigen Testung in den Einrichtungen. Verantwortliche in kirchlichen Einrichtungen mussten darüber hinaus ebenso wie alle anderen Arbeitgeber – wo möglich – ein Arbeiten im Homeoffice ermöglichen und dabei sicherstellen, dass diese Art des Arbeitens datenschutzkonform eingerichtet und durchgeführt werden konnte.

Das Infektionsschutzgesetz enthielt auch konkrete Vorgaben bezüglich der Informationspflichten von Beschäftigten bezüglich ihres Impf- und Serostatus, sofern sie in den im Gesetz genannten Einrichtungen tätig waren. Davon betroffen waren auch die entsprechenden kirchlichen Anbieter dieser Einrichtungstypen.[9]

Konkrete Vorgaben für die kirchlichen Einrichtungen im Zuständigkeitsbereich des Katholischen Datenschutzzentrums enthielt die Coronaschutzverordnung des Landes Nordrhein-Westfalen, welche im Laufe des Berichtszeitraums regelmäßig an die aktuellen Entwicklungen angepasst wurde. Die Verordnung konkretisierte die (bundes)gesetzlichen Vorgaben, insbesondere zu den Hygiene- und Infektionsschutzkonzepten sowie der Rückverfolgbarkeit. Spezielle Vorgaben betrafen die stationären Gesundheits- und Pflegeeinrichtungen und somit auch die in diesen Bereichen tätigen kirchlichen Einrichtungen. Für alle Verantwortlichen in kirchlichen Einrichtungen, unabhängig von ihren speziellen Angeboten, bestand die Verpflichtung, ihrer Arbeitgeberverantwortung gerecht zu werden und die in der Coronaschutzverordnung vorgegebenen Maßnahmen umzusetzen.

Für Gottesdienste galt es von den Pfarreien eine Rückverfolgbarkeit der Gottesdienstbesucher sicherzustellen.[10]

1.2.4 Evaluationsbericht des Bundesinnenministeriums zum Bundesdatenschutzgesetz

Das Bundesministerium des Innern und für Heimat (BMI) hat im Berichtszeitraum einen Evaluationsbericht zum Bundesdatenschutzgesetz (BDSG) vorgelegt. Evaluierungsgegenstand war das BDSG in der Fassung nach dem Zweiten Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. DSAnpUG-EU). Die Bewertung sollte insbesondere eine Beurteilung der Erreichung der beabsichtigten Ziele enthalten. Als Ziele wurden in dem Bericht des BMI definiert, die Öffnungsklauseln der nach der DSGVO bestehenden Gestaltungsmöglichkeiten im deutschen Recht zu nutzen, die Regelungsaufträge der DSGVO an die Mitgliedstaaten aufzugreifen und die Richtlinie (EU) 2016/680 umzuset-

[9] Siehe auch Abschnitt 2.1.1 dieses Berichts.

[10] Siehe hierzu auch das Verfahren vor den kirchlichen Datenschutzgerichten zur Einsicht eines Pfarrers in die Gottesdienstbesucherlisten (Abschnitt 1.7 dieses Berichts); zur Kontaktnachverfolgung siehe auch schon Abschnitt 3.1.2 des Jahresberichts 2020.

zen. Zugleich formulierte das BMI, dass die Regelungen des BDSG für die Normanwender praktikabel, verständlich und anwenderfreundlich sein sollten.

Zur Klärung der Fragen nach Sachgerechtigkeit, Praktikabilität und Normenklarheit wurden Verbände und Institutionen zu Stellungnahmen aufgefordert, die in die Bewertung eingeflossen sind.

Im Ergebnis stellt das BMI fest, dass die überwiegende Zahl der Regelungen als sachgerecht, praktikabel und normenklar angesehen werden kann. Auch die eingeholten Stellungnahmen haben zu einem Großteil der Regelungen weder Verständnis- noch Anwendungsschwierigkeiten aufgezeigt. Das BMI beabsichtigt, zu einigen Regelungen mögliche klarstellende Änderungen der bisherigen Formulierungen zu prüfen. Ferner wird das BMI in einigen Fällen untersuchen, ob inhaltliche Änderungen erforderlich werden. Schließlich sind nach den Feststellungen des BMI redaktionelle Änderungen erforderlich, z. B. an Stellen, an denen aufgrund gesetzlicher Entwicklungen Verweisungsnormen angepasst werden müssen.

Darüber hinaus nimmt das BMI kurz zu der Thematik einer weitergehenden Institutionalisierung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder Stellung. Nach Auffassung des BMI steht einer solchen Überlegung das Verbot der Mischverwaltung entgegen. Wegen insoweit bestehender verfassungsrechtlicher Grenzen sei für eine weitere Institutionalisierung der DSK eine Änderung des Grundgesetzes erforderlich.

1.2.5 Betriebsrat als datenschutzrechtlich Verantwortlicher

Durch das „Betriebsrätemodernisierungsgesetz“ vom 14.06.2021 und dem damit neu geschaffenen § 79a BetrVG (Betriebsverfassungsgesetz; Inkrafttreten der Gesetzesänderung 18.06.2021) hat der Bundes-Gesetzgeber versucht, die umstrittene Frage, ob ein Betriebsrat datenschutzrechtlich als Verantwortlicher nach Art. 4 Nr. 7 DSGVO (§ 4 Nr. 9 KDG) gilt, zu klären.

Wer der datenschutzrechtlich Verantwortliche im Rahmen der Datenschutz-Grundverordnung ist, ist u. a. relevant für die Beantwortung der Frage, wen die Pflichten aus Art. 5 Abs. 1 DSGVO (§ 7 Abs. 1 KDG) zur Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten treffen.

Sofern ein Betriebsrat im Rahmen seines Aufgabenbereiches also als datenschutzrechtlich Verantwortlicher angesehen würde, wäre er beispielsweise auch zur Wahrung der Betroffenenrechte verpflichtet und gegen ihn könnten Bußgelder verhängt werden.

Dies hat der Gesetzgeber nun aber ausdrücklich anders geregelt. So heißt nun in § 79a Satz 2 BetrVG: „Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften.“

Diese dem Wortlaut nach eindeutige Zuweisung der Verantwortlichkeit führt jedoch zu einigen Folgeproblemen.

Zum einen entscheidet der Betriebsrat in seinem Zuständigkeitsbereich vollkommen frei. Die Datenverarbeitung erfolgt zur Wahrnehmung von Beteiligungsrechten und nicht etwa im Interesse des Arbeitgebers. Auch steht dem Arbeitgeber gegenüber dem Betriebsrat kein Weisungsrecht zu.

Den Arbeitgeber treffen also die datenschutzrechtlichen Pflichten für den Zuständigkeitsbereich des Betriebsrates bei gleichzeitig eingeschränkten Kontroll- und Einflussmöglichkeiten. Dass eine fehlende Mithilfe des Betriebsrates etwa bei der Erfüllung eines Auskunftsanspruches zu einer Haftung des Arbeitgebers aufgrund eines Verstoßes gegen die Betroffenenrechte führen kann, versucht der Gesetzgeber über § 79a Satz 3 BetrVG zu kompensieren. Danach unterstützen sich Arbeitgeber und Betriebsrat „gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften". Wie weit diese Unterstützung reicht, wird jedoch nicht näher bestimmt.

Da der Betriebsrat als „Nicht-Verantwortlicher" keinen eigenen betrieblichen Datenschutzbeauftragten benötigt, stellt sich zudem die Frage, inwiefern der betriebliche Datenschutzbeauftragte seiner Überwachungsfunktion aus Art. 39 Abs. 1 lit. b) DSGVO gegenüber dem Betriebsrat nachkommen kann, während er gleichzeitig im Lager des Arbeitgebers steht.[11] Dieses Spannungsverhältnis versucht der Gesetzgeber wiederum über die Sätze 4 und 5 des § 79a BetrVG zu entschärfen, indem er den Datenschutzbeauftragten „gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen". Ob dies in der Praxis ausreicht, um zu einer Rechtsprechungsänderung seitens des Bundesarbeitsgerichts (BAG) zu führen, bleibt abzuwarten.

Des Weiteren gibt es Stimmen in der Literatur[12], die von einer Unionsrechtswidrigkeit des § 79a BetrVG aufgrund einer fehlenden Öffnungsklausel und einer damit einhergehenden Unanwendbarkeit (Art. 288 Abs. 1 Vertrag über die Arbeitsweise der Europäischen Union – AEUV) ausgehen. Eine solche Entscheidung obliegt letztendlich allerdings dem Gerichtshof der Europäischen Union.

Es zeigt sich, dass mit der Schaffung des § 79a BetrVG eine vorhandene Rechtsunsicherheit nicht endgültig behoben, sondern lediglich verlagert wurde. Bis zu einer höchstrichterlichen Klärung dieser Fragen kann es unter Umständen sinnvoll sein, die diesbezüglichen innerbetrieblichen Arbeitsabläufe zwischen dem Arbeitgeber und dem Betriebsrat durch eine Betriebsvereinbarung zu klären.

[11] Vgl. dazu BAG, Beschluss vom 11.11.1997 – 1 ABR 21/97.
[12] Maschmann: Der Arbeitgeber als Verantwortlicher für den Datenschutz im Betriebsratsbüro (§ 79a BetrVG)? (NZA 2021, 834).

Auswirkungen für kirchliche Einrichtungen

Die durch das Betriebsrätemodernisierungsgesetz im Betriebsverfassungsgesetz eingefügte Klarstellung zur Frage der Verantwortlichkeit des Betriebsrates wirkt nicht unmittelbar auch in den kirchlichen Bereich hinein. Für die kirchlichen Einrichtungen müsste eine vergleichbare Regelung in die Mitarbeitervertretungsordnung eingefügt werden. Insoweit fehlt es für die kirchlichen Einrichtungen weiter an einer positiv-gesetzlichen Regelung.

Das Katholische Datenschutzzentrum wird die vom Bundesgesetzgeber jetzt für die Betriebsräte gefundene Lösung zukünftig bei Beschwerden oder in der Beratung kirchlicher Einrichtungen als Grundlage seiner Auslegung dieser Frage nehmen.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Auch im kirchlichen Bereich sind im Berichtszeitraum ebenfalls neue Regelungen in Kraft getreten oder verabschiedet worden, die datenschutzrechtliche Vorgaben enthalten.

1.3.1 Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz in Kraft

Zum 01.02.2021 haben die fünf nordrhein-westfälischen (Erz-)Diözesen das Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz (KDS-VwVfG) in Kraft gesetzt, das jetzt die verfahrensrechtliche Grundlage für die Arbeit des Katholischen Datenschutzzentrums darstellt.

Das Gesetz bildet in großen Teilen Normen aus den staatlichen Verfahrensgesetzen ab. Es gibt den kirchlichen Datenschutzaufsichten Werkzeuge für ihre nach außen gerichtete Tätigkeit beziehungsweise zur Erfüllung ihrer Aufgaben aus den Kapiteln 6 und 7 KDG. Insbesondere werden Regelungen zu Verwaltungsakten und Bußgeldverfahren getroffen.

1.3.2 Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens

Im Berichtszeitraum haben die (Erz-)Diözesen in Deutschland ein neues „Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens (Seelsorge-PatDSG)“ erlassen. Es handelt sich dabei um eine besondere kirchliche Rechtsvorschrift im Sinne des § 2 Abs. 2 KDG, die konkrete bereichsspezifische Regelungen bezogen auf die Datenverarbeitungen im Zusammenhang

mit der Seelsorge in katholischen Einrichtungen des Gesundheitswesens enthält. Das neue Gesetz ist somit nicht als unmittelbare Nachfolgeregelung für die bisher in einigen (Erz-)Diözesen geltenden Bestimmungen zum Patientendatenschutz anzusehen, die jeweils als „Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen (PatDSO)" erlassen worden waren. Diese enthielten mehr auf den allgemeinen Patientendatenschutz in katholischen Einrichtungen des Gesundheitswesens ausgerichtete Normen und dienten auch als kircheneigene Regelungen im Verhältnis zu den Gesundheitsdatenschutzgesetzen der Bundesländer. Zu beachten ist in der Konsequenz, dass für die besonderen Datenverarbeitungen im Krankenhaus jetzt die Regelungen des KDG gelten und sichergestellt sein muss, dass diese Vorgaben in der Anwendung befolgt werden.

Bei den in der Krankenhausseelsorge verwendeten Daten handelt es sich um besondere personenbezogene Daten in Form von Gesundheitsdaten gemäß § 4 Nr. 17 KDG, worauf in § 2 Abs. 1 lit. b) Seelsorge-PatDSG ausdrücklich hingewiesen wird. Sie unterliegen daher den strengen Vorgaben bezüglich einer Datenübermittlung, insbesondere denjenigen, die in § 11 KDG niedergelegt sind. Dem entsprechend ist eine Verarbeitung dieser besonderen Kategorien personenbezogener Daten grundsätzlich unzulässig und lediglich bei Vorliegen eines der Ausnahmetatbestände, die abschließend in § 11 KDG geregelt sind, erlaubt. Dies entspricht auch den restriktiven Vorgaben der DSGVO im staatlichen Bereich.

„Mit dem neuen Gesetz werden neue Begriffe … eingeführt, die „implementierte Krankenhausseelsorge" … und die „nicht implementierte Krankenhausseelsorge" …"

Mit dem neuen Gesetz werden neue Begriffe in die Krankenhausseelsorge eingeführt, die „implementierte Krankenhausseelsorge" gemäß § 3 Seelsorge-PatDSG und die „nicht implementierte Krankenhausseelsorge" nach § 4 Seelsorge-PatDSG. Diese Unterscheidung der Formen der Seelsorge waren in den bisherigen Regelungen nicht vorgesehen. Die Gesetzgeber der neuen Bestimmungen lösen sich von den bisher geltenden Vorgaben in den PatDSO und erwarten von den Verantwortlichen in den Krankenhäusern die Realisierung bestimmter Modelle der Krankenhausseelsorge, damit dort die mit den neuen Regelungen verbundenen Möglichkeiten des Datenaustauschs genutzt werden können.

Für die Anwendung von § 3 Seelsorge-PatDSG ist erforderlich, dass der Krankenhausseelsorger in das Behandlungsteam des jeweiligen Patienten eingebunden wird. Dazu bedarf es eines klar ausgearbeiteten Konzepts der implementierten Seelsorge. Auf diese Situation muss im Rahmen des Behandlungsvertrags in geeigneter Weise hingewiesen werden, damit der Patient eine den datenschutzrechtlichen Anforderungen entsprechende informierte und freiwillige Einverständniserklärung abgeben kann. Krankenhäuser, die von den neuen Möglichkeiten Gebrauch machen wollen, sind gefordert, die erforderlichen Konzeptionen zu erarbeiten und die nach dem Gesetz notwendigen Anforderungen zu erfüllen. Dazu sollte jeder Verantwortliche eine Risikobewertung vornehmen und dies auch im Rahmen seiner Datenschutz-Folgenabschätzung dokumentieren.

Sofern in einem Krankenhaus keine implementierte Seelsorge nach § 3 Seelsorge-PatDSG eingerichtet ist, versucht der Gesetzgeber mit der Einführung einer nicht implementierten Seelsorge gemäß § 4 Seelsorge-PatDSG auch Seelsorgeangebote zu berücksichtigen, die nicht in der nach § 3 Seelsorge-PatDSG gebotenen Weise in die Strukturen

des Krankenhauses eingegliedert sind. Das Gesetz sieht vor, dass dann bestimmte in der Vorschrift aufgeführte Informationen in zulässiger Weise an die Seelsorger weitergegeben werden können. Der Patient muss in diesem Zusammenhang eine Aufklärung über die Freiwilligkeit der Angabe der Religion oder Konfession und über die Folgen seiner Angabe zum Zwecke der Seelsorge erhalten.

Mit § 5 Seelsorge-PatDSG wurde eine klarstellende Regelung eingeführt, wonach eine ausdrückliche Einwilligung des Patienten erforderlich ist, um die in der Vorschrift genannten Daten an die Heimat-Kirchengemeinde übermitteln zu dürfen. Damit wird der Selbstverantwortung des Patienten Rechnung getragen und diesem die Möglichkeit verschafft, sein Recht auf informationelle Selbstbestimmung wahrnehmen zu können. Die bloße Angabe der Religion beziehungsweise Konfession im Behandlungsvertrag genügt nicht als Nachweis einer Einwilligung des Patienten. Eine Datenübermittlung an die Heimat-Kirchengemeinde ohne den Willen des Patienten sollte damit ausgeschlossen sein.

1.3.3 Ordnung für das Verfahren zur Anerkennung des Leids

In den Vollversammlungen der Deutschen Bischofskonferenz im Jahr 2020 waren überarbeitete Grundsätze für die Weiterentwicklung des Verfahrens zur Anerkennung des Leids beraten und verabschiedet worden. Am 04.11.2020 wurde die Ordnung für das Verfahren zur Anerkennung des Leids verabschiedet, die zum 01.01.2021 in den (Erz-)Diözesen in Kraft getreten ist. Die aktuelle Fassung enthält die Änderungen des Ständigen Rats der Deutschen Bischofskonferenz vom 06.04.2021. Die Ordnung löst die zuvor geltenden Regelungen zum Verfahren zu Leistungen in Anerkennung zugefügten Leids ab.

Die Ordnung regelt die Aufgaben und die Zusammensetzung der Unabhängigen Kommission für Anerkennungsleistungen und deren Geschäftsstelle sowie die zugehörige Arbeitsweise und das Verfahren. In Ziffer 14 der Ordnung wird explizit festgelegt, dass es sich bei der Ordnung um ein bereichsspezifisches Gesetz handelt, das dem Gesetz über den Kirchlichen Datenschutz, aber auch der Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche (KAO) vorgeht, sofern deren Datenschutzniveau nicht unterschritten wird. Weiterhin wird ausdrücklich festgelegt, dass im Übrigen das KDG, die zu seiner Durchführung erlassene Ordnung (KDG-DVO) sowie die KAO gelten.

Als besondere Vorgabe, die im Zusammenhang mit Verfahren zur Anerkennung des Leids zu beachten ist, regelt Ziffer 14 Abs. 2 der Ordnung, dass personenbezogene Daten der Betroffenen aus Anträgen nur verarbeitet werden dürfen, wenn diese ausdrücklich mittels einer schriftlichen Einwilligung in die Verarbeitung der personenbezogenen Daten und der besonderen Kategorien personenbezogener Daten zum Zwecke der Antragsbearbeitung und der Erfüllung der Aufgaben der Unabhängigen Kommission für Anerkennungsleistungen eingewilligt haben.

1.3.4 Evaluation des Gesetzes über den Kirchlichen Datenschutz

Das Gesetz über den Kirchlichen Datenschutz enthält in seinem § 58 Abs. 2 die Vorgabe, dass das Gesetz innerhalb von drei Jahren ab Inkrafttreten überprüft werden soll. Der Verband der Diözesen Deutschlands hat innerhalb dieser Frist eine Arbeitsgruppe eingerichtet, die sich mit der Evaluation des KDG befasst. Diese Arbeitsgruppe hat ihre Tätigkeit aufgenommen, wobei im Berichtszeitraum die Bewertungen des Gesetzes noch nicht abgeschlossen werden konnten.

1.4 Gesetzgeberische Entwicklungen in der Evangelischen Kirche in Deutschland

Aus dem Bereich der Evangelischen Kirche in Deutschland (EKD) sind im Berichtszeitraum die folgenden zwei Gesetzgebungsvorhaben aus datenschutzrechtlicher Sicht interessant.

1.4.1 Die Aufarbeitungsverordnung der EKD

Die Evangelische Kirche hat durch eine „Gesetzesvertretende Verordnung des Rates der Evangelischen Kirche in Deutschland zur Änderung des EKD-Datenschutzgesetzes und dienstlicher Regelungen zum Zweck der institutionellen Aufarbeitung sexualisierter Gewalt (Aufarbeitungsverordnung – AVO)“ vom 24.07.2021 neue Begriffsbestimmungen im Datenschutz festgelegt und rechtliche Grundlagen für die Verarbeitung personenbezogener Daten im Rahmen der institutionellen Aufarbeitung sexualisierter Gewalt geschaffen. Diese Gesetzesvertretende Verordnung ist als Artikelregelung beschlossen worden und ändert das EKD-Datenschutzgesetz (DSG-EKD), das Pfarrerdienstgesetz der EKD, das Kirchenbeamtengesetz der EKD und das Disziplinargesetz der EKD. Datenschutzrechtlicher Schwerpunkt der Verordnung ist die Einfügung eines neuen § 50a in das DSG-EKD.

Hintergrund der Änderungen ist das von der Synode der EKD beschlossenen Vorhaben, eine externe wissenschaftliche Studie zum Komplex der sexualisierten Gewalt durchführen zu lassen, sowie das von Rat und der Kirchenkonferenz auf der Basis des Synodenbeschlusses konzipierte und beschlossene Forschungsprojekt zur wissenschaftlichen Aufarbeitung sexualisierter Gewalt in Kirche und Diakonie. Im Rahmen dieses Projekts sollen auch Einsichtnahmen in Personalakten vorgenommen werden. Vorbereitend hatte das Kirchenrechtliche Institut der EKD ein Gutachten zu der Frage erstellt, ob die bestehenden Regelungen ausreichend wären, um dem Anliegen Rechnung zu tragen. Im Ergebnis wurde der Bedarf an sicheren Rechtsgrundlagen und damit an einer spezialgesetzlichen Regelung gesehen. Wegen des beabsichtigten Beginns der geplanten Untersuchungen wurde dazu nicht der zeitlich längere Weg über ein synodales Kirchengesetz, sondern über eine gesetzesvertretende Verordnung gemäß Art. 20 Abs. 2 GO-EKD (Grundordnung der EKD) gewählt.

Die Verordnung beinhaltet eine Definition der institutionellen Aufarbeitung sexualisierter Gewalt in einem neuen § 4 Nr. 22 DSG-EKD, die dann in den weiteren Vorschriften vorausgesetzt wird.

Weiterhin enthält die Verordnung Ergänzungen aufgrund der erforderlichen Verweise, die sich aus der Einführung des § 50a DSG-EKD ergeben.

1.4.2 Der § 50a DSG-EKD als Rechtsgrundlage für die Missbrauchsaufarbeitung

Den Schwerpunkt der Aufarbeitungsverordnung[13] stellt die Einführung des § 50a DSG-EKD „Verarbeitung personenbezogener Daten zur institutionellen Aufarbeitung sexualisierter Gewalt" dar.

§ 50a Abs. 1 DSG-EKD erlaubt zunächst grundsätzlich die Verarbeitung personenbezogener Daten zum Zweck der institutionellen Aufarbeitung sexualisierter Gewalt. Dabei legt der Gesetzgeber fest, dass an der institutionellen Aufarbeitung sexualisierter Gewalt ein überragendes kirchliches Interesse besteht. Für mögliche Abwägungen schafft der Gesetzgeber somit bereits ein starkes Gewicht zugunsten einer Datennutzung für die Aufarbeitung.

Das Bestreben des Gesetzgebers, personenbezogene Daten für die Aufarbeitung zur Verfügung stellen zu können, verdeutlicht der nachfolgende § 50a Abs. 2 DSG-EKD. Nach dieser Vorschrift ist eine Offenlegung von Daten im Zusammenhang mit der institutionellen Aufarbeitung ausdrücklich ohne Einwilligung der Betroffenen zulässig. Voraussetzung dabei ist, dass Empfänger dieser Daten Wissenschaftler oder aber Beauftragte von zuständigen kirchlichen Stellen sind. Dabei wird nicht verlangt, dass diese Personen im Rahmen einer wissenschaftlichen Forschungsarbeit tätig werden, wohl aber müssen sie ein Datenschutzkonzept vorlegen.

Sofern im Zusammenhang mit der institutionellen Aufarbeitung Veröffentlichungen erfolgen sollen, ist dies gemäß § 50a Abs. 4 DSG-EKD zulässig, sofern die in der Vorschrift genannten Voraussetzungen erfüllt sind. Dabei bedarf es in jedem Fall der Zustimmung derjenigen Stelle, welche die Daten offengelegt hat. Für den Verfahrensablauf im Rahmen der Genehmigung hat der Gesetzgeber eine verpflichtende Anhörung der betroffenen Person vorgesehen. Die verwendeten Formulierungen lassen der entscheidenden Stelle keine Spielräume, wenn die in den Ziffern 1 und 2 des § 50a Abs. 4 DSG-EKD aufgeführten Voraussetzungen erfüllt sind. Ein starkes Korrektiv führt der Gesetzgeber insofern ein, als eine Einwilligung der betroffenen Person in die Veröffentlichung zu diesen Voraussetzungen gehört. Somit erhalten die Betroffenen von sexuellem Missbrauch durch § 50a Abs. 4 Nr. 2 DSG-EKD eine Entscheidungsmöglichkeit, die Veröffentlichung zu verhindern, wenn dies nicht ihren Vorstellungen entspricht. Allerdings sind von einer Veröffentlichung auch die Missbrauchstäter betroffen. Diese könnten nach dem Wortlaut des Gesetzes eine Veröffentlichung verhindern, es sei denn, bei ihnen würde es sich um eine Person der Zeitgeschichte im Sinne von § 50a Abs. 4 Nr. 1 DSG-EKD handeln.

[13] Siehe Abschnitt 1.4.1 dieses Berichts.

Der Gesetzgeber hat darauf verzichtet, mögliche Details im Gesetz selbst zu regeln. Stattdessen hat er in § 50a Abs. 5 DSG-EKD eine Ermächtigungsgrundlage geschaffen, die es dem Rat der Evangelischen Kirche in Deutschland erlaubt, durch Rechtsverordnung mit Zustimmung der Kirchenkonferenz nähere Regelungen zu erlassen.

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses

Im Berichtszeitraum hat sich der Europäische Datenschutzausschuss (EDSA) intensiv mit datenschutzrechtlichen und datenschutztechnischen Themen befasst. Nachstehend sind einige dieser Themen näher angesprochen.

1.5.1 Einige wenige Stichworte zur Arbeit des Europäischen Datenschutzausschusses im Jahr 2021

Der EDSA verabschiedete im Juli 2021 eine verbindliche Streitbeilegungsentscheidung auf der Basis von Art. 65 DSGVO in Bezug auf einen Streit zu einem Entscheidungsentwurf der irischen Datenschutzbehörde zu WhatsApp. Der EDSA stellte fest, dass das von WhatsApp IE verwendete Verfahren nicht zu einer Anonymisierung personenbezogener Daten von Nichtnutzern von WhatsApp führte. Darüber hinaus äußerte sich der EDSA zu der Berechnung von Bußgeldern und den dabei einzubeziehenden Grundlagen.

Weiterhin hat der EDSA im Berichtszeitraum weitere Leitlinien verabschiedet.[14] Diese betrafen u. a. Verhaltenskodizes (Codes of Conduct) als Instrument für Übertragungen, virtuelle Sprachassistenten, die Begriffe „Auftragsverarbeiter" und „Verantwortlicher" sowie Hilfestellungen für die Klärung der Frage, wann eine internationale Übermittlung vorliegen kann.

Der EDSA hat auf einer seiner Plenartagungen nach einer vorhergehenden öffentlichen Konsultation Empfehlungen zu ergänzenden Maßnahmen angenommen, die eine Unterstützung für die Verantwortlichen bieten sollen, um ein im Wesentlichen gleichwertiges Datenschutzniveau bei von ihnen in ein Drittland übermittelten Daten gewährleisten zu können.

Auch hat der EDSA eine Taskforce gemäß Art. 70 Abs. 1 lit. u) DSGVO eingerichtet, die sich mit Cookie-Bannern befassen soll. Sie dient dem Gedankenaustausch über rechtliche Analysen und mögliche Verstöße, der Unterstützung von Tätigkeiten auf nationaler Ebene sowie der Optimierung von Kommunikation der Datenschutzaufsichten. Die Taskforce soll weiterhin der Reaktion auf die Beschwerden über Cookie-Banner dienen, die von der NOYB, der unter anderem von Max Schrems gegründeten Nichtregierungsorganisation, bei verschiedenen Datenschutzaufsichten eingereicht worden waren.

[14] Die Leitlinien können – ebenso wie Pressemitteilungen und weitere Materialien des Europäischen Datenschutzausschusses – über dessen Internetseite (https://edpb.europa.eu) abgerufen werden.

1.5.2 Eine Reaktion auf Schrems II: Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (Empfehlungen 01/2020 des Europäischen Datenschutzausschusses)

Im Sommer 2020 urteilte der EuGH in dem Verfahren C-311/18 („Schrems II") unter anderem, dass eine Datenübertragung in ein Drittland nach den Bestimmungen der DSGVO nur dann erfolgen darf, wenn sie sich auf ein Übermittlungsinstrument nach Art. 46 DSGVO stützt, sofern für das empfangende Land kein Angemessenheitsbeschluss der EU-Kommission vorliegt und auch kein Ausnahmetatbestand nach Art. 49 DSGVO greift.[15]

Bei der Anwendung eines Übermittlungsinstrumentes, zu denen u. a. die Standardvertragsklauseln oder auch genehmigte verbindliche Unternehmensrichtlinien zählen, muss der Datenexporteur in jedem Einzelfall ggf. in Zusammenarbeit mit dem Datenimporteur prüfen, ob sich die im Übertragungsinstrument vereinbarten Schutzmechanismen im Geltungsbereich der Gesetzgebung des Empfängerlandes sowie dessen behördlicher Praxis auch wirklich effektiv umsetzen lassen. Falls es an der effektiven Umsetzung begründete Zweifel gibt, sind zusätzliche Maßnahmen zu treffen, die die Schutzmechanismen wirksam unterstützen und die Sicherheitslücken schließen.

Der Europäische Datenschutzausschuss veröffentlichte im Juni 2021 die Empfehlungen 01/2020 mit dem Ziel, die Forderung des EuGH nach einer Analyse der tatsächlichen Umstände eines jeden Datentransfers in Drittländer, der mit Instrumenten des Art. 46 DSGVO durchgeführt wird, zu systematisieren und in praktische Beispiele zu übersetzen und damit den Datenexporteuren Hilfen an die Hand zu geben.

In der Empfehlung wird besonders auf die Regeln und Verfahren des behördlichen Handelns im Drittland abgestellt. Dem Datenexporteur wird eindringlich nahegelegt, anhand der Gesetzgebung im Drittland und des dortigen behördlichen Vorgehens zu bewerten, ob die Schutzwirkungen der Übertragungsverfahren nach Art. 46 DSGVO (z. B. Standardvertragsklauseln oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules)) tatsächlich effektiv umsetzbar und durchzuhalten sind. Es wird u. a. konkretisiert, dass der behördliche Zugriff eines Drittlandes auf die übertragenen Daten sowohl im Laufe der Übertragung („in transit by accessing the lines of communication") als auch in Ruhe („while in custody of an intendent recipient") vorstellbar ist.

Ergänzende Maßnahmen zur Absicherung der Übertragungsverfahren sind nach technischen, zusätzlichen vertraglichen und organisatorischen Maßnahmen unterteilt. Im Abschnitt der technischen Maßnahmen werden Fallbeispiele („Use Cases") beschrieben und nach solchen, „in denen wirksame Maßnahmen gefunden werden können" und solchen, „in denen keine wirksame Maßnahme gefunden wurde" unterteilt. In den beiden weiteren Abschnitten werden vertragliche und orga-

[15] In dem Jahresbericht 2020 des Katholischen Datenschutzzentrums wurde das Urteil bereits ausführlich thematisiert (siehe dort Abschnitt 2.1.1 und 3.2 ff).

nisatorische Maßnahmen beschrieben, die je nach Gesetzeslage im Empfängerland wirksam sein können.

Zu den wirksamen technischen Maßnahmen gehört eine starke Verschlüsselung sowohl der ruhenden als auch der fließenden Daten, sofern die Schlüssel nur den Berechtigten bekannt sind. Ebenso kann eine Pseudonymisierung oder eine getrennte Verarbeitung („split processing" beziehungsweise „multi-party-processing") eine wirksame Schutzmaßnahme sein. Die Wirksamkeit der Schutzmaßnahmen stößt an ihre Grenzen, wo ein Zugriff auf Klardaten für die Verarbeitung im Drittland funktional notwendig ist, etwa zur Indizierung von Datenbeständen oder zur Ermittlung von Kommunikationsadressen. Dieses Fallbeispiel ist von großer Relevanz, da es dem typischen Szenario eines Software-as-a-Service (SaaS)-Anbieters für Office- und Kollaborationsanwendungen entspricht.

„Zu den wirksamen technischen Maßnahmen gehört eine starke Verschlüsselung … Ebenso kann eine Pseudonymisierung oder eine getrennte Verarbeitung … eine wirksame Schutzmaßnahme sein."

Zu den vorgeschlagenen vertraglichen Maßnahmen gehört z. B. die Verpflichtung des Datenempfängers im Drittland, den Datenexporteur nach bestem Wissen über die Gesetze und Regularien und/oder die tatsächlichen behördlichen Verfahren (auch ohne gesetzliche Grundlagen) zu informieren, denen er hinsichtlich der Datenübertragung und des potentiellen Zugriffs von Behörden in seinem Land auf die übertragenen Daten unterliegt. Eine andere Maßnahme könnte unter bestimmten Voraussetzungen die Verpflichtung des Importeurs sein, jede Aufforderung einer Behörde zur Offenlegung von Daten mit allen legalen Mitteln anzufechten und zu verzögern und parallel den Datenexporteur über die Aufforderung der Behörde zu informieren.

Unter den möglichen zusätzlichen organisatorischen Maßnahmen werden eine transparente und nachweisbare Dokumentation von Behördenanfragen sowie der Reaktion des Datenimporteurs und regelmäßige Veröffentlichungen dieser Dokumentationen genannt.

Konsequenz für Einrichtungen der katholischen Kirche

Der Themenbereich der Datenübertragung in Drittländer ist im KDG kompakt in den §§ 39–41 KDG ausgeführt. In der täglichen Arbeit der kirchlichen Einrichtungen spielen diese Fragen aber eine große Rolle. Auch die kirchlichen Einrichtungen beziehen viele Arten von IT-Dienstleistungen, die mit bewussten oder unbewussten Datenübermittlungen (auch von personenbezogenen Daten!) in Drittländer verknüpft sind. Hier können die Regelungen des Kapitels V der DSGVO als Auslegungshilfe herangezogen werden, wenn die Vorschriften des KDG auslegungsbedürftig erscheinen.

Die kirchlichen Einrichtungen sind deshalb gut beraten, sich bei allen Projekten zur Einführung einer Datenverarbeitung, die eine Datenübertragung in Drittländer vorsieht, an den Vorgaben der DSGVO beziehungsweise der Empfehlungen 01/2020 des EDSA zu orientieren.

1.6 40 Jahre Konvention Nr. 108 des Europarates

Im Berichtszeitraum jährt sich die Verabschiedung der Konvention „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108)" zum vierzigsten Mal.

Am 28.01.1981 wurde dieses Übereinkommen zwischen den seinerzeitigen Mitgliedstaaten des Europarates vereinbart. Die Konvention wurde am 19.06.1985 durch die Bundesrepublik Deutschland ratifiziert und trat am 01.10.1985 in den Staaten, die bis zu diesem Zeitpunkt unterzeichnet hatten, in Kraft. Mit dem Übereinkommen wurde ein erster bedeutender völkerrechtlich verbindlicher Vertrag zum Schutz vor einem Missbrauch personenbezogener Daten geschlossen. Der Einzelne sollte vor einem Missbrauch seiner Daten im Zusammenhang mit elektronischen Verarbeitungen geschützt werden. Zugleich wurde eine Regelung zur grenzüberschreitenden Übermittlung personenbezogener Daten getroffen. Die Unterzeichnerstaaten der Konvention hatten eine zunehmende Übermittlung automatisiert verarbeiteter personenbezogener Daten im Zusammenhang mit grenzüberschreitendem Verkehr festgestellt. Mithilfe der Datenschutz-Konvention 108 wollten diese Staaten sicherstellen, dass die Rechte und Grundfreiheiten für jedermann im Hoheitsgebiet der Vertragsstaaten geschützt würden, insbesondere das Recht auf einen Persönlichkeitsbereich bei der automatischen Verarbeitung personenbezogener Daten. Im Jahr 2001 wurde ein ergänzendes Zusatzprotokoll vereinbart und die Konvention am 08.11.2001 um das „Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr" erweitert, welches in Deutschland am 01.07.2004 in Kraft trat. In Anbetracht der fortschreitenden Entwicklungen im Datenaustausch und auf der technischen Seite begannen die Vertragsstaaten im weiteren Verlauf mit den Verhandlungen über eine Anpassung und Modernisierung der Konvention. Nach mehrjährigen Beratungen erfolgte dann eine Erweiterung der Konvention durch ein Änderungsprotokoll, welches im Jahr 2018 zur Signatur durch die beteiligten Staaten freigegeben wurde. Dieses beinhaltete eine Stärkung der Betroffenenrechte, die Verpflichtung zur Schaffung von unabhängigen Datenschutzaufsichtsbehörden sowie Meldepflichten bezüglich der Verletzungen des Datenschutzes an die zuständigen Aufsichtsbehörden.

Eine besondere Bedeutung des Übereinkommens liegt darin, dass erstmalig in einer Vereinbarung von der Bedeutung und der Reichweite der Datenschutz-Konvention grundlegende Datenschutzprinzipien für die automatisierte Verarbeitung personenbezogener Daten festgelegt wurden, so z. B. die Grundsätze der Zweckbindung, der Erforderlichkeit, der Datenverarbeitung nach Treu und Glauben oder des Informationsanspruchs von Betroffenen sowie die Forderung nach geeigneten Sicherungsmaßnahmen bei der Verarbeitung personenbezogener Daten.

Das Übereinkommen enthält Garantien und Vorgaben für die Verarbeitung personenbezogener Daten auf Computern. Darüber hinaus kategorisiert die Konvention bestimmte Daten als besondere Arten von Daten – wie Daten über rassische Herkunft, politische Anschauung,

religiöse Überzeugung, Gesundheit, Sexualleben, Strafurteile – und erlaubt deren automatische Verarbeitung nur, sofern das innerstaatliche Recht einen geeigneten Schutz gewährleistet.

Das Übereinkommen sieht ferner Individualrechte vor, auf die sich ein Berechtigter berufen kann, um die zu seiner Person gespeicherten Informationen zu erfahren, verbunden mit der Möglichkeit, Berichtigungen oder Löschungen einzufordern.

Der Schutz dieser Daten wird in dem Übereinkommen als so bedeutsam angesehen, dass die vereinbarten Rechte nur eingeschränkt werden können, wenn wichtige Staatsinteressen betroffen sind, wie z. B. öffentliche Sicherheit oder Erwägungen der Landesverteidigung.

Eine wesentliche Regelung stellt die Vorgabe dar, dass im Fall der Übermittlung in Staaten, in denen es keinen vergleichbaren Schutz personenbezogener Daten wie in den Unterzeichnerstaaten gibt, der grenzüberschreitende Datenverkehr eingeschränkt werden kann. Gleichzeitig wird mit der Konvention aber versucht, den grenzüberschreitenden Datenverkehr nicht zu sehr zu behindern, sondern zu ermöglichen.

Die Datenschutz-Konvention 108 des Europarates und ihre Fortentwicklungen zeigen sich als wesentliche Schritte auf dem Weg zu dem Datenschutz, der derzeit besteht und aktuell durch die Datenschutz-Grundverordnung und die vergleichbaren kirchlichen Datenschutzgesetze geprägt wird.

1.7 Aus der Rechtsprechung der Datenschutzgerichte der katholischen Kirche

In der Entscheidung vom 01.03.2021 (Az. IDSG 27/2020) des Interdiözesanen Datenschutzgerichts (IDSG) ging es um die Einsichtnahme in Gottesdienst-Besucherlisten innerhalb der Corona-Pandemie, als dies noch durch die Coronaschutzverordnung NRW vorgeschrieben war.

Die Beschwerdeführer hatten sich an das Katholische Datenschutzzentrum gewandt, da sie der Ansicht waren, dass der leitende Pfarrer unberechtigt in die Gottesdienst-Besucherlisten geschaut beziehungsweise diese mit der (nicht durch die Verordnung vorgegebene) vorherige Anmeldeliste abgeglichen habe. Die Beschwerdeführer sahen sich dabei in ihrem Persönlichkeitsrecht verletzt, da sie die Angaben ihrer personenbezogenen Daten nur aufgrund der Registrierungspflicht getätigt hätten und eine Einsichtnahme (außer zur Benachrichtigung im Falle eines Corona-Kontaktes) nicht erforderlich gewesen sei.

Das IDSG entschied in dieser Sache, welche als eilbedürftig eingestuft wurde, dass die Einsichtnahme durch den Pfarrer nicht gegen datenschutzrechtliche Bestimmungen verstößt, sondern durch § 6 Abs. 1 lit. a) und d) KDG in Verbindung mit der damals gültigen Fassung der Coronaschutzverordnung NRW gedeckt sei. Die Argumentation, dass eine Kontrolle der erfassten Daten nicht von dem Verordnungsgeber intendiert sei und gerade der neu geschaffene § 28 Abs. 4 IfSG gegen diese erfolgte Einsichtnahme spricht, wurde von dem Gericht nicht so bewertet, wie von dem Katholischen Datenschutzzentrum innerhalb

des Beschwerdeverfahrens. Dies spiegelt sich vor allem in der zweitinstanzlichen Entscheidung des Datenschutzgerichts der Deutschen Bischofskonferenz wider (vgl. DSG-DBK 01/2021), welches aufgrund der Beschwerde des Katholischen Datenschutzzentrums entschieden hatte.

Da die Pflicht zur Kontaktnachverfolgung in der Corona-Pandemie zwischenzeitlich aufgehoben wurde, ist die Rechtsfrage, inwiefern das Einsehen von entsprechenden Listen von Erlaubnisnormen des KDG gedeckt sein kann, zunächst nicht mehr von Relevanz. Abzuwarten ist, wie damit umgegangen wird, wenn es erneut eine vergleichbare Pflicht zur Datenerfassung im Laufe der Pandemie geben sollte.

Positiv zu erwähnen ist jedoch, dass das IDSG in dieser Sache innerhalb von 3 Monaten entschieden hat. Gerade aufgrund der damals aktuellen Rechtsfrage und der Vorbildfunktion für andere Pfarreien war diese Entscheidungszeit sehr zu begrüßen. Auch wenn es in der Kirchlichen Datenschutzgerichtsordnung (KDSGO) keine normierten Eilverfahren gibt und ein solcher Antrag in der Vergangenheit schon als unzulässig abgewiesen worden ist (vgl. IDSG 09/2019 – nicht mehr abrufbar), zeigt sich durch dieses Verfahren, dass aufgrund von tatsächlich bestehender Eilbedürftigkeit, eine schnellere Entscheidung herbeigeführt werden kann.

2 Aus der Tätigkeit des Datenschutzzentrums

Bei den Eingaben an das Katholische Datenschutzzentrum nahmen im Berichtszeitraum die Meldungen von Datenschutzverletzungen den zahlenmäßig größten Block ein. Auch wenn die Anfragen und Beschwerden beziehungsweise Hinweise von der Zahl her hinter den Meldungen zurückbleiben, so sind sie in der Bearbeitung der einzelnen Vorgänge sehr oft zeitaufwendiger.

2.1 Corona – auch im zweiten Jahr noch datenschutzrechtliche Fragen

Aufgrund der dynamischen Entwicklung der Pandemiesituation hat der Gesetzgeber auch im zweiten Jahr der Pandemie mehrfach mit geänderten Regelungen reagiert.[16] Daher waren auch im Berichtszeitraum immer wieder datenschutzrechtliche Fragen zum pandemiebedingten Umgang mit personenbezogenen Daten zu beantworten.

2.1.1 Impfnachweis im Arbeitsverhältnis[17]/Testnachweis

Der Umgang mit Impf- und Testnachweisen zu Covid-19 führte in 2021 zu zahlreichen Anfragen, Meldungen und auch einigen Beschwerden. Insbesondere die Anfertigung von Impfnachweiskopien war Gegenstand von Beschwerden.

Bei der Abfrage des Impfstatus von Mitarbeitenden geht es um die Verarbeitung personenbezogener Daten der besonderen Kategorie in Form

[16] Siehe hierzu auch Abschnitt 1.2.3 dieses Berichts.

[17] Anmerkung: Für den Zeitraum des Berichts (2021) findet die sog. „Partielle Impfpflicht" aus § 20a IfSG keine Berücksichtigung, da diese erst zum 15.03.2022 ihre Regelungswirkung entfaltet hat.

von Gesundheitsdaten (vgl. § 4 Nr. 2, 17 KDG). Diese unterliegen einem erhöhten Schutzniveau und ihre Verarbeitung ist gemäß § 11 Abs. 1 KDG grundsätzlich unzulässig.

Ausnahmen ergeben sich allerdings etwa in Bereichen der Gesundheitsvorsorge. Gemäß § 23a Satz 1 Infektionsschutzgesetz ist es Dienstgebern erlaubt, den Impfstatus ihrer Mitarbeitenden zu erfragen, wenn es sich um ein Beschäftigungsverhältnis im Gesundheitswesen (vgl. § 23 Abs. 3 IfSG) handelt. Auch aufgrund von § 28b IfSG a. F. konnten die Nachweise kontrolliert werden. Wobei der Arbeitgeber nach § 28b Abs. 3 IfSG a. F. jedoch nur zur Überwachung und Dokumentation der Nachweiskontrollen verpflichtet war. Eine Pflicht zum Vorhalten von Nachweiskopien war hingegen nicht ausdrücklich geregelt. Gleichwohl waren die Arbeitgeber und Beschäftigten nach Absatz 1 weiterhin verpflichtet, ihren gültigen 3G-Nachweis beim Betreten der Arbeitsstätte mit sich zu führen, zur Kontrolle verfügbar zu halten oder bei dem Arbeitgeber hinterlegt zu haben.

Unter anderem der Grundsatz der Datenminimierung aus § 7 Abs. 1 lit. c) KDG ist im Zuge der Verarbeitung von Impfnachweisen zu beachten. Danach müssen die personenbezogenen Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Aus der Sicht des KDSZ steht dieser Grundsatz einer generellen Vorhaltung der Nachweise in Kopie entgegen. Neben der Datenminimierung sind und waren die übrigen datenschutzrechtlichen Schutzmaßnahmen selbstverständlich ebenfalls einzuhalten.

Auch beschäftigten einige Anfragen zum Thema des Impfquoten-Monitorings das KDSZ. In diesem Zuge bestanden insbesondere datenschutzrechtliche Bedenken hinsichtlich der Datenübermittlung an Kommunen und kassenärztliche Vereinigungen und dem Vorliegen einer entsprechenden Rechtsgrundlage für diese Übermittlung.

Darüber hinaus gingen Meldungen dazu ein, dass im Bereich der Corona-Testungen Ergebnisse und andere personenbezogene Daten fehlerhaft versandt oder anderweitig offengelegt wurden.[18]

2.1.2 Zweckbindung von im Zusammenhang mit Corona erhobenen Daten

Der Grundsatz der Zweckbindung bei der Verarbeitung personenbezogener Daten, der in § 7 Abs. 1 lit. b) KDG gesetzlich verankert ist, ist eines der tragenden Prinzipien des Datenschutzes.

Dieser Grundsatz gilt auch für die Verarbeitungen der personenbezogenen Daten aus Anlass der Corona-Pandemie. Dies betrifft einmal die eigentliche Verarbeitung zu Pandemiezwecken, die gesetzlich normiert sein muss, es betrifft aber auch Verarbeitungen der einmal erhobenen Daten zu anderen Zwecken, als ursprünglich vom jeweiligen Gesetz vorgesehen.

[18] Vgl. hierzu auch Abschnitt 2.6.1 dieses Berichts.

So gab es vereinzelt Überlegungen, wie die Corona-bedingt erhobenen Daten auch noch anderweitig verarbeitet und damit genutzt werden könnten. Diese Überlegungen scheiterten zumeist an der strengen Zweckbindung, die der Gesetzgeber bei der Verarbeitung der Daten aus Anlass der Pandemie selbst in die Gesetze geschrieben hatte oder eine gesetzeskonforme Zweckänderung der Daten konnte nicht nachgewiesen werden.[19]

2.1.3 Die Luca-App

In der Corona-Pandemie im Jahr 2021 wurde in vielen Bundesländern neben der vom Bund betriebenen Corona-Warn-App die Luca-App eines privaten Anbieters als Kontaktnachverfolgungs-App lizenziert. Die Corona-Warn-App hatte zunächst keine Möglichkeit einer Kontaktnachverfolgung und wurde erst später im Jahr 2021 dahingehend erweitert.

Die Nutzung dieser App als Alternative zu der Erfassung der notwendigen Daten der Kunden und Gäste auf Papierbögen war eine Erleichterung für die Kunden beziehungsweise Gäste und die Einrichtungen beziehungsweise Unternehmen. In ihrer Stellungnahme vom 26.03.2021[20] weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aber darauf hin, dass auch diese elektronischen Verfahren zur Erfassung der Kontakt- und Anwesenheitsdaten datenschutzrechtlich korrekt verarbeitet werden müssen. Dazu gehört nach Ansicht des Europäischen Datenschutzausschusses und der DSK auch, dass die Nutzung der digitalen Werkzeugen für die Kontaktnachverfolgung in jedem Fall freiwillig sein muss, um das Risiko der Diskriminierung bei der Teilnahme am gesellschaftlichen Leben zu vermeiden und eine hohe Kooperationsbereitschaft zu fördern.

Bei der Nutzung dieser oder anderer, vergleichbarer Apps ist darauf zu achten, dass die Zweckbindung der erhobenen Daten eingehalten wird und die Daten solcher Apps nicht für andere Zwecke als die Kontaktnachverfolgung bei einer Infektion verwendet werden.[21]

„Bei der Nutzung dieser … Apps ist darauf zu achten, dass die Zweckbindung der erhobenen Daten eingehalten wird …“

[19] Über ein Beispiel einer unzulässigen Verarbeitung aus dem nicht-kirchlichen Bereich berichtete der SWR: Demnach hatte die Mainzer Polizei für Ermittlungen ohne rechtliche Grundlage auf Daten der Luca-App zugegriffen. Anlass war ein Vorfall, bei dem ein Mann nach dem Verlassen einer Gaststätte schwer stürzte und bevor er im Krankenhaus befragt werden konnte, an den Verletzungen aufgrund des Sturzes verstarb. Die Polizei fragte im Rahmen der Zeugenfindung eine Mitarbeiterin der Gaststätte ausdrücklich nach den Daten aus der Luca-App. Die Mitarbeiterin wurde daraufhin vom Gesundheitsamt gebeten, die Daten der Gäste für den betreffenden Abend freizugeben. Die Polizei ermittelte 21 Gäste als mögliche Zeugen und kontaktierte diese. Die Staatsanwaltschaft Mainz hat sich nach Bekanntwerden dieser Sache bei den betroffenen Personen für den unzulässigen Zugriff auf die Daten entschuldigt. Die Staatsanwaltschaft erklärte, es habe für den Zugriff keine hinreichende rechtliche Grundlage gegeben. (vgl. https://www.swr.de/swraktuell/rheinland-pfalz/mainz/polizei-ermittelt-ohne-rechtsgrundlage-mit-daten-aus-luca-app-100.html).

[20] https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/dsk_stellungnahmen/DSK-Stellungnahme_20210326_final.pdf

[21] Siehe hierzu auch Abschnitt 2.1.2 dieses Berichts.

2.2 Das Kirchliche Datenschutzmodell

Auf dem ökumenischen Datenschutztag der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche und der Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland am 21.04.2021 wurde das Kirchliche Datenschutzmodell (KDM) verabschiedet und wird nun in die Arbeit der kirchlichen Datenschutzaufsichten einfließen.

In den letzten drei Jahren hat sich, auf der Grundlage eines entsprechenden Beschlusses der evangelischen und katholischen Datenschutzaufsichtsbehörden aus dem Jahr 2019, eine ökumenische Arbeitsgruppe intensiv mit der Übernahme des im staatlichen Bereich eingeführten Standard-Datenschutzmodells (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder befasst.

„Das Ergebnis ist das Kirchliche Datenschutzmodell, welches geeignete Mechanismen bietet, um die Anforderungen der kirchlichen Datenschutzgesetze in technische und organisatorische Maßnahmen zu überführen."

Die ökumenische Arbeitsgruppe hat dabei das SDM auf die in der katholischen und evangelischen Kirche geltenden Vorschriften unter Beibehaltung der Methodik der staatlichen Vorlage angepasst.

Das Ergebnis ist das Kirchliche Datenschutzmodell, welches geeignete Mechanismen bietet, um die Anforderungen der kirchlichen Datenschutzgesetze in technische und organisatorische Maßnahmen zu überführen. Das Katholische Datenschutzzentrum sieht in dem KDM ein Werkzeug, das sowohl den Datenschutzaufsichten als auch den kirchlichen Stellen und Einrichtungen Vorteile bringt.

Das KDG fordert, für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen, die nach dem Stand der Technik und nach dem Risiko der Rechte und Freiheiten natürlicher Personen erforderlich und angemessen sind.

Diese Maßnahmen sind im KDG jedoch nicht an einer Stelle gebündelt formuliert worden und weisen keinen einheitlichen Konkretisierungsgrad auf. Teilweise weisen die Normen bereits konkrete Vorgaben wie Transparenz, Datenminimierung und Zweckbindung vor. Manchmal müssen die Anforderungen aber erst aus den Rechten, Pflichten und sonstigen Vorgaben abgeleitet werden. Häufig ist daher ein Zwischenschritt von der Ableitung aus dem Gesetzestext zur eigentlichen Maßnahme erforderlich.

Mit dem KDM wird das Ziel verfolgt, aus den gesamten Regularien diejenigen rechtlichen Anforderungen systematisch herauszuarbeiten, die durch technische und organisatorische Maßnahmen zu erfüllen sind. Anschließend werden sie in sogenannten Bausteinen zu Referenzmaßnahmen thematisch zusammengefasst. Die Erstellung der Bausteine erfolgt schrittweise. Durch die Verwendung der in den Bausteinen standardisierten technischen und organisatorischen Maßnahmen soll eine einheitliche datenschutzrechtliche Beratungs- und Prüfpraxis erreicht werden.

Die ökumenische Projektgruppe „Kirchliches Datenschutzmodell (KDM)" hat in Fortführung ihrer Arbeit im Jahr 2021 den Baustein 41 „Planen und Spezifizieren" und den Baustein 62 „Einschränken der Verarbeitung" für den Referenzmaßnahmenkatalog des Kirchlichen Datenschutzmodells freigegeben. Damit stehen den Anwendern jetzt schon

acht Bausteine zur Verfügung, die bei der Ermittlung passender Maßnahmen zur Behandlung von erkannten Risiken bei neuen oder geänderten Verarbeitungstätigkeiten unterstützen.

Weitere Bausteine werden in unregelmäßiger Folge erstellt und freigegeben. Dabei folgt die Projektgruppe zeitnah den von der Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder angetriebenen Entwicklungen des Standard-Datenschutzmodells.

Die ökumenische Arbeitsgruppe unter der Leitung des Beauftragten für den Datenschutz der EKD und des Leiters des Katholischen Datenschutzzentrums wird die Arbeit fortsetzen und das Informationsangebot erweitern.

Alle weiteren Dokumente und Informationen zum KDM finden Sie auf der Website des Projektes:

https://www.kirchliches-datenschutzmodell.de/

2.3 Betroffenenrechte weiterhin im Fokus von Betroffenen und Aufsicht

Die Wahrung der Betroffenenrechte stellt einen wichtigen Teil der Aufgaben der datenverarbeitenden kirchlichen Stellen wie auch der Datenschutzaufsicht dar. In der Präambel zum KDG ist als Aufgabe des Datenschutzes festgeschrieben, „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten bei der Verarbeitung dieser Daten zu schützen". Ziel ist es in diesem Rahmen insbesondere dafür zu sorgen, dass die betroffenen Personen jederzeit „Herr" über ihre Daten sind. Um diesem Ziel gerecht zu werden, sieht das KDG umfassende Betroffenenrechte, aber auch Pflichten der Verantwortlichen vor.

Von den Betroffenen wird zumeist das Auskunftsrecht aus § 17 KDG geltend gemacht, um überhaupt einen Überblick bezüglich der Datenverarbeitung zu erhalten. Dieses und weitere Betroffenenrechte wurden bereits ausführlich im Jahresbericht 2020 besprochen.[22]

Zum Auskunftsrecht nach § 17 KDG beziehungsweise der korrespondierenden Regelung des Art. 15 DSGVO haben sich seit Geltung der neuen Regelungen 2018 auch die meisten Auslegungsfragen bei den Betroffenenrechten ergeben. So hatte im Juni 2021 jetzt auch der Bundesgerichtshof (BGH) zu den Voraussetzungen und der Reichweite des Auskunftsanspruchs zu entscheiden.[23]

Konkret lag der Entscheidung des BGH ein Sachverhalt zugrunde, in dem der Kläger gegenüber einem Versicherer Ansprüche auf Datenauskunft gemäß Art. 15 DSGVO geltend gemacht hatte. Die zwischenzeitlich übersandten Informationen hielt der Kläger für unvollständig. In den ersten beiden Instanzen hatte der Kläger keinen Erfolg bei der

[22] Siehe den Jahresbericht 2020, Abschnitt 3.4 ff.
[23] Urteil des BGH vom 15.06.2021, Az. VI ZR 576/19.

gerichtlichen Geltendmachung seiner Anträge. Der BGH hat die Revision in den Punkten, in denen er sie für zulässig erachtet hat, auch als begründet angesehen.

Mit seiner Entscheidung trifft der BGH auch Aussagen zum Begriff der personenbezogenen Daten. Unter Bezugnahme auf die Vorschriften der DSGVO sowie auf die Rechtsprechung des Gerichtshofs der Europäischen Union führt der BGH u. a. aus, dass dieser Begriff weit zu fassen ist. Nach dem Verständnis des Gerichts sind nicht nur sensible oder private Daten umfasst, sondern „potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt."[24] Eine Reduktion auf signifikante biografische Informationen zum Betroffenen lehnt der BGH unter Verweis auf den EuGH und Stimmen in der Literatur ab.

Darüber hinaus bestätigt der BGH die Niederschwelligkeit der Anforderungen an die Formulierungen des Auskunftsverlangens. Nach den Vorstellungen des BGH ist es für die Antragsteller nicht erforderlich, im Detail darzulegen, welche konkreten Daten Gegenstand der Auskunft sein sollen. Das Gericht lässt es ausreichen, dass eine vollständige Datenauskunft gefordert wird.

Die Entscheidung des BGH schärft den Blick auf altbekannte Datenschutzgrundsätze, wie vorliegend konkret u. a. auf die Datensparsamkeit. Dem von Verantwortlichen gern genutzten Argument, die vollständige Auskunftserteilung würde einen unverhältnismäßigen Aufwand erfordern, begegnet aus Sicht des Gerichts Bedenken, um als relevante Begründung für die Zurückweisung oder nur teilweise Beantwortung einer Anfrage akzeptiert werden zu können.

Ferner hält der BGH fest, dass Voraussetzung für eine berechtigte Erhebung und Speicherung von Daten die Beachtung der zugehörigen Zweckbindung ist. Keinesfalls sind Verantwortliche, wie hier im Entscheidungsfall die Versicherungsgesellschaft, berechtigt, anlasslos jedwede Information über eine bestimmte Person zu erheben und zu speichern.

Sofern die Zweckbindung beachtet wird, kann der Umfang der für die Beantwortung zusammenzustellenden Daten nicht so erheblich sein, als dass eine Zusammenführung der Daten durch den Verantwortlichen für diese Kompilation nicht leistbar wäre. Anderenfalls würde dieser nach den Ausführungen des Gerichts durch den Verweis auf den zu betreibenden Aufwand bei der Beantwortung des Auskunftsanspruchs signalisieren, dass er in weitergehendem Maße als dem zulässigen Umfang Daten über die auskunftsersuchende Person gespeichert hat.

Der BGH lässt in seiner Entscheidung deutlich erkennen, dass der nach Art. 15 DSGVO bestehende Auskunftsanspruch zu erfüllen ist. Dieser betrifft die vom Verantwortlichen verarbeiteten Daten des Anspruchstellers. Erfüllt ist dessen Auskunftsanspruch nach Auffassung des Gerichts dann, wenn die Angaben nach den Vorstellungen des Auskunftsersuchenden die mit der Auskunft erbetenen Informationen im geschuldeten Gesamtumfang darstellen. Dazu soll die erteilte Auskunft

[24] BGH, Urteil vom 15.06.2022, Az. VI ZR 576/19, Rz 22.

erkennen lassen, dass der Gegenstand des berechtigten Auskunftsbegehrens vollständig abgedeckt ist. Daran kann es fehlen, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt haben sollte.

Im konkreten Fall hat der BGH weiter ausgeführt, dass der Betroffene bezüglich der Verarbeitung seiner personenbezogenen Daten die Vorgehensweise des Verantwortlichen nachprüfen können muss. Dazu gehört, dass er auch über weitergehende Informationen, wie z. B. zwischen den Beteiligten geführte Korrespondenz, verfügen muss, um diesem Recht nachgehen zu können. Insbesondere wenn – wie im Entscheidungsfall – der Betroffene konkrete Bestandteile seines Auskunftsbegehrens formuliert und dem Verantwortlichen mitgeteilt hat, hat der Verantwortliche über diese Bereiche Auskunft zu geben. Insoweit kommt das Gericht zu dem Ergebnis, dass bei fehlender Berücksichtigung dieser Elemente der Anfrage nicht von einer vollständigen Auskunft gesprochen werden könne.

Bezüglich des Umfangs der Auskunftserteilung ist nach den Ausführungen des BGH zu beachten, dass nicht jede Information auch ein der Auskunft unterfallendes personenbezogenes Datum darstellt. So können – wie auch schon der EuGH festgestellt hat – in rechtlichen Analysen personenbezogene Daten enthalten sein, diese Analysen selbst oder die daraus resultierenden Beurteilungen der Rechtslage müssen keine Daten darstellen, die im Rahmen des Auskunftsanspruchs darzustellen sind.

Mit Hinweisen auf Stimmen in der Literatur führt der BGH ferner aus, dass auch Korrespondenz, die dem Betroffenen bereits vorliegt, zum Bereich der zu beauskunftenden Unterlagen zählt. Begründet wird dies damit, dass der Betroffene in die Lage versetzt werden soll, zu beurteilen, wie die auskunftsverpflichtete Stelle diese Daten verarbeitet und gespeichert hat.

Aus diesem Teil der Ausführungen des Gerichts müssen Verantwortliche die Schlussfolgerung ziehen, dass sie sich bei der Beauskunftung nicht in allen Bereichen darauf zurückziehen können, dass bestimmte Informationen dem Betroffenen bereits bekannt sind und/oder vorliegen. Vielmehr ist eine Information über diese Daten zu geben, insbesondere wenn sie wie im Fall der vom Gericht angesprochenen Korrespondenz weiterverarbeitet worden sind.

2.4 Prüfungen

Trotz der anhaltenden Corona-Pandemie, die Prüfungen in den kirchlichen Einrichtungen vor Ort erheblich erschwerte, hat das Katholische Datenschutzzentrum auch im Berichtszeitraum versucht, mit Querschnitts- und Schwerpunktprüfungen das Datenschutzniveau kirchlicher Einrichtungen zu überprüfen.

2.4.1 Die Querschnittsprüfung kirchlicher Kindertagesstätten

Über die im Herbst 2019 begonnene Querschnittsprüfung kirchlicher Kindertagesstätten wurde im letzten Jahresbericht schon mit einem längeren Zwischenbericht informiert.[25]

In diesem Zwischenbericht hatte das KDSZ beschrieben, dass aus einer Gesamtmenge von ca. 2.600 katholischen Kindertagesstätten nach einem Zufallsprinzip unter Beachtung des regionalen Proporzes 100 Einrichtungen ausgewählt und gebeten wurden, einen elektronischen Fragebogen zu den verschiedenen Aspekten des Datenschutzes in ihren Einrichtungen zu beantworten. Die Fragen reichten von den Informationen über die Benennung und der Arbeit der jeweiligen betrieblichen Datenschutzbeauftragten bis zum Schutz personenbezogener Daten durch technische und organisatorische Maßnahmen. Gefragt wurde nach der Absicherung von Serverräumen, Speichermedien und Endgeräten. Auch die Gestaltung der genutzten Anwendungen etwa durch Berechtigungskonzepte oder vorgegebene Löschfristen wurde thematisiert.

In einem zweiten Schritt wurden auf Basis der Antworten der Kindertagesstätten bei Unklarheiten Rückfragen an die Einrichtungen gestellt.

Nach Abschluss der dann folgenden Auswertung wurden die teilnehmenden Kindertagesstätten sowie die Trägereinrichtungen (Fachabteilungen der Diözesen und der diözesanen Caritasverbände) über die Ergebnisse im Einzelnen oder in aggregierter Form informiert.

„Ziel der Querschnittsprüfung war es, insgesamt einen noch besseren Überblick über die datenschutzrechtliche Situation in den katholischen Kindertagesstätten … zu erhalten, auf Seiten der Kitas … das Bewusstsein für den Datenschutz zu schärfen und dabei wiederkehrende Problempunkte zu identifizieren und anzusprechen.“

Die Bewertung aller erhobenen Informationen basiert auf einem vierstufigen Schema: Falls die Antwort auf eine Frage im ersten elektronischen Fragebogen bereits vollständig und zufriedenstellend erfolgte, erübrigten sich für das Katholische Datenschutzzentrum weitere Nachfragen. Wurde eine Nachfrage gestellt, so konnte die Antwort in vielen Fällen eine Unklarheit beseitigen beziehungsweise bereits initiierte Verbesserungen erläutern. In den anderen Fällen musste das KDSZ bewerten, ob in dem konkreten Fall in der jeweiligen Einrichtung ein eher leichteres datenschutzrelevantes Versäumnis oder sogar ein schwerwiegender Mangel beziehungsweise Verstoß gegen Datenschutzvorschriften vorliegt.

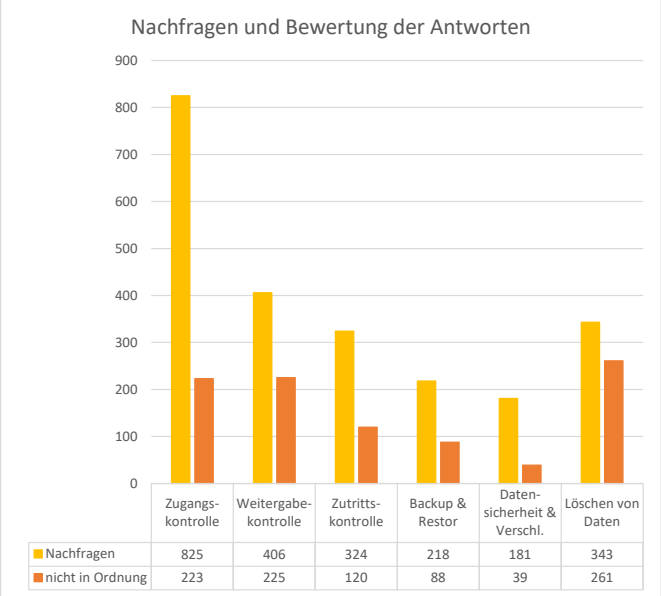
Ein leichteres Versäumnis führte in der Konsequenz zu einem Hinweis an die Einrichtung, wie der Datenschutz im konkreten Fall verbessert werden sollte. Ein festgestellter Gesetzesverstoß führte zu einer Beanstandung und verbindlichen Anordnungen gemäß § 47 Abs. 5 KDG.

Ziel der Querschnittsprüfung war es, insgesamt einen noch besseren Überblick über die datenschutzrechtliche Situation in den katholischen Kindertagesstätten im Zuständigkeitsbereich des Katholischen Datenschutzzentrums zu erhalten, auf Seiten der Kitas und deren Träger das Bewusstsein für den Datenschutz zu schärfen und dabei wiederkehrende Problempunkte zu identifizieren und anzusprechen. Als Ergebnis der Prüfung ist daher für alle 2.600 Einrichtungen interessant, in welchen Themenbereichen die meisten Nachfragen gestellt werden muss-

[25] Siehe Abschnitt 3.5 des Jahresberichts 2020.

ten und zu welchem Anteil die gestellten Nachfragen zufriedenstellend – oder eben nicht zufriedenstellend – beantwortet werden konnten. Anhand dieser Stichworte sollten alle Einrichtungen ihre eigene Situation und die datenschutzrechtlichen Vorkehrungen nochmals überprüfen.

Relevant ist nicht nur die reine Anzahl der Nachfragen, sondern auch die Quote derjenigen Antworten auf diese Nachfragen, die vom KDSZ als „nicht zufriedenstellend" eingestuft wurden, also einen Hinweis oder sogar eine Beanstandung auslösten. In der folgenden Tabelle und Grafik sind beide Kennzahlen verdeutlicht:



	Zugangs-kontrolle	Weitergabe-kontrolle	Zutritts-kontrolle	Backup & Restor	Daten-sicherheit & Verschl.	Löschen von Daten
Nachfragen	825	406	324	218	181	343
nicht in Ordnung	223	225	120	88	39	261

Aus der Übersicht wird u. a. deutlich, dass ein großes Verbesserungspotential in den Bereichen der Weitergabekontrolle (also den Regelungen bei der Übertragung und Weitergabe von Daten an andere Stellen, etwa kommunale Behörden) und des Löschens von Daten besteht.

In Bezug auf Mängel bei der Weitergabekontrolle wurde häufig die Argumentation vorgetragen, die Kita nutze zentrale Systeme (etwa KitaPLUS) und habe deshalb mit diesen Themen „nichts zu tun". Dabei wird von den Verantwortlichen jedoch übersehen, dass auch bei Beauftragung eines Dienstleisters und der Verwendung eines zentralen Systems die Verantwortung für die Datenverarbeitung nicht abgegeben werden kann. So sollten den Verantwortlichen beispielsweise die Abläufe und die Aufbewahrungsfristen bekannt sein, damit die Betroffenen (hier die Eltern und Beschäftigten) zutreffend informiert werden können. Leider war das Löschkonzept in KitaPLUS zum Zeitpunkt der Prüfung noch nicht vollständig umgesetzt.

Erfreulich war aus Sicht des Katholischen Datenschutzzentrums, dass die Endgeräte (PC, Laptop) in den Kitas inzwischen fast durchgängig verschlüsselt sind. Dies kann als einer der positiven Effekte der Prüfung angesehen werden, da einer der Auslöser der Querschnittsprüfung gerade die hohe Zahl von gemeldeten Datenschutzverletzungen in den Jahren 2018 und 2019 war, die aus Einbruchdiebstählen resultierten und bei denen regelmäßig unverschlüsselte Endgeräte und Datenträger gestohlen wurden. Nachdem das Katholische Datenschutzzentrum das Thema der Verschlüsselung mehrfach und intensiv thematisiert hatte,

wurde fast überall reagiert und zumindest bei Neuanschaffungen auf einen wirksamen Verschlüsselungsschutz geachtet.

Als Ergebnis der Prüfung konnten bei fast allen in die Prüfung einbezogenen Kitas einige oder mehrere Hinweise zur Verbesserung ihres Datenschutzniveaus gegeben werden. Lediglich bei wenigen Einzelfällen der geprüften Einrichtungen mussten aufgrund der Schwere der Verstöße eine formale Beanstandung und entsprechende Anordnungen ausgesprochen werden. Bei einer Einrichtung wurde ein Vor-Ort-Termin durchgeführt, um die Prüfung abschließen zu können.

Das Ergebnis zeigt, dass der Datenschutz in den katholischen Kindertageseinrichtungen in den fünf nordrhein-westfälischen (Erz-)Diözesen auf einem guten Weg ist und die Einrichtungen schon einen hohen Datenschutzstandard erreicht haben. Positiv ist ebenfalls festzuhalten, dass das Thema Datenschutz durchweg mit der nötigen Priorität behandelt wird. Noch festgestellte Schwachstellen können in den Einrichtungen meist durch einfache Maßnahmen beseitigt werden.

Neben dem erfreulichen fachlichen Fazit kann aus Sicht des Katholischen Datenschutzzentrums noch positiv festgestellt werden, dass die Zusammenarbeit mit den geprüften Kindertagesstätten fast ausnahmslos sehr kooperativ und offen verlief.

2.4.2 Prüfung zur sachgerechten Beseitigung der „Hafnium"-Sicherheitslücke in MS Exchange Server und dem Umgang mit den Folgen dieser

Im Februar 2021 musste Microsoft eine schwere Sicherheitslücke in dem weitverbreiteten Programm „Exchange Server" einräumen. Der Server bietet u. a. die Möglichkeit, über das https-Protokoll und den Port 443 auf die Postfächer auch dann zuzugreifen, wenn der Anwender kein Client-Programm (etwa MS Outlook) verwendet, sondern nur einen Webbrowser zur Verfügung hat. Genau über diesen Weg war es aber lange Zeit auch möglich, unberechtigten Zugriff auf die Daten des Servers zu nehmen und dadurch etwa Daten und Adressen von E-Mails auszulesen oder Schadsoftware auf dem Server zu platzieren.

Alle Betreiber von Servern mit MS Exchange standen vor der Aufgabe, die Sicherheitslücke schnellstens durch Einspielen eines Updates („Sicherheitspatch") zu schließen und ihre Systeme daraufhin zu untersuchen, ob die Sicherheitslücke bereits ausgenutzt worden war, also nachweislich Schadsoftware installiert wurde oder sogar bereits Daten abgeflossen waren.

Von mehreren Einrichtungen wurden dem Katholischen Datenschutzzentrum – meistens vorsorglich – Datenschutzverletzungen gemeldet, die darin bestanden, dass die Sicherheitslücke bestanden hatte oder dass sogar Schadsoftware gefunden worden war.

Vor dem Hintergrund der möglichen Auswirkungen für die Nutzer der E-Mail-Server und der Zahl möglicher betroffener Nutzer dieser Sicherheitslücke, hat das Katholische Datenschutzzentrum im April 2021 eine Reihe von kirchlichen Einrichtungen einer Prüfung unterzogen, mit der

die sachgerechte Beseitigung der Sicherheitslücke und der Umgang mit eventuellen Folgen untersucht wurde.

In einem ersten Schritt wurden die öffentlich verfügbaren Informationen der E-Mail-versendenden Server (DNS- und MX-Einträge) abgefragt. Auf diese Zieladressen wurde das MS Detektionsskript angewendet, welches das Vorhandensein der Sicherheitslücke anzeigt. Zum Zeitpunkt der Prüfung war die Sicherheitslücke bei allen geprüften Einrichtungen bereits geschlossen.

Im zweiten Schritt wurden den zu prüfenden Einrichtungen die ermittelten Informationen mitgeteilt und die Verantwortlichen gebeten, das Vorgehen beim Schließen der Sicherheitslücke zu beschreiben und darzulegen, was als weiterer Umgang mit eventuellen Folgen geplant ist, etwa das Beobachten eventueller ungewöhnlicher Datenströme als Anzeichen einer unberechtigten Datenübertragung durch Schadsoftware.

Die Antworten der angeschriebenen Einrichtungen zeigten durchweg ein angemessenes und professionelles Verhalten der Verantwortlichen. In einigen Fällen hatte der Vorfall dazu geführt, dass der Serverbetrieb an einen professionellen Dienstleister abgegeben wurde oder kleine Einrichtungen sich der IT-Struktur von übergeordneten Verbünden angeschlossen haben. In keinem Fall musste eine Anordnung ausgesprochen werden.

Insgesamt konnte das Katholische Datenschutzzentrum ein positives Resümee aus der Prüfung ziehen. Die Ergebnisse der Prüfung zeigen, dass die geprüften kirchlichen Stellen umgehend und im erforderlichen Umfang auf die bekannt gewordene Sicherheitslücke reagiert haben.

„Die Ergebnisse der Prüfung zeigen, dass die geprüften kirchlichen Stellen umgehend und im erforderlichen Umfang auf die bekannt gewordene Sicherheitslücke reagiert haben."

2.5 Beschwerden und Hinweise

Personen, die sich durch eine Verarbeitung ihrer personenbezogenen Daten durch eine katholische Einrichtung in ihren Rechten verletzt fühlen, können bei der Datenschutzaufsicht im Rahmen einer Beschwerde beziehungsweise eines Hinweises (wenn nicht die eigenen Daten betroffen sind) die Verarbeitung der kirchlichen Stelle überprüfen lassen. Im Berichtszeitraum haben wieder viele Personen von dieser Möglichkeit Gebrauch gemacht. Neben Themen, die schon an anderen Stellen in diesem Jahresbericht erwähnt sind, werden nachfolgend exemplarisch einige wenige Sachverhalte aus der Menge der Beschwerdesachverhalte herausgegriffen.

2.5.1 Auskunftsersuchen

Auch in diesem Berichtszeitraum erreichten das Katholische Datenschutzzentrum Beschwerden Betroffener bezüglich der Bearbeitung und der Beantwortung von Auskunftsbegehren durch kirchliche Einrichtungen. Kritisiert wurden insbesondere tatsächliche oder subjektiv

empfundene Unvollständigkeiten bei der Erteilung der Auskünfte sowie erst mit Verspätung erfolgende Reaktionen.

In einem Teil der Fälle bestätigten sich die Vorwürfe der nur unvollständig gegebenen Auskünfte und der Nichteinhaltung der gesetzlich vorgegebenen Antwortfristen. In einigen Fällen waren die Antworten dagegen objektiv vollständig und aus Sicht des Katholischen Datenschutzzentrums nicht zu beanstanden.

In diesem Zusammenhang möchte das Katholische Datenschutzzentrum erneut auf die Beachtung der gesetzlichen Grundlagen im Rahmen der Beantwortung von Auskunftsersuchen von Betroffenen hinweisen.

Gemäß § 17 KDG hat eine betroffene Person das Recht, von dem Verantwortlichen einer kirchlichen Stelle eine Auskunft über die Verarbeitung der diese Person betreffenden personenbezogenen Daten zu verlangen. § 17 KDG enthält einen Katalog von Informationen, der im Rahmen der Auskunftserteilung abzuarbeiten ist, sodass eine umfassende und vollständige Auskunft gegeben werden kann. Darüber hinaus sind die weiteren Anforderungen, die in § 17 KDG formuliert sind, zu beachten. Verantwortliche in kirchlichen Einrichtungen müssen daher dafür Sorge tragen, dass sorgfältig ermittelt wird, welche personenbezogenen Daten über die betreffende Person vorhanden sind. Es muss sichergestellt sein, dass keine Bereiche übersehen werden, sodass nicht das Risiko einer unvollständigen Beantwortung entstehen kann.

Ebenso sorgfältig ist dann die Antwort gegenüber der anfragenden Person zu erteilen. Dabei sind die Vorgaben des § 14 KDG zu beachten und einzuhalten. Dazu zählt insbesondere die Anforderung nach § 14 Abs. 1 KDG, wonach eine Mitteilung gemäß § 17 KDG in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache, gegebenenfalls auch mit standardisierten Bildsymbolen, zu übermitteln ist. Weiterhin ist § 14 Abs. 3 KDG notwendig zu beachten. Danach hat der Verantwortliche einer anfragenden betroffenen Person die im Auskunftsverfahren begehrten Informationen nach § 17 KDG unverzüglich nach Eingang des Antrags zur Verfügung zu stellen. Der maximale Zeitraum, innerhalb der die Antwort gegeben werden muss, beträgt – sofern nicht außergewöhnliche Umstände im Sinne von § 14 Abs. 3 S. 2 KDG vorliegen – einen Monat ab dem Zeitpunkt des Antragseingangs. Verantwortliche müssen für ihre Einrichtungen sicherstellen, dass die Beauskunftung innerhalb dieser Vorgabe bearbeitet und abgeschlossen wird. Die in § 14 Abs. 3 S. 2 KDG vorgesehene mögliche Verlängerung der Frist um zwei Monate stellt einen Ausnahmetatbestand dar. Auf diesen kann sich ein Verantwortlicher nur bei Vorliegen der dort geschilderten Ausnahmesituationen berufen, die eher selten gegeben sein dürften. Zu beachten ist, dass dabei innerhalb der ursprünglichen Monatsfrist eine Unterrichtung über die Fristverlängerung und der Angaben der Gründe für die Verzögerung erfolgen muss.

2.5.2 Weitergabe personenbezogener Daten an Dritte

Weil katholische Einrichtungen in diversen Bereichen des Lebens tätig sind, wie beispielsweise dem Betrieb von Kindertagesstätten, Altenheimen oder Behindertenwerkstätten, kommt es immer wieder zu Daten-

abfragen durch staatliche oder auch nicht-staatliche Einrichtungen (beispielsweise Gesundheitsämter oder Kostenträger). Auch wenn die personenbezogenen Daten hier von staatlichen oder öffentlichen Stellen angefordert werden, ist in jedem Fall die Frage nach der Rechtsgrundlage für die konkrete Weiterleitung der Daten zu klären.

Bei der Weiterleitung von personenbezogenen Daten an Dritte handelt es sich in den Worten des KDG um eine „Offenlegung durch Übermittlung", welche wiederum eine Verarbeitung i. S. d. § 4 Nr. 3 KDG darstellt. Eine solche Verarbeitung bedarf einer Rechtsgrundlage. Welche Rechtsgrundlage in Betracht kommt, richtet sich nach der Kategorie der übermittelten personenbezogenen Daten. Sollen etwa Gesundheitsdaten (vgl. § 4 Nr. 17 KDG) übermittelt werden, liegt eine besondere Kategorie personenbezogener Daten nach § 4 Nr. 2 KDG vor und die Verarbeitung der Daten richtet sich nach § 11 KDG. Im Übrigen richtet sich die Rechtmäßigkeit einer Verarbeitung vor allem nach § 6 KDG.

Im Jahr 2021 kam es aufgrund der Corona-Pandemie u. a. zu Anforderung von personenbezogenen Daten durch die Gesundheitsämter. Im Falle einer Beschwerde etwa, wurden personenbezogene Daten der Kinder und Erziehungsberechtigten zur Kontaktnachverfolgung angefordert. Für einen solchen Fall muss der Verantwortliche im Rahmen seiner Nachweispflicht aus § 7 Abs. 2 KDG sicherstellen, dass die Übermittlung nur beim Vorliegen einer entsprechenden Rechtsgrundlage erfolgt und dass dies zu einem festgelegten und legitimen Zweck geschieht.

Immer wieder kommt es seitens der Verantwortlichen in solchen Situationen zu Verunsicherungen, da bei den Anforderungen von Daten durch staatliche Behörden in vielen Fällen keine Rechtsgrundlage genannt wird. Angesichts der Tatsache, dass die übermittelnden Stellen, also hier die kirchlichen Einrichtungen, für die Rechtmäßigkeit der Übermittlung verantwortlich sind, müssen diese sich aber der Rechtsgrundlage bewusst sein. Ein bloßes Vertrauen darauf, dass staatliche Behörden nur in zulässigen Fällen Daten anfordern, genügt insofern nicht.

Neben der grundlegenden Pflicht aus § 7 Abs. 1 lit. a) KDG, dass die Verarbeitung rechtmäßig sein muss und der Nachweispflicht aus Absatz 2, erfüllt die Feststellung der Rechtsgrundlage vor der konkreten Verarbeitung allerdings auch den nicht zu unterschätzenden Zweck der Selbstkontrolle. Kommt es aufgrund einer Weitergabe von Daten zu einer Anfrage von Betroffenen, kann diese kurzfristig beauskunftet werden. Dies hätte vermutlich in einigen Fällen eine Beschwerde an die Datenschutzaufsicht vermieden.

2.5.3 Fotos und Scans von Impfzertifikaten

Im Laufe der Covid-19-Pandemie erreichten das Katholische Datenschutzzentrum verschiedenste Anfragen und Beschwerden zu Impfzertifikaten beziehungsweise den sogenannten 3G-Nachweisen.[26] Teil der Beschwerden waren auch Sachverhalte, in denen betroffene Personen ihre Impfzertifikate und Nachweise durch katholische Einrichtungen in

[26] Siehe z. B. Abschnitt 2.1.1 in diesem Bericht.

unzulässiger Weise verarbeitet sahen. So kam es z. B. vor, dass betroffene Personen ihre Impfzertifikate von Mitarbeitenden in einem kirchlichen Gastronomiebetrieb in unzulässiger Weise fotografiert glaubten. Auf die Zulässigkeit der Verarbeitung von Impfzertifikaten in Gastronomiebetrieben soll hier beispielhaft eingegangen werden.[27]

Bei Impfnachweisen beziehungsweise Zertifikaten handelt es sich um Gesundheitsdaten. Diese sind den besonderen Kategorien von personenbezogenen Daten gemäß § 4 Nr. 2 und 17 KDG zuzuordnen. Die Verarbeitung von personenbezogenen Daten der besonderen Kategorie richtet sich nach § 11 KDG. Grundsätzlich ist die Verarbeitung nach § 11 Abs. 1 KDG untersagt. Etwas anderes gilt nur, wenn einer der Ausnahmetatbestände des § 11 Abs. 2 KDG vorliegt. So ist die Verarbeitung von Gesundheitsdaten z. B. aufgrund von kirchlichen oder staatlichen Normen zulässig, wenn diese im angemessenen Verhältnis zum verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorgesehen werden.

Betreiber von Gastronomien waren zeitweise dazu verpflichtet Impfnachweise gemäß der jeweils geltenden Coronaschutzverordnung des Landes Nordrhein-Westfalen zu kontrollieren. In der Fassung der Verordnung vom 19.10.2021 stellte § 4 Abs. 2 Nr. 5 und Abs. 5 CoronaSchVO die staatliche Rechtsgrundlage für diese Kontrollpflicht dar.

Ziel dieser Kontrollpflicht war die Fortsetzung der erfolgreichen Bekämpfung der Pandemie in Form der Begrenzung eines erneuten Anstiegs der Infektionszahlen, die weitere Gewährleistung ausreichender medizinischer Versorgungskapazitäten und geimpften und genesenen Personen wieder eine weitgehend uneingeschränkte Nutzung von gesellschaftlichen, kulturellen, sozialen und sportlichen Angeboten und Einrichtungen zu ermöglichen und so eine größtmögliche Normalisierung in den entsprechenden Lebensbereichen zu erreichen. Zu diesem Zeitpunkt der Pandemie stand eine Impfnachweiskontrolle im angemessenen Verhältnis zu dem oben angegebenen Ziel.

Zur Bestimmung angemessener und geeigneter Maßnahmen zum Schutz der Rechte der betroffenen Personen konnte der Grundsatz der Datenminimierung herangezogen werden. Dieser Grundsatz beinhaltet, dass nur die für den Verarbeitungsvorgang notwendigen personenbezogenen Daten erhoben werden. Das bedeutet für den vorliegenden Sachverhalt konkret, dass lediglich die Gültigkeit des Impfnachweises kontrolliert werden soll. Fotoaufnahmen wären daher unzulässig gewesen. Der Impfnachweis konnte aber entweder durch die Inaugenscheinnahme des ordentlichen Impfausweises oder Scan des digitalen Impfzertifikats mit der CovPassCheck-App kontrolliert werden. Das geschieht jeweils in Kombination mit dem Personalausweis oder einem anderen amtlichen Lichtbildausweis der betroffenen Person. Bei diesen Methoden werden keine langfristigen Kopien der Datensätze auf einem mobilen Endgerät gespeichert. Der Grundsatz der Datenminimierung wird dabei gewahrt. Die Kontrolle durch App und digitales Impfzertifikat war dabei die vorzugswürdige Methode, da lediglich ein QR-Code

[27] Hier erfolgt eine beispielhafte Darstellung. In Verbindung mit dieser Thematik sind viele weitere Sachverhaltskonstellationen denkbar. Es handelt sich stets um eine Einzelfallbetrachtung. Die Fallbewertungen können sich unterscheiden, insbesondere durch die ständigen Weiterentwicklungen beziehungsweise Änderungen der verschiedenen Rechtsgrundlagen im Verlauf der Pandemie.

gescannt wurde und die kontrollierende Person nicht mehr Informationen bekam, sie für die Prüfung benötigte.

Die oben ausgeführten Vorgaben wurden von den katholischen Einrichtungen auch grundsätzlich eingehalten. Zu unzulässigen Fotografien von Impfnachweisen kam es in den Beschwerdefällen nicht.

2.5.4 Verwendung privater E-Mail-Konten zu dienstlichen Zwecken

Ein Thema, welches mit zunehmender Digitalisierung bei gleichzeitig begrenzten finanziellen Mitteln immer wieder auftaucht, ist die Nutzung privater IT-Systeme zu dienstlichen Zwecken.

Fallen Mitarbeitende beispielsweise aufgrund von Corona-Quarantäne aus, sind allerdings symptomfrei und könnten theoretisch arbeiten, kommt schnell der Gedanke auf, dass die Arbeit zumindest in Teilen auch vom privaten Rechner zuhause erledigt werden kann. Eine Weiterleitung von dienstlichen E-Mails mit personenbezogenen Daten an das private E-Mail-Konto der Mitarbeitenden ist jedoch nicht so einfach möglich. Eine automatische Weiterleitung ist nach § 20 Abs. 4 KDG-DVO sogar in jedem Fall unzulässig.

Die Nutzung privater IT-Systeme – wie etwa Mobiltelefone, Notebooks oder E-Mail-Konten – zu dienstlichen Zwecken ist gemäß § 20 KDG-DVO grundsätzlich untersagt. Zweck dieser Regelung ist es, dass der Verantwortliche die Kontrolle über die Verarbeitung und damit wiederum auch über den Schutz der personenbezogenen Daten behält. § 20 KDG setzt keine schriftliche Dienstvereinbarung zu der Nutzung voraus. Vielmehr wird von einem grundsätzlichen Verbot ausgegangen, von welchem in Ausnahmefällen durch den Verantwortlichen unter den dort genannten Voraussetzungen abgewichen werden kann.

Durch die Nutzung privater IT-Systeme zu dienstlichen Zwecken entsteht eine besondere Gefahrenlage, da beispielsweise einheitliche Voreinstellungen zur Umsetzung der datenschutzrechtlichen Vorgaben und Sicherheitsvorgaben – wie sie bei dienstlichen Geräten vorgegeben sein sollten – nicht gegeben sind. Da der Verantwortliche deren Sicherstellung allerdings dennoch gewährleisten muss, sind gegebenenfalls Maßnahmen wie die Einrichtung eines Fernzugriffs erforderlich. Durch einen solchen kann etwa im Falle des Verlustes eines Endgerätes eine Fernlöschung durchgeführt werden, um die Vertraulichkeit der personenbezogenen Daten sicherzustellen. Eine solche Zugriffsmöglichkeit des Arbeitgebers auf die privaten Geräte stößt verständlicherweise bei vielen Mitarbeitenden auf Unbehagen. Auch die Einhaltung von Löschfristen und die Erfüllung des Auskunftsrechts der betroffenen Personen aus § 17 KDG gestalten sich schwieriger.

Es ist jedoch nicht ausschließlich die Arbeitgeberseite, die die Nutzung privater IT-Systeme anstößt. Auch durch die Mitarbeitenden werden teilweise unaufgefordert und – im Sinne der obigen Regelung des § 20 KDG-DVO – unzulässigerweise dienstliche Aufgaben auf dem privaten Smartphone oder Laptop erledigt. Für den Verantwortlichen bedeutet dies stets ein Kontrollverlust über die Verarbeitungstätigkeit. Angesichts

dieses Risikos erscheint es sinnvoll bei den Mitarbeitenden, ergänzend zu dem ohnehin bestehenden gesetzlichen Verbot, ein geschärftes Bewusstsein für diese Problematik zu schaffen. In welcher Form dies geschieht ist dabei offen. Eine Option wäre die Aufnahme der Thematik in die Datenschutzschulung oder eine schriftliche Dienstanweisung mit einer deklaratorischen Wiederholung der bestehenden Verbote.

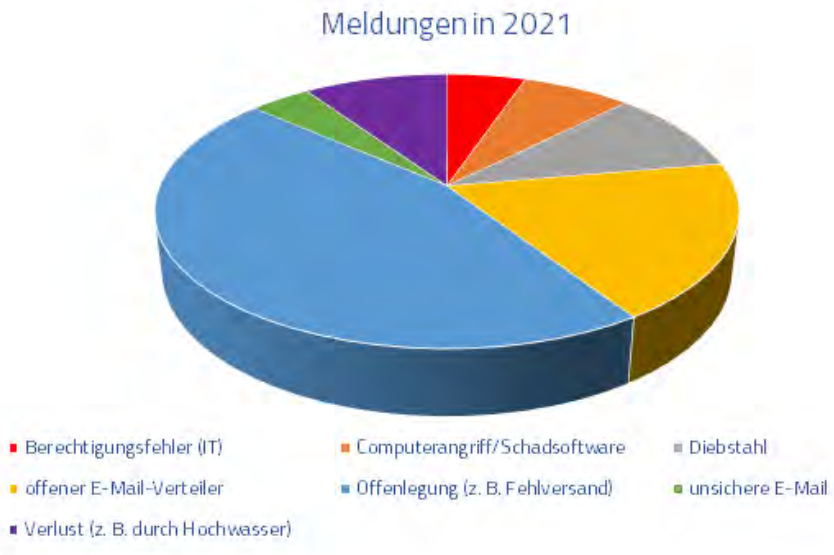
2.6 Meldungen von Datenschutzverletzungen

Auch in diesem Berichtszeitraum erreichten das Katholische Datenschutzzentrum weiterhin eine hohe Anzahl von Meldungen von Datenschutzverletzungen nach § 33 KDG. Zwar sank die Zahl im Vergleich zum Jahr 2020 leicht. Sie liegt aber immer noch erheblich über der Zahl der Meldungen des Jahres 2019.

Bei den eingereichten Meldungen waren auch im letzten Jahr oft noch Nachfragen notwendig, da die Meldungen nicht alle notwendigen Informationen enthielten. Hier erleichterte es die Bearbeitung für beide Seiten, wenn die auch im Meldeformular schon abgefragten Informationen direkt bereitgestellt würden.

Aus Sicht des Katholischen Datenschutzzentrums ist positiv hervorzuheben, dass die Aufarbeitung von gemeldeten Datenschutzverletzungen zwischen der kirchlichen Einrichtung und der Aufsicht meist kooperativ verläuft und dass die Einrichtungen auch gewillt sind, die notwendigen Maßnahmen zu ergreifen, um vergleichbare Datenschutzverletzungen für die Zukunft auszuschließen.

Die nachfolgende Darstellung zeigt eine grobe thematische Einordnung der eingegangenen Meldungen im Berichtszeitraum.



> **„... ist positiv hervorzuheben, dass die Aufarbeitung von gemeldeten Datenschutzverletzungen ... meist kooperativ verläuft und dass die Einrichtungen auch gewillt sind, die notwendigen Maßnahmen zu ergreifen, um vergleichbare Datenschutzverletzungen für die Zukunft auszuschließen."**

2.6.1 Unbefugte Offenlegung von personenbezogenen Daten

Auch im Berichtsjahr 2021 liegt einer der Schwerpunkte der eingegangenen Meldungen von Datenschutzverletzungen nach § 33 KDG bei der unbefugten Offenlegung von personenbezogenen Daten gegenüber Dritten.

Insbesondere dann, wenn es sich um hoch sensible Daten wie Gesundheitsdaten oder Gehaltsabrechnungen mit Kontoinformationen handelt, stellt die Verletzung des Schutzes der personenbezogenen Daten ein besonders hohes Risiko für das Persönlichkeitsrecht der betroffenen Personen dar.

Häufigste Ursache für den Fehlversand von personenbezogenen Daten ist menschliches Versehen. Die Vorfälle reichen von unbeabsichtigt mitgesandten E-Mail-Anhängen über vertauschte Unterlagen bei der Kuvertierung von Briefen bis hin zu falsch ausgewählten E-Mail-Adressen oder falsch eingegeben Faxnummern.

Wo Menschen arbeiten, passieren Fehler. Dessen ist sich auch das Katholische Datenschutzzentrum bewusst. Im hektischen Arbeitsalltag fällt es oft schwer die gebotene Aufmerksamkeit stets hoch zu halten. Umso unverständlicher ist es jedoch, dass gerade die Bereiche, in denen man menschliche Fehler durch technische und organisatorische Maßnahmen verhindern beziehungsweise deren Folgen deutlich abmildern kann, auch nach vier Jahren Geltung des KDG offenbar nicht flächendeckend umgesetzt werden. So sollten Softwarefehler, wie die falsche Zuordnung von Namen, im Rahmen des Test- und Freigabeverfahrens gefunden und behoben werden. Auch die Vermischung von Corona Testergebnissen mit einfachen Materialbestellungen wäre in einem Fall durch ein entsprechendes Berechtigungskonzept zu vermeiden gewesen.

2.6.2 Diebstahl und Verlust von Endgeräten

Ein weiteres, stetiges Begleitthema im Bereich der Meldungen ist der Diebstahl und Verlust von digitalen Endgeräten. Neben der Art des Gerätes (z. B. Laptops, Mobiltelefone oder Kameras) variiert auch der Ort und die Art des Abhandenkommens. Häufige Fälle sind hier Einbrüche in die Einrichtung oder in einen Pkw oder das Gerät wird schlicht in der Bahn vergessen.

Durch den Kontrollverlust über das Endgerät sind häufig insbesondere die Schutzziele der Vertraulichkeit und der Verfügbarkeit personenbezogener Daten betroffen.

Eine leicht umsetzbare Lösung für die Sicherstellung des Schutzziels der Vertraulichkeit ist die flächendeckende und voreingestellte Verschlüsselung der Speichermedien. Bei einer Festplattenverschlüsselung, welche dem aktuellen Stand der Technik entspricht, kann aus Sicht des Katholischen Datenschutzzentrums davon ausgegangen werden, dass unbefugten Dritten – ohne unverhältnismäßigen Aufwand – der Zugriff auf die Daten nicht gelingt. Auf diese Weise sind auch verse-

hentlich lokal gespeicherte Daten geschützt, sofern das Gerät nicht in eingeschaltetem Zustand abhandenkommt.

Ein zumindest bei größeren oder fest verankerten Tresoren eher seltener, aber im Jahr 2021 gemeldeter Fall eines Einbruchdiebstahls, bei dem ein ganzer Tresor mitgenommen wurde, stellt eine Ausnahmesituation dar, welche sich kaum ausschließen lässt. Wobei auch hier eine Verschlüsselung die Daten auf den digitalen Geräten zuverlässig schützen kann.

Neben technischen Maßnahmen kann die Wahrscheinlichkeit des Verlustes von Endgeräten auch durch regelmäßige Sensibilisierung und dem Mitdenken der Mitarbeitenden erheblich reduziert werden. So sollten Endgeräte etwa nicht in einem abgestellten Pkw gelagert werden (auch nicht kurzzeitig). Ebenso sollten diese nicht im öffentlichen Raum (z. B. Kaufhaus oder Straßenbahn) abgelegt werden, um ein Vergessen zu vermeiden. Grundsätzlich sollten Endgeräte nur in tatsächlich erforderlichen Fällen transportiert werden.

2.6.3 Angriffe auf IT-Systeme durch Schadsoftware

Im Berichtsjahr 2021 wurden dem Katholischen Datenschutzzentrum auch wieder Angriffe auf IT-Systeme durch Schadsoftware gemeldet. Dabei tauchte unter anderem das bereits bekannte Schadprogramm „Emotet“ wieder auf.

Neben zahlreichen Sofortmaßnahmen wie z. B. der Entfernung der Schadsoftware, der Neuaufsetzung betroffener Geräte, der Änderung von Zugangsdaten sowie der Löschung befallener Daten mit anschließender Wiederherstellung dieser aus einem Backup, waren auch im Nachgang weitere Maßnahmen erforderlich, um die Wahrscheinlichkeit einer erneuten Infektion zu minimieren und damit mögliche Schäden zukünftiger Infektionen möglichst gering zu halten.

Bei der Analyse der Ursachen eines Befalls in den Einrichtungen zeigte sich, dass häufig der Risikofaktor „Mensch“ durch Phishing-Mails ausgenutzt wurde, um die Schadsoftware einzuschleusen. Dies bekräftigt die hohe Bedeutung regelmäßiger Datenschutzschulungen, um bei den Mitarbeitenden ein geschärftes Bewusstsein für derartige Fallen zu schaffen. Ein aufmerksamer Umgang mit E-Mails oder mobilen Speichermedien ist essenziell, um die Zahl der erfolgreichen Angriffe auf IT-Systeme zu reduzieren.

Neben „Emotet“ beschäftigte das KDSZ auch eine kritische Schwachstelle in Microsoft Exchange-Servern[28], zu welcher sich neben den Veröffentlichungen auf der Internetseite des KDSZ unter anderem auch beim BSI Informationen und Maßnahmen finden.[29]

[28] Siehe auch Abschnitt 2.4.2 dieses Berichts.

[29] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Server/Microsoft-Exchange_Schwachstelle/schwachstelle_exchange_server_node.html

2.6.4 Fehler bei der Vergabe von Berechtigungen

Viele Fälle von Meldungen von Datenschutzverletzungen im Berichtsjahr hatten als Auslöser mangelnde oder fehlende Regelungen zu den Zugriffsrechten von IT-Systemen. Ein funktionierendes Berechtigungskonzept ist unabdingbar, um zu gewährleisten, dass nur diejenigen Mitarbeitenden auf personenbezogene Daten zugreifen können, für die dieser Zugriff aufgrund ihres Aufgabenbereiches tatsächlich notwendig ist. Eine immer wieder geäußerte Fehlvorstellung ist, dass die Verpflichtung der Mitarbeitenden auf das Datengeheimnis und eine Verschwiegenheitsvereinbarung einen hinreichenden Schutz der personenbezogenen Daten gewährleisten. Doch auch wenn die abgerufenen Informationen aufgrund dieser ergänzenden Maßnahmen in der Theorie nicht nach außen dringen, stellt bereits das Abfragen durch unberechtigte Mitarbeitende einen Datenschutzverstoß dar.

Gemeldete Vorfälle waren beispielsweise fälschlicherweise vergebene Leseberechtigungen an unzuständige Mitarbeitende durch den IT-Dienstleister oder eine aufgrund technischer Fehler entstandene Einsichtmöglichkeit in fremde E-Mail-Postfächer. In diesen Situationen ist es entscheidend, dass aufgrund klar verteilter Zuständigkeiten ein schnelles Handeln sichergestellt ist, um den Fehler zu beheben. Für die Zukunft sind dann entsprechende technische und organisatorische Maßnahmen zu ergreifen, damit individuelle Versäumnisse nicht mehr auftreten beziehungsweise frühzeitig abgefangen werden können.

2.7 Beratungen und Anfragen

Die Beantwortung von Anfragen und ganz allgemein die Beratung kirchlicher Stellen sind wichtige Bestandteile der Arbeit des Katholischen Datenschutzzentrums. Mit dieser Beratungstätigkeit, die das KDG an mehreren Stellen als Aufgabe der Datenschutzaufsicht hervorhebt, kann den kirchlichen Stellen mit der datenschutzrechtlichen Expertise der Datenschutzaufsicht bei offenen Fragen geholfen werden. Durch die Kommunikation im Vorfeld von Datenverarbeitungen können die kirchlichen Einrichtungen datenschutzrechtliche Fragen klären und Probleme vermeiden. Hierdurch kann die Beratungsfunktion des Katholischen Datenschutzzentrums die Beratung der betrieblichen Datenschutzbeauftragten vor Ort in den Einrichtungen ergänzen.

Die Möglichkeit, mit der Aufsicht offenen Fragen im Vorfeld möglicher Konflikte zu klären, wurde im Berichtszeitraum auch weiterhin intensiv genutzt. Die Zahl der an das Katholische Datenschutzzentrum gerichteten Anfragen und Beratungswünsche war im Jahr 2021 weiterhin auf einem sehr hohen Niveau.

2.7.1 Datenschutzkonformer Einsatz von Videokonferenzsystemen, Lernplattformen und Streamingdiensten

Auch im Jahr 2021 erreichten das Katholische Datenschutzzentrum Anfragen zum datenschutzkonformen Einsatz von Videokonferenzsystemen, Lernplattformen und Streamingdiensten (nachfolgend Kommunikationsanwendungen). Häufig fragen Verantwortliche dabei nach einer pauschalen Empfehlung für eine dieser Kommunikationsanwendungen. Allgemeine Empfehlungen für ein bestimmtes Produkt kann die Datenschutzaufsicht aber nicht abstrakt abgeben, da eine datenschutzrechtliche Beurteilung des Einsatzes einer Anwendung immer in der konkret geplanten Einsatzsituation vorgenommen werden muss. Hier kann das Katholische Datenschutzzentrum nur allgemeine Kriterien benennen, die bei der Auswahl von Kommunikationsanwendungen berücksichtigt werden sollten. Damit versucht das KDSZ auch die Unsicherheit im Zusammenhang mit dem Einsatz solcher Anwendungen nach der Schrems II-Entscheidung des EUGH zu mildern.[30]

Zur Bewertung der Konformität einer Kommunikationsanwendung mit datenschutzrechtlichen Bestimmungen sind die Umstände der Verarbeitung personenbezogener Daten heranzuziehen. So wären z. B. Art und Umfang der verarbeiteten Daten, der Ort der Verarbeitung der Daten, der Speicherort der Daten, Berechtigungen zum Zugriff auf die Daten oder – sofern z. B. bei einer Lernplattform notwendig – ein Backup-Konzept zu untersuchen. Dabei müssen nicht immer alle der aufgeführten Gesichtspunkte geprüft werden. Welche Kriterien zu prüfen sind, hängt stets von der konkreten Anwendung ab. Im Gesundheitssektor geht es z. B. häufig um die Verarbeitung von personenbezogenen Daten der besonderen Kategorie gemäß § 4 Nr. 2 KDG. Dort ist ein höherer Maßstab für die Prüfung anzulegen als in anderen Nutzungsszenarien.

Bei der datenschutzrechtlichen Bewertung des geplanten Einsatzes der konkreten Anwendung müssen u. a. die Funktionen der Anwendung bewertet werden, die eingesetzt werden sollen. Aber auch die Funktionen, die vielleicht nicht genutzt werden sollen, aber für die Nutzer verfügbar sind, sollten in den Blick genommen werden. So kann z. B. eine Funktion zur Aufzeichnung von Videokonferenzen in der Anwendung vorhanden sein. Auch wenn die kirchliche Stelle diese Funktionalität gar nicht nutzen will, müsste die Funktion daraufhin bewertet werden, was es datenschutzrechtlich bedeuten würde, wenn ein Teilnehmer – evtl. sogar ohne Kenntnis der anderen Teilnehmenden – eine Aufzeichnung anfertigt. In dem Beispiel wären dann – je nach Einsatzszenario – technische (Abschaltung der Aufzeichnungsfunktion) oder organisatorische Schutzmaßnahmen (interne Vorgaben zum Umgang mit der Aufzeichnungsfunktion) zu treffen.

„Eine Verarbeitung der Daten innerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums wird in der Regel … als unproblematisch zu bewerten sein."

Eine Verarbeitung der Daten innerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums wird in der Regel, aufgrund des einheitlichen Standards durch die DSGVO, als unproblematisch zu bewerten sein. Verantwortliche sollten jedoch seit der Schrems II-Entscheidung des Europäischen Gerichtshofs ein erhöhtes Augenmerk auf die Datenverarbeitung in Drittländern legen. Viele der heute

[30] Zu der Entscheidung siehe auch den Jahresbericht 2020, Abschnitt 2.1.1.

gängigen Kommunikationsanwendungen stammen von Unternehmen außerhalb der EU beziehungsweise mit Verarbeitungsstandorten in Drittländern. Eine Verarbeitung der Daten in diesen Ländern dürfte als unproblematisch anzusehen sein, solange für das entsprechende Drittland ein Angemessenheitsbeschluss gemäß § 40 Abs. 1 KDG vorliegt. Andernfalls muss vom Verantwortlichen sichergestellt werden, dass ein dem KDG entsprechendes Schutzniveau in dem Drittland erreicht werden kann. Im Falle der USA sollte nach den Feststellungen des EuGH in dessen Entscheidung besonders genau geprüft werden, ob eine datenschutzkonforme Übertragung möglich ist. Eine solche sollte in der Regel aufgrund der derzeitigen gesetzlichen Situation dort unzulässig sein.[31] Gleiches gilt im Übrigen für eine Verarbeitung durch US-Unternehmen mit Serverstandorten in der EU / dem EWR. Aufgrund des „CLOUD Acts" werden Verantwortliche in der Regel nicht sicherstellen können, dass personenbezogene Daten nicht doch in die USA übertragen werden.[32]

Verantwortliche können durch technische und organisatorische Maßnahmen eine höhere Datenschutzkonformität von Anwendungen erreichen. Eine Möglichkeit ist z. B. die Ende-zu-Ende Verschlüsselung der Kommunikation. Denkbar sind u. a. auch die manuelle Anpassung der Einstellungen einer Anwendung (z. B. Abschalten von Trackingfunktionen), die Beschränkung der Teilnehmerzahl oder das Hosten der Anwendung auf eigenen Servern.

Die angedeutete Fülle an Bewertungskriterien und möglichen Schutzmaßnahmen soll verdeutlichen, warum das Katholische Datenschutzzentrum keine pauschalen Empfehlungen für Kommunikationsanwendungen aussprechen kann. Die Beurteilung des datenschutzkonformen Einsatzes von solchen Kommunikationsanwendungen bleibt eine Einzelfallentscheidung.[33]

2.7.2 Benennung betrieblicher Datenschutzbeauftragter

Bei Vorliegen der in § 36 Abs. 1 und 2 KDG genannten Voraussetzungen haben kirchliche Stellen einen betrieblichen Datenschutzbeauftragten zu benennen. Die Benennung ist nach § 36 Abs. 4 S. 2 KDG dem Katholischen Datenschutzzentrum anzuzeigen.

Bei der Auswahl und der Benennung der betrieblichen Datenschutzbeauftragten ist von den kirchlichen Stellen sicherzustellen, dass die von § 36 Abs. 6 KDG geforderte erforderliche Fachkunde und Zuverlässigkeit vorhanden ist. Dabei ist auch zu beachten, dass der betriebliche Datenschutzbeauftragte durch weitere wahrzunehmende Aufgaben keinen Interessenkonflikten ausgesetzt wird (vgl. § 36 Abs. 7 KDG). Außerdem hat der Verantwortliche die nach § 37 KDG fachlich unabhängige Aufgabenwahrnehmung des betrieblichen Datenschutzbeauftragten sicherzustellen.

[31] Siehe die Entscheidung des EuGH, Jahresbericht 2020, Abschnitt 2.1.1.

[32] Zum CLOUD Act siehe auch das gemeinsame Papier des Europäischen Datenschutzbeauftragten und des Europäischen Datenschutzausschusses. Abrufbar unter: https://edps.europa.eu/sites/default/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf (nur in Englisch verfügbar).

[33] Siehe auch die Arbeitshilfe des Katholischen Datenschutzzentrums in Frankfurt zu diesem Thema (abrufbar unter: https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/Online-Meeting-Tools-04-2022-KDSZ-FFM.pdf).

Weiterhin sollten die Verantwortlichen in kirchlichen Einrichtungen ihrer Anzeigepflicht gegenüber der Datenschutzaufsicht nachkommen und die Meldung bei entsprechenden Änderungen umgehend aktualisieren.

2.7.3 Wahrnehmung von Betroffenenrechten

Betroffene können seit Einführung des KDG deutlich mehr Informationen über die Verarbeitung ihrer personenbezogenen Daten erhalten und Einfluss auf diese ausüben. Daher überrascht es nicht, dass die Beratung der katholischen Stellen bezüglich der Betroffenenrechte weiterhin einen Schwerpunkt der Arbeit des Katholischen Datenschutzzentrums darstellt.[34]

Besonders häufig werden Fragen zum Auskunftsanspruch gem. § 17 KDG an das KDSZ gerichtet. Dabei treten häufig Unsicherheiten zu Art und Umfang des Auskunftsanspruches auf.[35]

Das Recht auf Berichtigung der eigenen Daten gem. § 18 KDG und das Recht auf Löschung gem. § 19 KDG sind in der Beratungstätigkeit des Katholischen Datenschutzzentrums nicht so präsent.[36] Insgesamt sollten die kirchlichen Einrichtungen der gestiegenen Bedeutung der Betroffenenrechte noch stärkere Beachtung schenken und – soweit noch nicht geschehen – interne Prozesse vorsehen, damit sie die Betroffenenrechte, insbesondere das Recht auf Auskunft, auch gesetzeskonform erfüllen können.

2.8 Datenschutzrechtliche Hinweise zum Themenkreis „Videoüberwachung“

Das Thema der Videoüberwachung kirchlicher Gebäude und Räume bildet nach wie vor einen permanenten Schwerpunkt der Beratung katholischer Einrichtungen durch das Katholische Datenschutzzentrum. Auch im Jahr 2021 wurde eine Vielfalt von Fragestellungen in diesem Themenbereich an das KDSZ herangetragen. Der Großteil der Fragen kommt von Verantwortlichen katholischer Einrichtungen, die eventuelle Videoüberwachungen datenschutzkonform ausgestalten möchten.

Seit September 2020 kann in dieser Beratung inhaltlich auch eine neue „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ der Datenschutzkonferenz, des Gremiums der unabhängigen deutschen Datenschutzaufsichten des Bundes und der Länder, berücksichtigt werden. Die Orientierungshilfe ist eine Überarbeitung der Fassung aus dem Jahr 2014, die schon aufgrund der rasant fortschreitenden technischen Entwicklungen auf dem Gebiet der Video- und Übertragungstechnik notwendig wurde.

[34] Für einen Überblick der Betroffenenrechte siehe Abschnitt 3.4 ff des Jahresberichts 2020.

[35] Siehe dazu auch Abschnitt 2.5.1 dieses Jahresberichts. Einer detaillierteren Darstellung aktueller Fragen rund um den Auskunftsanspruch widmet sich auch der Beitrag Pau/Melzow, Das Auskunftsrecht nach § 17 KDG in der aufsichtsrechtlichen Praxis, in: KuR, 2021, Heft 2, S. 176 ff.

[36] Die Nichtbeachtung des Rechts auf Berechtigung hat dennoch in der Vergangenheit bereits zu Bußgeldern geführt und sollte daher von Verantwortlichen auch gewissenhaft behandelt werden (siehe Abschnitt 4.9 des Jahresberichts 2020).

Der Begriff der Videoüberwachung steht i. d. R. für einen oder beide der folgenden Verarbeitungsvorgänge: *Videobeobachtung*, bei der eine Live-Übertragung auf einen Monitor erfolgt und *Videoaufzeichnung*, bei der die Aufnahmen für eine bestimmte Zeit gespeichert werden und prinzipiell für Auswertungen zur Verfügung stehen. Bereits die Aufnahme von eindeutig identifizierbaren Personen stellt eine Verarbeitung personenbezogener Daten dar und unterliegt im kirchlichen Bereich dem Gesetz über den Kirchlichen Datenschutz. Der Einsatz von ausgeschalteten Kameras dürfte grundsätzlich nicht in den Anwendungsbereich des KDG fallen.[37]

„Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, um zulässig zu sein."

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, um zulässig zu sein. Im Bereich des KDG wird die Zulässigkeit der Videoüberwachung in § 52 KDG geregelt. Die Zulässigkeit der Videoüberwachung von Beschäftigten in nicht öffentlich zugänglichen Räumen richtet sich nach § 53 KDG.

§ 52 Abs. 1 KDG erlaubt eine Videoüberwachung zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkrete Zwecke, sofern sie erforderlich ist und die Interessen und Grundrechte der betroffenen Personen nicht überwiegen. Eine Differenzierung des beobachteten Raumes nach „öffentlichem" und „privatem" (beziehungsweise „kirchlichem") Eigentum erfolgt nicht. Zumindest bei legalem Betreten eines privaten Grundstückes oder Raumes (etwa einer Kirche oder eines Kirchplatzes) genießt jede Person grundsätzlich die gleichen Persönlichkeitsschutzrechte wie auf der offenen Straße.

Eine Beobachtung zur Aufgabenerfüllung i. S. d. Norm liegt vor, wenn der überwachte Raum einen kirchlichen Zweck erfüllt.[38] Das Hausrecht umfasst die Befugnis zu entscheiden, wer bestimmte kirchliche Gebäude und Räume betreten und sich darin aufhalten darf. Mit der Videoüberwachung zur Wahrnehmung des Hausrechts können zum einen präventive Zwecke verfolgt werden. Zweck der präventiven Maßnahme muss sein, dass Personen von der Begehung von Rechtsverstößen innerhalb des vom Hausrecht geschützten Bereichs abgehalten werden sollen. Auch repressive Zwecke können verfolgt werden, etwa wenn es um die Aufklärung von Straftaten oder die Durchsetzung zivilrechtlicher Schadensersatzansprüche geht.[39]

Das berechtigte Interesse ist als Auffangtatbestand zu verstehen und daher eng auszulegen. Es kann ideeller, wirtschaftlicher oder rechtlicher Natur sein.[40] Ferner muss es konkret belegt werden können, d. h. es darf nicht rein spekulativ oder subjektiv sein. Die bloße Befürchtung eines Einbruchs oder eine beabsichtigte Abschreckung ist keine ausreichende Grundlage für eine Überwachungsmaßnahme. Bei bereits dokumentierten Vorfällen oder besonderen Situationen, die nach der Lebenserfahrung ein besonderes Risiko für einen Einbruchsdiebstahl darstellen (etwa die Aufbewahrung und Ausstellung besonders wertvoller Kunstgegenstände) kann dagegen ein berechtigtes Interesse an einer Überwachung belegt werden.

[37] So entschied jedenfalls das OVG Rheinland-Pfalz im Bereich der DSGVO durch Urteil vom 25.06.2021 - 10 A 10302/21.OVG. Die im Urteil dargestellten Grundsätze dürften sich auf das KDG übertragen lassen.
[38] Vgl. Fuhrmann in: Sydow, Kirchliches Datenschutzrecht, 1. Auflage 2021, § 52 KDG Rn. 16.
[39] VG Oldenburg, Urteil vom 12.03.2013 – 1 A 3850/12.
[40] Vgl. Fuhrmann in: Sydow, Kirchliches Datenschutzrecht, 1. Auflage 2021, § 52 KDG Rn. 17–18.

Die Einwilligung als Rechtsgrundlage für die Videoüberwachung ist dagegen in fast allen Fällen untauglich zur Begründung der Rechtmäßigkeit einer Überwachung. In der Regel fehlen die vollständige Information der Beobachteten und die Freiwilligkeit der Zustimmung.

Wie bei jeder Verarbeitung personenbezogener Daten muss zunächst der Einsatz milderer Mittel geprüft werden, d. h. ob der Zweck der Überwachung auch mit anderen Mitteln, die weniger in die Persönlichkeitsrechte der Betroffenen eingreifen, erreicht werden kann. Beispielsweise könnte eine Verstärkung des passiven Einbruchschutzes (Sicherung von Türen und Fenstern) auch den Zweck der Sicherung des Eigentums erfüllen. Die Prüfung der alternativen Maßnahmen ist zu dokumentieren.

Das berechtigte Interesse des Verantwortlichen an einer Videoüberwachung ist gegen die legitimen Interessen der Betroffenen z. B. an einer ungestörten Privatsphäre abzuwägen. Dabei handelt es sich bei jeder Abwägung um eine Einzelfallentscheidung. Gerade im kirchlichen Bereich steht dabei das Recht auf freie Religionsausübung der Betroffenen im Vordergrund. Eingriffe in dieses Recht müssen so schonend wie möglich erfolgen. Das ist insbesondere bei der Videoüberwachung von Kirchengebäuden der Fall.

Grundsätzlich dürfte die Überwachung des gesamten Kirchenbereichs die Rechte der Besucher und Gläubigen in unangemessener Weise beeinträchtigen. Es sollte außerhalb der Gottesdienstzeiten sichergestellt werden, dass die Besucher die Möglichkeit haben, einen Platz zu finden, an dem sie ungestört und unbeobachtet beten können. Das gilt z. B. insbesondere im Bereich vor den Beichtstühlen. Während der Gottesdienste wird eine Videoüberwachung regelmäßig nicht erforderlich sein, weil in dieser Zeit im Allgemeinen keine konkreten Gefahren für Altäre, Kunstwerke und andere bedeutende Gegenstände bestehen.[41] Auch muss berücksichtigt werden, was ein Betroffener vernünftigerweise erwartet, z. B. sich zu normalen Zeiten unbeobachtet in einem Kirchenraum zum Gebet aufhalten zu können.

In diesem Rahmen ist auch das Prinzip der Minimierung der Datenverarbeitung zu beachten. Bei der Videobeobachtung ist in ihrer konkreten Ausgestaltung zu berücksichtigen, dass z. B. der Erfassungsbereich der Kameras auf die kritischen Orte und die Zeit der Beobachtung oder Aufzeichnung auf die kritischen Stunden (z. B. Zeiten ohne normalen Besucherverkehr) beschränkt werden. Bei einer Speicherung dürfen die Aufnahmen nur so lange verwahrt werden, wie es der Zweck der Speicherung verlangt. Werden z. B. Aufnahmen gespeichert, um eine eventuelle Straftat aufzuklären, reicht eine Speicherdauer von 72 Stunden i. d. R. aus, um die Relevanz der Aufnahmen zu beurteilen.

Der Verantwortliche hat über den Umstand der Videobeobachtung beziehungsweise Videoaufzeichnung angemessen, adressatengerecht, transparent und fair zu informieren. Das geschieht durch Hinweise, die auch zweistufig aufgebaut sein können: Ein vorgelagertes Hinweisschild informiert vor Betreten des überwachten Bereiches über die wichtigsten Aspekte der Videoüberwachung und weist auf die vollständigen Informationen hin, die auch in einem anderen Medium vorliegen

[41] Vgl. Fuhrmann in: Sydow, Kirchliches Datenschutzrecht, 1. Auflage 2021, § 52 KDG Rn. 40.

können, etwa auf der Homepage des Verantwortlichen. Ein Muster für das vorgelagerte Hinweisschild und die vollständige Information zur Videoüberwachung kirchlicher Immobilien kann im Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 04.07.2019 eingesehen oder auf der Website des Katholisches Datenschutzzentrums abgerufen werden.[42]

Videoüberwachung ist meistens eine Form der systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche, oft auch eine Verarbeitung besonderer Kategorien von personenbezogenen Daten (etwa bei der Auswertung biometrischer Merkmale). Ihre Einführung wird nach § 35 Abs. 4 lit. b) und c) KDG demnach in der Regel die Erstellung einer Datenschutz-Folgenabschätzung erfordern. An dieser sind der betriebliche Datenschutzbeauftragte und eventuell die Datenschutzaufsicht zu beteiligen (§ 35 Abs. 2, 3, 11 KDG).

Weitere Ausführungen, etwa auch eine ausführliche Darstellung der Rahmenbedingungen zur Videoüberwachung von Beschäftigten kann der Orientierungshilfe der DSK entnommen werden. Dort sind ebenfalls Ausführungen zu neuen technischen Entwicklungen wie Webcams, Dashcams und Drohnen enthalten.[43]

2.9 Konferenz der Diözesandatenschutzbeauftragten veröffentlicht technische Empfehlung zu Windows 10

Beim Betrieb eines Computers werden vom Betriebssystem viele – auch personenbezogene – Daten verarbeitet. Das auf Desktop-Rechnern und Laptops immer noch am häufigsten verwendete Betriebssystem Windows bietet vielfältige Konfigurationsmöglichkeiten im Bereich des Datenschutzes. Um den kirchlichen Einrichtungen Hilfestellungen für einen möglichst datensparsamen Betrieb von Windows an die Hand geben zu können, hat der Arbeitskreis Technik der Konferenz der Diözesandatenschutzbeauftragten technische Hinweise erarbeitet, die eine möglichst datensparsame Nutzung von Windows 10 aufzeigen wollen. Die Hinweise beschäftigen sich mit den bestehenden Problemen der Telemetriedatenübermittlung an Microsoft sowie weiteren notwendigen technischen Einstellungen zu einem datensparsamen Betrieb der Software.

Die generelle Problematik, ob Windows 10 in dem konkreten Nutzungsszenario aufgrund der Übermittlung personenbezogener Daten an ein Drittland überhaupt datenschutzkonform einsetzbar ist, ist nicht Inhalt dieser Arbeitshilfen und ist daher getrennt zu bewerten.

Im Mai 2021 wurden das Manteldokument sowie die ersten technischen Hinweise veröffentlicht. Im Laufe des Jahres wurden weitere technische Hinweise erarbeitet und über die Internetseiten der Diözesandatenschutzbeauftragten zur Verfügung gestellt. Auf der Internet-

[42] Beschluss abrufbar unter: https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2019/09/KDB-Muster-zur-Video%C3%BCberwachung-vom-04.07.2019.pdf

[43] Die Orientierungshilfe ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf

seite des Katholischen Datenschutzzentrums sind unter dem Menüpunkt „Infothek“ in der Rubrik „Arbeits- und Formulierungshilfen“ u. a. die Dokumente zum datensparsamen Betrieb von Windows 10 abgelegt und stehen zum Download bereit.

Im Manteldokument sind allgemeine Informationen sowie ausgewählte Referenzen zu Microsoft, dem Bundesamt für Sicherheit in der Informationstechnologie und der Datenschutzkonferenz zu Windows 10 enthalten. Die Reihe der technischen Hinweise richtet sich an Administratoren und andere Systemverantwortliche in kirchlichen Einrichtungen, um den Einsatz von Windows 10 datensparsam zu gestalten.

Bisher wurden zu folgenden Themen technische Hinweise bereitgestellt: Windows 10 Suchfunktion, Windows 10 Installation, Entfernung von automatisch installierten Applikationen, Online Spracherkennung und Webbrowser.[44]

2.10 Datenvernichtung durch Überflutung und Hochwasser

Am 14. und 15.06.2021 waren große Gebiete im Westen Deutschlands von einer Flutkatastrophe betroffen. Unvorstellbare Wassermassen überfluteten in kürzester Zeit ganze Orte und Stadtteile. Dabei wurden auch zahlreiche kirchliche Einrichtungen (z. B. Schulen, Caritas-Stationen, Krankenhäuser) in ihrer Bausubstanz und ihrem Inventar stark beschädigt. Im Zuständigkeitsbereich des Katholischen Datenschutzzentrums waren u. a. Gebiete im Raum Hagen (Westf.), im Bergischen Land, im rechtsrheinischen Bereich von Wupper und Sieg sowie linksrheinisch im Raum Euskirchen und Düren betroffen.

Oft wurden ganze Aktenräume samt Inhalt zerstört oder viele Aktenmeter in Fußbodennähe durchnässt und beschädigt. In der Folge erreichten das Katholische Datenschutzzentrum etliche Meldungen von Datenschutzverletzungen, da die personenbezogenen Daten, die in diesen Akten enthalten waren, durch die Beschädigungen verloren gegangen und jetzt nicht mehr verfügbar sind.

Nach Ablauf einiger Wochen, in denen bei den betroffenen Einrichtungen die nötigsten Aufräumarbeiten und vor allem die Sicherstellung der eigenen Arbeit im Fokus standen, hat das Katholische Datenschutzzentrum mit den betroffenen Einrichtungen überlegt, welche Erkenntnisse für die Zukunft, also für die Neueinrichtung von Aktenräumen und Registraturen umgesetzt werden sollten.

Nach den Erfahrungen der Flutkatastrophe wurde der Auswahl des Raumes für die Aktenlagerung große Bedeutung zugemessen. Der Raum sollte möglichst (hochwasser-)sicher sein. Dabei sollte ein möglicher Wassereintritt sowohl „von innen“ durch z. B. Abflüsse, Ausgüsse oder Toiletten als auch „von außen“ durch Türen und Fenster berücksichtigt werden.

[44] Siehe Abschnitt 4.3.4 dieses Berichts.

Wasser-Warngeräte können erste Flutungen melden und – zumindest bei langsam steigenden Hochwässern – eine rechtzeitige Evakuierungen der Menschen wie auch evtl. noch die Sicherung wichtiger Akten anstoßen.

Daneben wurden mit den kirchlichen Einrichtungen die folgenden vorausschauenden organisatorischen Maßnahmen als mögliche Gesichtspunkte bei der Neuorganisation von Aktenräumen besprochen:

- Die Anordnung der Ablage in den Regalen kann z. B. nach Wichtigkeit und Restlaufzeit der Aufbewahrungsfrist in den Regalen von oben nach unten erfolgen. Die wichtigsten Unterlagen und solche mit langer Restlaufzeit wären dann am wenigsten durch eindringendes Wasser bedroht.

- Die Digitalisierung von Informationen kann den Bedarf für die Aufbewahrung von Papierunterlagen vermindern. Auch kann mit einer digitalen Kopie neben dem Papierbestand einem Totalverlust der Unterlagen bei Überflutung vorgebeugt werden. Ein Backup der Daten auf verschiedenen Medien und an verschiedenen Orten erhöht die Wiederherstellbarkeit und damit die Verfügbarkeit der Daten.

- Die Aufbewahrungs- beziehungsweise Löschfristen sind zu beachten. Mit der Erledigung des Zweckes der Verarbeitung und dem Ablauf eventuell längerer gesetzlicher Aufbewahrungsfristen (z. B. aus handels- oder steuerrechtlichen Vorgaben) sind die personenbezogenen Daten zu löschen. Diese Daten sollten daher in einem strukturierten Prozess gelöscht und vernichtet werden. Durch eine regelmäßige Aktenvernichtung nach Ablauf der Aufbewahrungsfristen kann sich der Aufwand für die Aufbewahrung und Sicherung von Papierakten verringern. Für die kirchlichen Stellen ist dabei zu beachten, dass vor der Löschung von Daten beziehungsweise der Vernichtung von Papierakten die Daten beziehungsweise Akten dem Diözesanarchiv der jeweiligen (Erz-)Diözese anzubieten sind. Nur soweit das Archiv die Akten beziehungsweise Daten nicht in das Archiv aufnimmt, können diese gelöscht beziehungsweise vernichtet werden.

- Auch bei der Vernichtung von „nassen Akten" ist eine datenschutzkonforme Behandlung und Vernichtung sicherzustellen. Bei der Trocknung/Restauration und auch im Vernichtungsprozess ist die Vertraulichkeit zu wahren. Bei der Vernichtung können herkömmliche Aktenvernichtungsgeräte und auch die „Datentonne" von Entsorgern an ihre Grenzen stoßen, wenn durchnässte und verklebte, evtl. sogar kontaminierte Papierstapel verarbeitet werden müssen.

Alle kirchlichen Einrichtungen, bei denen eine Überflutung der Räume zur Aufbewahrung von Akten nicht ausgeschlossen werden kann, sollten die vorhandenen Ablageorte im Hinblick auf ihre Hochwasser-Festigkeit bewerten und eventuell notwendige Maßnahmen zur Risikominderung schnell umsetzen.

„Alle kirchlichen Einrichtungen, bei denen eine Überflutung der Räume zur Aufbewahrung von Akten nicht ausgeschlossen werden kann, sollten die vorhandenen Ablageorte im Hinblick auf ihre Hochwasser-Festigkeit bewerten und eventuell notwendige Maßnahmen zur Risikominderung schnell umsetzen."

2.11 Kann auf den Schutz technischer und organisatorischer Maßnahmen verzichtet werden?

Verantwortliche sind nach § 26 Abs. 1 KDG[45] dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten und den Rechten Betroffener zu treffen. Die Maßnahmen müssen dem jeweiligen Schutzniveau der personenbezogenen Daten angepasst werden. Dies kann durch den Verantwortlichen oder den Auftragsverarbeiter u. a. mithilfe der in Absatz 1 aufgezählten Maßnahmen erreicht werden. Wie hoch das Schutzniveau sein muss, muss gemäß § 26 Abs. 2 KDG durch den Verantwortlichen ermittelt werden. Eine Kategorisierung der Schutzklassen und -niveaus wird in den §§ 11 ff. KDG-DVO vorgenommen. Dort finden sich auch Beispiele für geeignete technische Standards, z. B. für den Schutz von IT-Systemen.

In der Diskussion, ob durch betroffene Personen in ein niedrigeres als das gesetzlich geforderte Schutzniveau eingewilligt werden kann und es sich damit bei § 26 KDG um disponible Vorgaben handelt, hat die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland ihren Beschluss von September 2019[46] mit Beschluss vom 15.06.2022 aufgehoben und ihre Stellung zu dem Thema angepasst.[47] Nunmehr vertritt die Konferenz der Diözesandatenschutzbeauftragten die Ansicht, dass der Verantwortliche sicherstellen muss, dass ein entsprechendes Schutzniveau gewährleistet wird und auf Betroffenenseite in das Nichtanwenden von einzelnen technischen und organisatorischen Schutzmaßnahmen gemäß § 6 Abs. 1 lit. b) beziehungsweise § 11 Abs. 2 lit. a) KDG auf informierte Weise eingewilligt werden kann. Diese Dispositionsbefugnis soll aber nur gegeben sein, wenn der Verantwortliche eine Übermittlung der betreffenden personenbezogenen Daten auch auf gesichertem Weg (ohne Wegfall einzelner, im konkreten Fall in die Disposition des Betroffenen fallende Maßnahmen) anbietet und diese Wahlmöglichkeit der betroffenen Person keinen Nachteil bringt.

In der Praxis des Katholischen Datenschutzzentrums tritt diese Problematik beispielsweise häufig in Bezug auf E-Mails auf. Nach Durchführung der Risikoanalyse und Feststellung des notwendigen Schutzniveaus für die konkrete Verarbeitung durch den Verantwortlichen kann es für den Schutz mancher Datenkategorien angezeigt sein, dass der E-Mail-Verkehr Ende-zu-Ende verschlüsselt wird. Da sich dies als aufwendig erweisen kann, wollen Verantwortliche von dem Erfordernis der E-Mail-Verschlüsselung häufig abweichen. Da gemäß dem Beschluss der Konferenz die Dispositionsbefugnis über den Entfall eigentlich notwendiger technisch-organisatorischer Schutzmaßnahmen nur gegeben sein soll, wenn der Verantwortliche eine Übermittlung der betreffenden personenbezogenen Daten auch auf gesichertem Weg (ohne Wegfall

[45] Art. 32 DSGVO ist die korrespondierende Vorschrift im staatlichen Datenschutzrecht.

[46] Die Konferenz der Diözesandatenschutzbeauftragten hatte zunächst mit Beschluss vom September 2019 vertreten, dass es sich bei den Anforderungen aus § 26 KDG um nicht abdingbare Vorgaben handele und betroffene Personen nicht in ein niedrigeres Schutzniveau einwilligen können (dieser – mittlerweile überholte – Beschluss aus 2019 kann auf der Internetseite des Katholischen Datenschutzzentrums unter Infothek ➪ Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten abgerufen werden).

[47] Der aktuelle Beschluss von Juni 2022 kann ebenfalls auf der Internetseite des Katholischen Datenschutzzentrums unter Infothek ➪ Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten abgerufen werden.

einzelner, im konkreten Fall in die Disposition des Betroffenen fallende Maßnahmen) anbietet und diese Wahlmöglichkeit der betroffenen Person keinen Nachteil bringt, kann ein Verantwortlicher in dem Beispiel also nicht vermeiden, eine E-Mail-Verschlüsselung als Alternative einzurichten, selbst wenn betroffene Personen eine nicht verschlüsselte Kommunikation wünschen.

2.12 Keine Gruppenfotos im Internet ohne Einwilligung

Mit einer Entscheidung des Oberverwaltungsgerichts Lüneburg wurde mit der Thematik rund um die Einwilligung für die Veröffentlichung von Fotos ein Thema erneut beleuchtet, das unmittelbar nach Einführung des KDG 2018 für viel Aufregung und Diskussion gesorgt hatte.

Das OVG Lüneburg hat am 19.01.2021 entschieden, dass ein Verantwortlicher wegen einer Veröffentlichung eines Gruppenfotos im Internet, ohne dass alle abgebildeten Personen der Veröffentlichung zugestimmt hatten, zu Recht verwarnt wurde.[48]

Kläger war ein Ortsverein einer Partei, welcher das streitgegenständliche Foto – welches vier Jahre zuvor während einer öffentlichen Veranstaltung in Form eines Ortstermins im Zusammenhang mit dem Bau einer Ampelanlage entstanden war – auf seiner Facebookseite veröffentlichte, um über seine parteipolitischen Aktivitäten und Erfolge zu informieren und damit – jedenfalls mittelbar – auch an der politischen Willensbildung des Volkes mitzuwirken. Dieses Anliegen stellte aus Sicht des Gerichts ein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 lit. f) DSGVO dar.

Neben der Feststellung, dass ein berechtigtes Interesse vorliegt, sind für eine Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 lit. f) DSGVO auch die Erforderlichkeit und eine Interessenabwägung von zentraler Bedeutung. Der in der Datenschutz-Grundverordnung nicht gesondert definierte Begriff der Erforderlichkeit ist unter Berücksichtigung von Erwägungsgrund 39 Satz 9 DSGVO dahingehend auszulegen, dass die Erforderlichkeit zu bejahen ist, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Kann das Ziel einer Datenverarbeitung auch durch die Verarbeitung anonymisierter Daten erreicht werden, ist eine nicht-anonymisierte Verarbeitung nicht erforderlich. Die Datenverarbeitung ist somit auf das „absolut Notwendige“ zu begrenzen.

Für den konkreten vom Gericht beurteilten Fall bedeutete dies, dass es für die Wahrung des berechtigten Interesses des Klägers als Verantwortlichen nicht darauf ankam, dass gerade die betroffenen Personen als solche (Individuen) in einen spezifischen Kontext zur politischen Tätigkeit des Klägers gesetzt werden. Da es dem Kläger nur darum gegangen sei, zu dokumentieren, dass das Thema, für das er sich politisch eingesetzt habe, eine größere Anzahl von Personen interessiere,

[48] OVG Lüneburg, Beschluss vom 19.01.2021, Az. 11 LA 16/20; abgerufen am 25.03.2022 unter der URL: https://www.rechtsprechung.niedersachsen.de/jportal/portal/page/bsndprod.psml?doc.id=MWRE210000311&st=ent&doctyp=juris-r&showdoccase=1&paramfromHL=true#focuspoint

reiche es in diesem Fall aus, das streitgegenständliche Foto unter Unkenntlichmachung der abgebildeten Personen, z. B. durch Verpixelung der Gesichter, zu verwenden. Dies sei auch zumutbar, da eine Verpixelung mithilfe gängiger Bildbearbeitungssoftware ohne erheblichen Kosten- und Zeitaufwand umgesetzt werden könne. Zudem sei weder davon auszugehen, dass eine Unkenntlichmachung der betroffenen Personen auf dem streitgegenständlichen Foto zu einem Wegfall der Glaubwürdigkeit beziehungsweise Seriosität des Facebook-Posts und des vom Kläger mit der Veröffentlichung verfolgten Ziels geführt hätte, noch dass durch eine Unkenntlichmachung die Mitwirkung an der politischen Willensbildung maßgeblich beeinträchtigt worden wäre.

Zudem vermochte der Kläger nicht mit seinem Vortrag durchzudringen, dass die betroffenen Personen „lediglich in einer großen Menschenmenge" gezeigt würden. Denn nach Art. 4 Nr. 1 DSGVO komme es allein darauf an, ob die betroffene Person direkt oder indirekt, insbesondere mittels Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden könne.

In diesem Zusammenhang wies das Gericht auch auf den Unterschied zwischen einer zeitnahen Veröffentlichung von Pressefotos öffentlicher Veranstaltungen in gedruckten Medien und einer – wie im gegebenen Fall – Jahre später erfolgenden Verwendung der Aufnahmen in sozialen Medien oder anderen Internetdarstellungen hin. Es habe keine Beziehung zwischen den betroffenen Personen und dem Kläger vorgelegen, die eine Veröffentlichung des streitgegenständlichen Fotos mehr als vier Jahre später vernünftigerweise absehbar gemacht hätte.

Auch seien bei der nach Art. 6 Abs. 1 lit. f) DSGVO vorzunehmenden Interessenabwägung die für die Betroffenen mit der Datenverarbeitung verbundenen Risiken, einschließlich einer evtl. Missbrauchsanfälligkeit, zu berücksichtigen. So sei eine Veröffentlichung von Fotos im Internet im Allgemeinen und in sog. sozialen Netzwerken wie Facebook im Besonderen mit erheblichen (Missbrauchs)Risiken für die Betroffenen verbunden. Diese Risiken ergäben sich primär daraus, dass ein einmal im Internet veröffentlichtes Foto beliebig oft und von einer unbestimmten Vielzahl von Personen gespeichert, vervielfältigt, verfremdet und an andere Personen übermittelt werden könne. Werde ein Foto verändert und anschließend weitergeleitet, sei es für den Empfänger des veränderten Fotos i. d. R. noch nicht einmal erkennbar, ob beziehungsweise in welchen Punkten das Foto vom Original abweiche. Hinzu komme, dass es sich bei Facebook um ein weltweit verbreitetes und von Millionen von Menschen genutztes Netzwerk handele. Durch die Kumulation dieser beiden Faktoren – erhebliche Missbrauchsmöglichkeiten und große Reichweite – sei es für die Betroffenen sehr schwierig bis unmöglich, den Überblick über sämtliche über sie veröffentlichte Daten zu behalten und ggf. sämtliche veröffentlichte Daten dauerhaft und restlos aus dem Internet entfernen zu lassen.

Ein weiterer vom Gericht angesprochener Punkt war, dass das Foto ohne Kenntnis der betroffenen Personen aufgenommen wurde. Damit hätten diese bereits zum Zeitpunkt der Datenerhebung keinerlei Kontrolle über ihre Daten gehabt und konnten sich bis zur Kenntniserlangung über die streitgegenständliche, erst vier Jahre nach Erstellung des

Fotos erfolgte Veröffentlichung nicht gegen die (weitere) Verarbeitung ihrer personenbezogenen Daten wehren.

Dass „lediglich" die Sozialsphäre der betroffenen Personen tangiert worden sei, führe zu keiner anderen Beurteilung. Denn zum einen seien auch personenbezogene Daten, die „nur" die Sozialsphäre betreffen, vom Schutz der Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 DSGVO erfasst und einer – grundsätzlich ergebnisoffenen – Abwägung nach Art. 6 Abs. 1 lit. f) DSGVO zugänglich. Zum anderen werde die Intensität des Eingriffs in die Persönlichkeits- und Datenschutzrechte der betroffenen Personen vorliegend gerade dadurch erhöht, dass mit der Veröffentlichung des streitgegenständlichen Fotos auf der Facebook-Seite des Klägers die aufgezeigten, besonderen Risiken verbunden sind. Diese Risiken bestünden unabhängig davon, ob es sich um ein Bild von einer öffentlichen oder einer privaten Veranstaltung handelt.

Die Entscheidung des OVG ist auch für die kirchlichen Stellen relevant, da die kirchliche Regelung des § 6 Abs. 1 lit. g) KDG parallel zu der dem Beschluss zugrunde liegenden Regelung des Art. 6 Abs. 1 lit. f) DSGVO ausgestaltet ist und daher die Erwägungen des Gerichts auch auf die Gestaltung im kirchlichen Bereich übertragen werden können.

Der Beschluss des OVG Lüneburg zeigt, dass auch beim Vorliegen eines berechtigten Interesses genauestens zu prüfen ist, ob die Verarbeitung der personenbezogenen Daten zur Wahrung dieses Interesses auch tatsächlich erforderlich ist. Zudem hat eine umfassende, auf den konkreten Einzelfall bezogene Abwägung der widerstreitenden Interessen zu erfolgen, bei der verschiedenste Punkte Berücksichtigung finden und unterschiedlich gewichtet werden können.

3 Das Katholische Datenschutzzentrum

Das Katholische Datenschutzzentrum als Körperschaft des öffentlichen Rechts bildet den Rahmen für die Arbeit des Diözesandatenschutzbeauftragten (DDSB).

3.1 Aktuelles aus dem Katholischen Datenschutzzentrum

Im Berichtszeitraum gab es nicht nur viele berichtenswerte fachliche Themen, sondern auch Mitteilungen zur Arbeit des Katholischen Datenschutzzentrums selbst.

3.1.1 Katholische (Erz-)Diözesen in NRW bestätigen ihren Diözesandatenschutzbeauftragten

Mit Wirkung zum 01.09.2021 haben die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster Steffen Pau erneut für fünf Jahre zum Diözesandatenschutzbeauftragten bestellt. Er nimmt damit weiterhin die kirchliche Datenschutzaufsicht für die katholischen Einrichtungen in den fünf (Erz-)Diözesen (in Münster für den nordrhein-westfälischen Teil der Diözese) wahr und leitet das Katholische Datenschutzzentrum (KdöR) in Dortmund.

Zugleich hat der Vorsitzende der Deutschen Bischofskonferenz, Bischof Dr. Georg Bätzing, mit Wirkung zum 01.09.2021 Steffen Pau ebenfalls für fünf Jahre erneut als Datenschutzaufsicht für den Verband der Diözesen Deutschlands (KdöR), dem Rechtsträger der Deutschen Bischofskonferenz, und dessen Einrichtungen bestellt.

3.1.2 Das Katholische Datenschutzzentrum (KdöR) besteht seit fünf Jahren

Das Katholische Datenschutzzentrum konnte am 01.09.2021 auf fünf Jahre erfolgreicher Arbeit zurückblicken. Das Datenschutzzentrum wird vom gemeinsamen Diözesandatenschutzbeauftragten der fünf nordrhein-westfälischen (Erz-)Diözesen geleitet und unterstützt diesen bei der Ausübung der Datenschutzaufsicht über die katholischen Einrichtungen in den fünf (Erz-)Diözesen Aachen, Essen, Köln, Münster und Paderborn. Eine Datenschutzaufsicht in den einzelnen (Erz-)Diözesen gab es parallel zu den staatlichen Datenschutzaufsichten bereits vor der Gründung des Katholischen Datenschutzzentrums, aber erst mit dem Amtsantritt des ersten gemeinsamen Diözesandatenschutzbeauftragten für die fünf nordrhein-westfälischen (Erz-)Diözesen am 01.09.2016 nahm auch das Katholische Datenschutzzentrum seine übergeordnete Arbeit auf.

Diese Entscheidung, dem gemeinsamen Diözesandatenschutzbeauftragten auch organisatorisch eine unabhängige Basis in Form des Katholischen Datenschutzzentrums als einer Körperschaft des öffentlichen Rechts zu geben, war vorbildhaft. In der Folge entstand für die südwestlichen (Erz-)Diözesen in Deutschland das „Katholische Datenschutzzentrum Frankfurt am Main" (KdöR). Auch die Freisinger Bischofskonferenz plant zur Unterstützung des gemeinsamen Diözesandatenschutzbeauftragten der bayerischen (Erz-)Diözesen ein „Kirchliches Datenschutzzentrum" in Nürnberg zu errichten.

Das Katholische Datenschutzzentrum in Dortmund war von den fünf nordrhein-westfälischen (Erz-)Diözesen als Umsetzung der Rechtsprechung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden als eigenständige und unabhängige Körperschaft des öffentlichen Rechts gegründet worden. Der Diözesandatenschutzbeauftragte ist zugleich Leiter dieser Körperschaft. Das für die Erfüllung der Aufgabe der Datenschutzaufsicht notwendige Personal ist bei dem Katholischen Datenschutzzentrum als Körperschaft direkt angestellt. Mit dieser organisatorischen Trennung und der im Gesetz über den Kirchlichen Datenschutz festgeschriebenen Unabhängigkeit der Funktion des Diözesandatenschutzbeauftragten ist sichergestellt, dass die Datenschutzaufsicht die gesetzlich vorgesehene Kontrollfunktion auch unbeeinflusst wahrnehmen kann.

3.1.3 Informationsaustausch mit der neuen Landesdatenschutzbeauftragten Bettina Gayk

Im September 2021 besuchten der Diözesandatenschutzbeauftragte und seine Stellvertreterin die neu gewählte Landesdatenschutzbeauftragte Bettina Gayk in Düsseldorf und wünschten ihr für ihr neues Amt alles Gute und viel Erfolg. Die Gesprächsteilnehmer tauschten sich über aktuelle Fragen und gemeinsame Themen aus.

3.2 Zuständigkeitsbereich

Der Diözesandatenschutzbeauftragte und Leiter des Katholischen Datenschutzzentrums ist als Datenschutzaufsicht im Sinne des Art. 91 Abs. 2 DSGVO und der §§ 42 ff. KDG zuständig für die Erzdiözese Köln, die Erzdiözese Paderborn, die Diözese Aachen, die Diözese Essen und die Diözese Münster (nordrhein-westfälischer Teil). Diese sind von der Fläche deckungsgleich mit dem Bundesland Nordrhein-Westfalen. Hinzu kommen noch einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zur Erzdiözese Köln gehören, und von Niedersachsen und Hessen, die zur Erzdiözese Paderborn gehören. In diesem Gebiet leben fast 6,6 Millionen Menschen römisch-katholischen Glaubens (Stand 2020).

Neben den fünf (Erz-)Bischöflichen Generalvikariaten als den zentralen Verwaltungsbehörden der (Erz-)Diözesen werden die vielen Pfarreien vor Ort vom Katholischen Datenschutzzentrum betreut. Hinzu kommen fünf Caritasverbände auf Diözesanebene und 89 örtliche Verbände der

Caritas mit ihren Beratungsangeboten und Beratungsstellen (Stand 2018). Daneben gibt es in den fünf (Erz-)Diözesen noch über 140 Schulen in kirchlicher Trägerschaft, über 2.600 katholische Kindergärten, rund 200 katholische Krankenhäuser, über 1.200 Altenpflegeeinrichtungen und rund 390 Einrichtungen der Jugendhilfe, für die der DDSB zuständig ist (Stand 2018). Darüber hinaus fallen noch diverse Vereine, Verbände und Stiftungen im kirchlichen Bereich in die Zuständigkeit des DDSB. Auch die Bundesverbände kirchlicher Vereinigungen, die ihren Sitz in Nordrhein-Westfalen haben, fallen aufgrund ihres Sitzes in die Zuständigkeit des Katholischen Datenschutzzentrums.

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands[49] zuständig. Der VDD ist Rechtsträger der Deutschen Bischofskonferenz. Er wurde 1968 als Körperschaft des öffentlichen Rechts gegründet. Im VDD sind die 27 rechtlich und wirtschaftlich selbstständigen (Erz-)Diözesen zusammengeschlossen. Neben dem Sekretariat der Deutschen Bischofskonferenz in Bonn gehören unter anderem die Geschäftsstelle des VDD in Bonn, das Kommissariat der deutschen Bischöfe – Katholisches Büro in Berlin und weitere Einrichtungen des VDD zum Zuständigkeitsbereich des Katholischen Datenschutzzentrums.

3.3 Aufbau der Einrichtung

Das Katholische Datenschutzzentrum ist eine eigenständige Körperschaft des öffentlichen Rechts. Die Körperschaft des öffentlichen Rechts wurde von den Erzdiözesen Köln und Paderborn und den Diözesen Aachen, Essen und Münster gegründet[50].

In den Verwaltungsrat des Katholischen Datenschutzzentrums haben die (Erz-)Bischöfe ihre jeweiligen Generalvikare entsandt. Der Vertreter der Erzdiözese Paderborn, Herr Generalvikar Hardt, wurde vom Verwaltungsrat zum Vorsitzenden des Gremiums gewählt, die Geschäftsführung wurde dem Leiter des Katholischen Datenschutzzentrums übertragen.

Die Leitung des Katholischen Datenschutzzentrums nimmt der gemeinsame Diözesandatenschutzbeauftragte der fünf Mitgliedsdiözesen wahr. Er vertritt die Körperschaft nach außen.

Dem DDSB sind eine Vertreterin, Referenten und Sachbearbeiter zur Seite gestellt, die auch vom Katholischen Datenschutzzentrum selbst angestellt sind. Es sind im Berichtszeitraum elf Stellen vorgesehen, die zum Jahresende nicht alle besetzt sind.

Durch die eigenständige Körperschaft des öffentlichen Rechts und das im eigenen Haus angestellte Personal wird die notwendige Unabhängigkeit des Diözesandatenschutzbeauftragten und seiner Mitarbeitenden gewährleistet.

[49] Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter".

[50] Siehe hierzu auch Marcus Baumann-Gretza, Zur Entstehungsgeschichte und Struktur des Katholischen Datenschutzzentrums in Dortmund, in: Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung (Band 2 der Schriften zum kirchlichen Datenschutz des KDSZ), Dortmund 2021, S. 81-90.

	Soll	Ist
Leitung (Diözesandatenschutzbeauftragter und Vertreterin)	2	2
Referentinnen/Referenten	5	5
Sachbearbeiterinnen/Sachbearbeiter inkl. Sekretariat	4	3
Gesamt	11	10

Abb.: Stellensoll des KDSZ und besetzte Stellen

„Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofs vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden geachtet."

Bei der Planung des Katholischen Datenschutzzentrums wurde konsequent auf die Umsetzung des Urteils des Europäischen Gerichtshofs vom 09.03.2010 zur Unabhängigkeit und Selbständigkeit der Datenschutzaufsichtsbehörden[51] geachtet und die Veränderungen durch die Europäische Datenschutz-Grundverordnung beziehungsweise deren Umsetzung in kirchliches Recht wurden berücksichtigt.

Das Katholische Datenschutzzentrum hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn.

Nach der Übernahme der Aufgaben des Diözesandatenschutzbeauftragten der fünf (Erz-)Diözesen in NRW zum 01.09.2016, konnten in den folgenden Jahren, auch im Berichtszeitraum unter den Bedingungen der Corona-Pandemie, der Aufbau das Katholischen Datenschutzzentrums vorangetrieben und die Erfüllung der Aufgaben sichergestellt werden.

3.4 Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums

Mit der Gründung des Katholischen Datenschutzzentrums als der gemeinsamen Datenschutzaufsicht der fünf nordrhein-westfälischen (Erz-)Diözesen wurde dem Katholischen Datenschutzzentrum von den (Erz-)Diözesen auch ein Schutzpatron mitgegeben.

Der hl. Ivo lebte im 13. Jahrhundert in der Bretagne. Der Bischof von Tréguier ernannte den Priester, der auch Rechtswissenschaften studiert hatte, zu seinem Offizial. Dieses kirchliche Richteramt füllte er mit Mut und Unbestechlichkeit aus und setzte sich vor allem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein, was ihm den Ruf eines „Anwalts der Armen" einbrachte. Er wurde im 14. Jahrhundert heiliggesprochen. Sein Gedenktag ist der 19. Mai. Die Reliquien des hl. Ivo werden in der Kathedrale von Tréguier aufbewahrt[52].

[51] Siehe hierzu auch Burkhard Kämper / Jan Gers, Handlungsbedarf für die katholische Kirche durch das Urteil des EuGH von 2010 zur Unabhängigkeit der Datenschutzaufsichten in Deutschland, in: Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung (Band 2 der Schriften zum kirchlichen Datenschutz des KDSZ), Dortmund 2021, S. 69 - 80.

[52] Ausführlich zum Leben und Wirken des hl. Ivo: Michael Streck / Annette Rieck, St. Ivo (1247-1303) - Schutzpatron der Richter und Anwälte, 2007; Artikel „Ivo Hélory" auf Wikipedia (https://de.wikipedia.org/wiki/Ivo_Hélory). In dem Beitrag bei Wikipedia wird auch erwähnt, dass der hl. Ivo das Siegel des Katholischen Datenschutzzentrums ziert.

Das Bildnis des hl. Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums, sodass der Schutzpatron in der täglichen Arbeit immer gegenwärtig ist.

Abb.: Darstellung des Siegels des KDSZ im Amtsblatt der Erzdiözese Paderborn

3.5 Aufgabenkatalog

Die Aufgaben des Diözesandatenschutzbeauftragten beziehungsweise des Verbandsdatenschutzbeauftragten des VDD als Datenschutzaufsicht sind im KDG beziehungsweise im KDG-VDD[53] beschrieben. Wer der Ansicht ist, dass bei der Verarbeitung von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 48 KDG an die Datenschutzaufsicht wenden. Diese prüft den Sachverhalt und hört dazu die beteiligte kirchliche Stelle an, soweit ein Verstoß gegen datenschutzrechtliche Regelungen vorliegen könnte. Wichtig ist dabei das Benachteiligungsverbot des § 48 Abs. 3 KDG: „Niemand darf gemaßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an die Datenschutzaufsicht gewendet hat."

Das Überwachen der Einhaltung datenschutzrechtlicher Vorgaben gehört nicht nur im Rahmen der Beschwerdebearbeitung, sondern als allgemeine Kernaufgabe zu den Tätigkeiten der Datenschutzaufsicht (vgl. § 44 Abs. 1 KDG).

§ 44 Abs. 3 lit. g) KDG ergänzt § 44 Abs.1 KDG. Danach soll die Datenschutzaufsicht „Untersuchungen über die Anwendung dieses Gesetzes durchführen, auch auf Grundlage von Informationen einer anderen Datenschutzaufsicht oder einer anderen Behörde."

Auf Basis dieser Regelung kann und muss die Datenschutzaufsicht Überprüfungen auf Grundlage der bei ihr eingehenden Beschwerden vornehmen. Sie kann aber auch ohne den konkreten Bezug zu einer Beschwerde anlasslos prüfen, ob Einrichtungen das Gesetz richtig anwenden[54].

[53] Im Folgenden wird nicht immer explizit auf die gleichlautende Vorschrift des KDG-VDD verwiesen.

[54] Vgl. Hense in Sydow, Kirchliches Datenschutzrecht, § 44 KDG, Rn. 27; zur Auslegung der inhaltsgleichen Vorschrift des Art. 57 Abs. 1 lit. h) DSGVO vgl. Selmayr in Ehmann/Selmayr, Kommentar DSGVO, 2. Aufl. 2018, Art. 57 Rn. 9 und Kugelmann/Buchmann in Schwartmann u. a., Heidelberger Kommentar DSGVO/BDSG, 2. Aufl. 2020, Art. 57 Rn. 74.

Für kirchliche Stellen im Sinne des § 3 Abs. 1 KDG macht § 44 Abs. 2 KDG nochmals deutlich, dass sie die Arbeit der Datenschutzaufsicht durch Auskünfte, die Ermöglichung von Einsichtnahme in Akten und Räume zu unterstützen und Untersuchungen und Prüfungen zuzulassen haben. Den Anweisungen der Datenschutzaufsicht ist nach § 44 Abs. 2 lit. a) KDG Folge zu leisten.

Hierzu führt sie anlassbezogen aufgrund der bei ihr eingehenden Beschwerden oder ohne Anlass – im Rahmen regelmäßiger Kontrollen – Prüfungen zur Verbesserung des Datenschutzes durch[55]. Hierbei spielt die Einhaltung der rechtlichen Vorgaben (Datenschutzrecht) ebenso eine Rolle wie die Umsetzung der notwendigen technisch-organisatorischen Schutzmaßnahmen gemäß den datenschutzrechtlichen Vorgaben (Datensicherheit). Beide Komponenten, die Umsetzung der rechtlichen Vorgaben und der technisch-organisatorischen Schutzmaßnahmen, müssen beachtet werden, damit Datenschutz wirksam werden kann und die betroffenen Personen den gesetzlich vorgesehenen Schutz genießen können.

Kommt die Datenschutzaufsicht im Rahmen einer Prüfung oder der Bearbeitung einer Beschwerde zu dem Ergebnis, dass ein bestimmter von der kirchlichen Stelle durchgeführter oder unterlassener Vorgang bei der Verarbeitung personenbezogener Daten zu beanstanden ist, wird dies dokumentiert und dem Verantwortlichen schriftlich mitgeteilt. Je nach Schwere des Verstoßes gegen die datenschutzrechtlichen Vorgaben kann das Katholische Datenschutzzentrum verschiedene Maßnahmen ergreifen, die bis zu einer Untersagung der konkreten Datenverarbeitung und der Verhängung eines Bußgeldes reichen können.

Um datenschutzrechtlichen Verstößen vorzubeugen, steht das Team des Katholischen Datenschutzzentrums im Rahmen seiner Aufgaben beratend zur Verfügung, um über die Anforderungen der datenschutzrechtlichen Regelungen zu informieren. Die Datenschutzaufsicht kann als Referent oder mit schriftlichen Informationen allgemeine Hinweise zur Umsetzung des Datenschutzes geben oder im Wege der Beratung im Einzelfall weiterhelfen.

3.6 Finanzen

Das Katholische Datenschutzzentrum wird von den fünf (Erz-)Diözesen als Mitgliedern der Körperschaft des öffentlichen Rechts getragen. Wie in § 43 Abs. 4 KDG beschrieben, stellen sie die für die Erfüllung der Aufgaben des Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung. Außerdem verfügt der DDSB über einen eigenen jährlichen Haushalt.

Für das Kalenderjahr 2021 hat der Verwaltungsrat des Katholischen Datenschutzzentrums auf Vorschlag des Diözesandatenschutzbeauftragten den Haushaltsplan in Höhe von 1.390.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben bewilligt. Für das Folgejahr 2022 wird sich das genehmigte Budget leicht auf 1.396.000 Euro erhöhen.

[55] Siehe hierzu auch Abschnitt 2.4 ff dieses Berichts zu Prüfungen.

3.7 Mitarbeit in Gremien und Arbeitsgruppen

Das Katholische Datenschutzzentrum bringt seine Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von kirchlichen Gremien und Arbeitsgruppen ein. Die Beratung der Gremien und Arbeitsgruppen ist Teil des gesetzlichen Auftrags der Datenschutzaufsichten.

Im Berichtszeitraum unterstützte das Katholische Datenschutzzentrum die Arbeit der Unterkommission Datenschutz- und Melderecht/ IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands durch Beteiligung an der Arbeit der Gremien. Diese Beteiligung erfolgte durch Stellungnahmen zu Gesetzentwürfen oder Einzelfragen, die im Rahmen dieser kirchlichen Gesetzgebungsverfahren aufkamen. Teilweise nahm das Katholische Datenschutzzentrum an den Besprechungen teil. Dabei konnte die Datenschutzaufsicht ihre Expertise als unabhängiger Berater einbringen.

Als Datenschutzaufsicht für den VDD und die angeschlossenen Einrichtungen berät das Katholische Datenschutzzentrum darüber hinaus auch in datenschutzrechtlichen Fragen, die in anderen Gremien besprochen werden.

Bei der Weiterentwicklung der diözesanen Gesetze und der Diskussion von grundsätzlichen Rechtsfragen sind die Justitiare der fünf (Erz-) Diözesen und des Katholischen Büros NRW in Düsseldorf die ersten Ansprechpartner des Katholischen Datenschutzzentrums.

Das Katholische Datenschutzzentrum hält daher einen regelmäßigen Kontakt zu den Rechtsabteilungen der Generalvikariate und zum Katholischen Büro NRW.

3.8 Vernetzung

3.8.1 Vernetzung mit kirchlichen Stellen

Die fünf Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen stehen untereinander und mit den Gemeinsamen Ordensdatenschutzbeauftragten der Deutschen Ordensobernkonferenz (DOK) in ständigem Austausch zu aktuellen Fragen und grundsätzlichen Themen. Die Besprechungen und Telefon- oder Videokonferenzen dienen diesem Austausch und der Vorbereitung und Verabschiedung gemeinsamer Beschlüsse[56]. Im Arbeitskreis Technik der Konferenz der Diözesandatenschutzbeauftragten arbeitet das KDSZ aktiv mit.

Der Beauftragte für den Datenschutz der EKD hat neben seinem Hauptsitz in Hannover noch vier Außenstellen. Die Außenstelle in Dortmund ist u. a. für die Landeskirchen und Diakonien in NRW zuständig. Mit der Außenstelle Dortmund des Beauftragten für den Datenschutz der EKD ist im Berichtszeitraum der regelmäßige Austausch fortgesetzt worden.

[56] Siehe Abschnitt 4.1.2 dieses Jahresberichts zur Konferenz der Diözesandatenschutzbeauftragten.

Außerdem unterstützt das Katholische Datenschutzzentrum im Rahmen seiner zeitlichen Möglichkeiten Arbeitskreise betrieblicher Datenschutzbeauftragter kirchlicher Einrichtungen. Hierbei steht es für kurze Vorträge und allgemeinen Erfahrungsaustausch zur Verfügung. So ist das KDSZ beispielsweise regelmäßiger Gast bei den Treffen der betrieblichen Datenschutzbeauftragten der Generalvikariate.

3.8.2 Vernetzung mit staatlichen Stellen

Der Kontakt und der Austausch mit dem Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten als staatlichen Datenschutzaufsichtsbehörden ist nach § 46 KDG Bestandteil der Aufgaben des Diözesandatenschutzbeauftragten. Im Berichtszeitraum gab es vielfältige regelmäßige Kontakte in Grundsatzfragen und bei der Bearbeitung von konkreten Datenschutzproblemen.

Diese Kontakte zu den staatlichen Stellen helfen, vergleichbare Auslegungen der Gesetze bei gleichartigen Vorgängen und damit ein vergleichbares Datenschutzniveau im kirchlichen Bereich bei Anwendung des KDG und im außerkirchlichen Bereich bei Anwendung der DSGVO sicherzustellen.

§ 18 Abs. 1 Satz 4 BDSG sieht eine Beteiligung der kirchlichen Datenschutzaufsichten bei bestimmten Sachverhalten vor, die vom Europäischen Datenschutzausschuss beraten werden, wenn die kirchlichen Datenschutzaufsichten von dieser Frage betroffen sind. Die Einzelheiten zur Anwendung dieser Vorschrift sind zwischen den staatlichen Datenschutzaufsichten und den Datenschutzaufsichten der Rundfunkanstalten und der Kirchen noch in der Diskussion. Die in der Datenschutzkonferenz zusammengeschlossenen unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder haben mit Beschluss vom 13.05.2019 („Beschluss zur Beteiligung der spezifischen Aufsichtsbehörden gem. § 18 Abs. 1 Satz 4 BDSG an der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der EU“) ihren Standpunkt dazu festgehalten. Die dort beschriebene enge Auslegung der Vorschrift entspricht nicht der Auslegung der kirchlichen Datenschutzaufsichten oder der ebenfalls davon betroffenen Rundfunkdatenschutzbeauftragten.[57]

3.9 Öffentlichkeitsarbeit

Das kirchliche Datenschutzrecht stellt ebenso wie die Datenschutz-Grundverordnung die Bedeutung der Information der Öffentlichkeit, der kirchlichen Stellen und der Verantwortlichen für die Datenverarbeitungen über Rechte und Pflichten beim Umgang mit personenbezogenen Daten besonders heraus. Der Aufgabenkatalog der Datenschutzaufsichten in § 44 Abs. 3 KDG betont dieses Thema gleich mehrfach.

[57] Siehe hierzu auch das „Positionspapier zur Zusammenarbeit der nationalen Datenschutzbehörden, insbesondere im Verfahren nach § 18 Abs. 1 BDSG“ der Konferenz der Rundfunkdatenschutzbeauftragten vom Juli 2021 (https://www.rundfunkdatenschutz.de/infothek/taetigkeitsberichte-und-positionen/positionspapier-zusammenarbeit-datenschutzaufsicht-.file.html/Positionspapier%20Zusammenarbeit%20Datenschutzaufsicht.pdf).

So sollen die Datenschutzaufsichten gemäß § 44 Abs. 3 lit. a) KDG die „Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären", wobei „spezifische Maßnahmen für Minderjährige" besondere Beachtung finden sollen. Weiterhin sollen die Datenschutzaufsichten „kirchliche Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten" (§ 44 Abs. 3 lit. b) KDG), „die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz entstehenden Pflichten sensibilisieren" (§ 44 Abs. 3 lit. c) KDG) und „auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes zur Verfügung stellen" (§ 44 Abs. 3 lit. d) KDG).

Das Katholische Datenschutzzentrum macht daher auf vielfältige Weise auf den Datenschutz in der katholischen Kirche und seine Arbeit aufmerksam und informiert die kirchlichen Einrichtungen, die betroffenen Personen und die interessierte Öffentlichkeit über den Datenschutz in der katholischen Kirche.

„Das Katholische Datenschutzzentrum macht daher auf vielfältige Weise auf den Datenschutz in der katholischen Kirche und seine Arbeit aufmerksam und informiert … über den Datenschutz in der katholischen Kirche."

3.9.1 Internetauftritt

Über die Internetpräsenz **www.katholisches-datenschutzzentrum.de** stellt das Katholische Datenschutzzentrum vielfältige Informationen rund um den kirchlichen Datenschutz und die Arbeit der Datenschutzaufsicht zur Verfügung. Diese Informationen sind als Internetseiten online verfügbar oder stehen dort als Infoblätter/Broschüren zum Download bereit. Hierbei reicht das Spektrum von einschlägigen Gesetzestexten für die jeweilige (Erz-)Diözese über Hilfestellungen bis hin zu Mustern und Vorlagen.

Teil der Internetseite des Katholischen Datenschutzzentrums ist auch ein gesichertes Kontaktformular. Über diese Kontaktmöglichkeit will das Katholische Datenschutzzentrum jedem Beteiligten eine gesicherte Kontaktaufnahme ermöglichen. Auf der Internetseite ist ebenfalls der öffentliche Schlüssel für die zentrale E-Mail-Adresse des Katholischen Datenschutzzentrums hinterlegt, sodass auch eine verschlüsselte Kommunikation per E-Mail möglich ist. Zum Ende des Berichtszeitraums hat das Katholische Datenschutzzentrum mit der Einrichtung eines eigenen „besonderen elektronischen Behördenpostfachs (beBPo)" auch die Anbindung an den elektronischen Rechtsverkehr umgesetzt.

Das Katholische Datenschutzzentrum verschickt zudem einen Newsletter, der über neue Informationen auf der Internetseite informiert. Der Newsletter kann über die Internetseite abonniert werden.

3.9.2 Vorträge

Auf Präsenzveranstaltungen wurde im Berichtszeitraum bedingt durch die Pandemie weitestgehend verzichtet, viele Anfragen und Angebote wurden und werden wohl wieder in das Folgejahr verlegt.

Aufgrund der pandemiebedingten Einschränkungen wurden neue Formate für Vorträge erarbeitet und angeboten. Bei Informationsveranstaltungen ist das Katholische Datenschutzzentrum als Referent zugegen (online oder in Präsenz), organisiert die Veranstaltungen aber nicht selbst. Mit diesen Vorträgen konnten erneut viele Multiplikatoren und Verantwortliche erreicht werden.

Das Katholische Datenschutzzentrum stellt auch vor dem Hintergrund der Pandemiesituation einen weiterhin hohen Informationsbedarf der kirchlichen Stellen, der betroffenen Personen und der Öffentlichkeit zum kirchlichen Datenschutz fest.

3.9.3 Informationen/Broschüren/Arbeitshilfen/Muster

Neben den Auskünften auf der Internetseite stellt das Katholische Datenschutzzentrum auch weitergehende Informationen in Form von Informationsblättern, Broschüren, Arbeitshilfen, Mustern oder Checklisten bereit.

In diesen Publikationen behandelt das Katholische Datenschutzzentrum grundsätzliche oder aktuelle Themen, auf die es entweder selbst aufmerksam oder durch vermehrte Anfragen zu einem Thema ein erhöhter Informationsbedarf deutlich wird. Das Angebot an Informationen wird stetig ausgebaut.

3.10 Antragsverfahren vor dem Interdiözesanen Datenschutzgericht und Beschwerde bei dem Datenschutzgericht der Deutschen Bischofskonferenz

Im Berichtsjahr wurde eine Beschwerde des Katholischen Datenschutzzentrums gegen einen Beschluss des Interdiözesanen Datenschutzgerichts zurückgewiesen. Die zweite Instanz folgte der Rechtsansicht des Interdiözesanen Datenschutzgerichts und stellte sich gegen die Ansicht der Aufsicht, dass eine Kontrolle von Coronabesucherlisten durch den leitenden Pfarrer nicht mit den datenschutzrechtlichen Bestimmungen vereinbar ist.

In einem weiteren erstinstanzlichen Verfahren, welches noch nicht abgeschlossen ist, wendet sich ein Mitarbeiter gegen die Datenverarbeitung im Beschäftigtenverhältnis beziehungsweise den korrekten Umgang mit seiner Personalakte und deren Führung. Das Verfahren zeigt, dass gerade im Beschäftigtenkontext und damit in den Personalabteilungen datenschutzrechtliche Sensitivität gefordert ist, um die Betroffenenrechte nicht zu untergraben.

Das letzte Verfahren gegen einen Bescheid des Katholischen Datenschutzzentrum wurde von einem Beschwerdeführer anhängig gemacht, der eine Verletzung seiner Rechte darin begründet sah, dass im Rahmen eines Angestelltenverhältnisses möglicherweise personenbezogene

Daten ausgetauscht wurden. Das Interdiözesane Datenschutzgericht wies die Anträge als unbegründet zurück. Auch hier wurde deutlich, dass die persönliche Ansicht, wann datenschutzrechtliche Betroffenenrechte oder Informationsrechte verletzt sind, von den Antragstellern oft anders bewertet werden, als dies rechtlich geboten scheint. Wichtig ist jedoch, dass sich jeder Betroffene zunächst an die Datenschutzaufsicht wenden kann und das Recht auf Befassung mit seiner Beschwerde hat. Danach oder auch gleichzeitig ist der Rechtsbehelf nach § 49 KDG zum Interdiözesanen Datenschutzgericht möglich, was der betroffenen Person nochmals eine rechtliche Überprüfung eröffnet. In der Sache ist bereits die zweite Instanz angerufen worden.

4 Dokumentation

4.1 Die Datenschutzaufsicht in der katholischen Kirche

4.1.1 Struktur der Aufsichtsstellen

Die Datenschutzaufsicht in der katholischen Kirche wird nicht von einer einzigen Stelle wahrgenommen. Vergleichbar den einzelnen Bundesländern mit eigener Gesetzgebung und jeweils eigenen Landesdatenschutzbeauftragten hat auch jeder Diözesanbischof in Deutschland aufgrund seiner Gesetzgebungsgewalt das kirchliche Datenschutzrecht für die eigene (Erz-)Diözese in Kraft gesetzt und hat, wie im Gesetz vorgesehen, für den eigenen Wirkungskreis einen Diözesandatenschutzbeauftragten ernannt. Dieser DDSB nimmt die Funktion wahr, die im staatlichen Bereich der oder die Landesdatenschutzbeauftragte als Datenschutzaufsicht wahrnimmt.

Zur effektiven und effizienten Wahrnehmung der Aufgaben der Datenschutzaufsicht und in Umsetzung des Urteils des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden aus dem Jahr 2010 haben jeweils mehrere (Erz-)Diözesen gemeinsame Diözesandatenschutzbeauftragte als Datenschutzaufsicht bestellt. Die Verteilung ist in der nachfolgenden Übersicht dargestellt:

Abb.: Struktur der Datenschutzaufsichten der (Erz-)Diözesen in Deutschland

Daneben gibt es noch eine eigene Datenschutzaufsicht für die katholische Militärseelsorge, die in Personalunion vom Diözesandatenschutzbeauftragten für die ostdeutschen (Erz-)Diözesen wahrgenommen wird. Außerdem besteht eine eigenständige Datenschutzaufsicht für den Verband der Diözesen Deutschlands und die nachgeordneten Ein-

richtungen. Diese Aufsichtsfunktion wird in Personalunion vom Diözesandatenschutzbeauftragten für die nordrhein-westfälischen (Erz-) Diözesen wahrgenommen.

Für den Bereich der Ordensgemeinschaften päpstlichen Rechts hat die Deutsche Ordensobernkonferenz, der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung der Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.

4.1.2 Konferenz der Diözesandatenschutzbeauftragten

„Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der Diözesandatenschutzbeauftragten aus."

Zu den Aufgaben des DDSB gehört gemäß §§ 44 Abs. 3 lit. f) und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten.

Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der Diözesandatenschutzbeauftragten aus. Neben den DDSB werden zu den Konferenzen auch die von der Deutschen Ordensobernkonferenz bestellten Ordensdatenschutzbeauftragten für die päpstlichen Ordensgemeinschaften eingeladen. Im Rahmen der Konferenzen ist ebenfalls ein jährlicher Austausch mit Vertretern des Verbandes der Diözesen Deutschlands, der Unterkommission Datenschutz- & Melderecht/IT-Recht der Rechtskommission des VDD, dem Katholischen Büro und der Deutschen Ordensobernkonferenz vorgesehen. Beratend können weitere Vertreter an den Tagungen teilnehmen.

Die Beratungen dienen dazu, gemeinsame Standpunkte zu verabschieden und gemeinsame Vorgehensweisen zu Themen zu finden. Ziel ist die möglichst einheitliche Auslegung des KDG in allen deutschen (Erz-) Diözesen durch die kirchlichen Datenschutzaufsichten.

Im Berichtszeitraum fanden sieben Konferenzen der Diözesandatenschutzbeauftragten statt, aufgrund der Corona-Pandemie überwiegend als Videokonferenzen. Gegenstand der Beratungen waren sowohl aktuelle Fragestellungen als auch Grundsatzfragen zum KDG, die sich bei der Umsetzung der Anforderungen des Datenschutzrechts für die kirchlichen Einrichtungen ergeben haben. Im Jahr 2021 hat die Konferenz der Diözesandatenschutzbeauftragten drei Beschlüsse gefasst. Die Beschlüsse sind in diesem Bericht in Abschnitt 4.3 dokumentiert.

Auch zwischen den Konferenzen stehen die Diözesandatenschutzbeauftragten in regelmäßigem Austausch über aktuelle Fragen.

Zur Vorbereitung technischer Sachverhalte hat die Konferenz der DDSB einen Arbeitskreis Technik ins Leben gerufen. Die Leitung dieses Arbeitskreises wechselt jährlich zwischen den Datenschutzaufsichten.

Die katholischen und evangelischen Datenschutzaufsichten haben vor dem Hintergrund vergleichbarer Anforderungen und Fragestellungen beschlossen, sich regelmäßig über datenschutzrechtliche Themen auszutauschen und jährlich eine gemeinsame Sitzung der Konferenz der

Diözesandatenschutzbeauftragten mit den evangelischen Datenschutzaufsichten durchzuführen. Aufgrund der Corona-Pandemie fand auch dieser Austausch im Jahr 2021 online statt.

4.1.3 FAQ zur Konferenz der Diözesandatenschutzbeauftragten

Zur Konferenz der Diözesandatenschutzbeauftragten werden immer wieder Fragen an das KDSZ herangetragen, die gerne aus Sicht des Katholischen Datenschutzzentrums beantwortet werden:

Auf welcher (Rechts-)Grundlage ist das Gremium der Konferenz der Diözesandatenschutzbeauftragen gebildet worden?

Das KDG gibt den Diözesandatenschutzbeauftragten in den §§ 44 Abs. 3 lit. f) und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten vor. Ein formales Gremium sieht das Gesetz aber nicht vor.

Die „Konferenz der Diözesandatenschutzbeauftragten" ist die von den Diözesandatenschutzbeauftragten selbst gewählte formalisierte Form dieser Vorgabe des KDG zur Zusammenarbeit.

Kann ich als Gast an den Sitzungen teilnehmen?

Die Konferenz besteht aus den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen.

Durch die Beauftragung einzelner Diözesandatenschutzbeauftragter durch mehrere (Erz-)Diözesen gibt es derzeit fünf Diözesandatenschutzbeauftragte.

Als ständige Gäste nehmen die von der Deutschen Ordensobernkonferenz bestellten Gemeinsamen Ordensdatenschutzbeauftragten für die Datenschutzaufsichten der päpstlichen Ordensgemeinschaften an den Sitzungen teil, um auch hier die enge Abstimmung sicherzustellen.

Gemäß der Absprache in der Konferenz können themenbezogen oder zu einzelnen Sitzungen weitere Gäste eingeladen werden. Es besteht aber kein Anspruch einzelner Verbände oder Gremien auf Teilnahme an den Sitzungen.

Welche Verbindlichkeit/Rechtswirkungen haben die Beschlüsse der Konferenz?

Da die Konferenz kein gesetzlich vorgesehenes Gremium mit gesetzlichen Aufgaben und Befugnissen ist, können die Beschlüsse auch keine direkte bindende Wirkung per Gesetz entfalten.

Die Beschlüsse der Konferenz sind eine gemeinsame Auslegung der datenschutzrechtlichen Vorschriften und deren Anwendung auf bestimmte Sachverhalte durch die Diözesandatenschutzbeauftragten.

Der Beschluss an sich ist daher für die kirchlichen Einrichtungen nicht verbindlich. Er entfaltet gegenüber den kirchlichen Stellen aber indirekt dadurch Wirkung, dass die eigene zuständige Datenschutzaufsicht den Beschluss zur Grundlage ihrer Entscheidung im konkreten Einzelfall machen wird, die dann für die Einrichtung verbindlich ist.

Der Wert der Beschlüsse ergibt sich daher aus Sicht des Katholischen Datenschutzzentrums daraus, dass es eine einheitliche Auslegung der Sachverhalte zwischen den Diözesandatenschutzbeauftragten der deutschen (Erz-)Diözesen gibt. Für die kirchlichen Stellen bringen diese Beschlüsse dadurch ein großes Stück Berechenbarkeit der Datenschutzaufsichten, da sich die Einrichtungen anhand der Beschlüsse auf die Entscheidung ihrer zuständigen Datenschutzaufsicht im konkreten Einzelfall besser einstellen können.

Welche Funktion hat die Sprecherin oder der Sprecher der Konferenz?

Die Konferenz wählt aus ihrer Mitte jährlich eine Sprecherin beziehungsweise einen Sprecher. Ihre/Seine Aufgabe ist die Vorbereitung und Leitung der Sitzungen der Konferenz. Außerdem nimmt sie/er als Gast an der Unterkommission Datenschutz- und Melderecht/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands teil und nimmt andere Termine für die Konferenz wahr.

Wie kann ich mich direkt an die Konferenz wenden?

Die Konferenz der Diözesandatenschutzbeauftragten hat zur leichteren Erreichbarkeit eine „Geschäftsstelle" eingerichtet. Diese befindet sich beim Katholischen Datenschutzzentrum in Dortmund. Sie erreichen die Konferenz postalisch unter der Adresse des Katholischen Datenschutzzentrums in Dortmund oder per E-Mail unter ddsb@kdsz.de.

„Mit den Schriften zum kirchlichen Datenschutz möchte das Katholische Datenschutzzentrum den fachlichen und wissenschaftlichen Austausch zu Themen des kirchlichen Datenschutzes unterstützen und voranbringen."

4.2 Veröffentlichungen des Katholischen Datenschutzzentrums – Auszug –

Im Berichtszeitraum 2021 hat das Katholische Datenschutzzentrum wieder einige Hilfestellungen zur Auslegung und Umsetzung datenschutzrechtlicher Vorgaben für die Arbeit der kirchlichen Einrichtungen veröffentlicht. Damit führt es die Praxis der letzten Jahre fort, den kirchlichen Einrichtungen praktische Hilfestellungen für deren Arbeit an die Hand zu geben, gleichzeitig aber auch die fachlichen und wissenschaftlichen Diskussionen zu Aspekten des kirchlichen Datenschutzes und der Umsetzung datenschutzrechtlicher Vorgaben im kirchlichen Bereich voranzubringen.

4.2.1 Schriften zum kirchlichen Datenschutz

Mit den Schriften zum kirchlichen Datenschutz möchte das Katholische Datenschutzzentrum den fachlichen und wissenschaftlichen Austausch zu Themen des kirchlichen Datenschutzes unterstützen und voranbringen. Im Jahr 2020 konnten mit dem ersten Band der Schriftenreihe die

Ergebnisse des Symposiums des Katholischen Datenschutzzentrums aus dem Jahr 2019 dokumentiert werden.

Im Berichtszeitraum konnte das Katholische Datenschutzzentrum nun auf die ersten fünf Jahre seines Bestehens als Körperschaft des öffentlichen Rechts zurückblicken. Aus diesem Anlass hat das KDSZ mit Band 2 der Schriften zum kirchlichen Datenschutz u. a. zurückgeblickt auf die Entstehung des Hauses. Unter dem Titel "Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung" konnten zahlreiche Autorinnen und Autoren für grundlegende Betrachtungen zum kirchlichen Datenschutz und der Entstehung des Datenschutzzentrums gewonnen werden.

Diese Veröffentlichung ist ebenso wie Band 1 der Schriften über die Internetseite des Katholischen Datenschutzzentrums (Infothek ⇨ Publikationen) als PDF-Datei abrufbar.

Abb.: Band 2 der Schriftenreihe zum kirchlichen Datenschutz

4.2.2 Fragenkatalog zur Querschnittsprüfung katholischer Kindertageseinrichtungen

Nach Beendigung der Querschnittsprüfung kirchlicher Kindertageseinrichtungen stellt das KDSZ nachfolgend den bei der Prüfung verwendeten Fragenkatalog zur Verfügung. Anhand dieser Fragen können andere Kindertageseinrichtungen – aber auch andere kirchliche Einrichtungen – im Rahmen eines selbst durchgeführten Audits überprüfen, wie sie bei den geprüften Themen abgeschnitten hätten.

Das Katholische Datenschutzzentrum sieht die Veröffentlichung des Fragenkatalogs daher als Instrument für die kirchlichen Einrichtungen, selbst zu überprüfen, ob die eigene Einrichtung bei den geprüften Themenfeldern datenschutzkonform aufgestellt ist. So erkannte Defizite der eigenen Erfüllung datenschutzrechtlicher Vorgaben können und sollten dann auch ohne eine ausdrückliche Anweisung der Datenschutzaufsichtsbehörde abgestellt werden.

In der folgenden Auflistung sind die Fragen hintereinander aufgeführt. In der Online-Version des Fragebogens wurden Abhängigkeiten zwischen den Fragen berücksichtigt, sodass einige Fragen nur gestellt wurden, wenn eine vorherige Frage entsprechend beantwortet wurde. Diese Abhängigkeiten werden in der nachfolgenden Auflistung nicht berücksichtigt, sodass es teilweise so aussieht, als wenn sich aufeinander folgende Fragen widersprechen oder ausschließen würden.

Allgemeine Fragen zur Einrichtung

- Wie lautet die genaue Bezeichnung der Einrichtung?
- Geben Sie bitte – falls vorhanden – die Adresse der Homepage der Einrichtung an.
- Zu welchem (Erz-)Bistum gehört die Einrichtung?
- Wer steht als Ansprechpartner für Rückfragen zur Verfügung?
- Welche Organisation ist Träger der Einrichtung?
- Wie viele Mitarbeitende hat die Einrichtung? Bitte geben Sie die Zahl aller mitarbeitenden Personen inklusive Ehrenamtlichen, BufDi´s, FSJ, Praktikanten usw. an.
- Wie viele Kinder werden in der Einrichtung betreut?
- Werden Kinder im Rahmen von Inklusionsmaßnahmen betreut?
- Wo liegt die Einrichtung (Wohngebiet/Gewerbegebiet/Mischgebiet)?

Betrieblicher Datenschutzbeauftragter

- Wurde für Ihre Einrichtung ein betrieblicher Datenschutzbeauftragter benannt?
- Warum wurde kein betrieblicher Datenschutzbeauftragter benannt?
- Bitte geben Sie die dienstlichen Kontaktdaten des betrieblichen Datenschutzbeauftragten an.
- Wurde der betriebliche Datenschutzbeauftragte der zuständigen Datenschutzaufsicht gemeldet?
- Art des betrieblichen Datenschutzbeauftragten (intern/extern)?
- Wie hoch ist der durch den Verantwortlichen festgelegte Anteil der Stelle des betrieblichen Datenschutzbeauftragten – gemessen an einer Vollzeitstelle – zur Wahrnehmung seiner Aufgaben?
- Wie hoch ist das für Ihre Einrichtung vorgesehene monatliche Kontingent bei dem externen betrieblichen Datenschutzbeauftragten?
- Welche Aufgaben übernimmt Ihr betrieblicher Datenschutzbeauftragter?

Datensicherung

- Wie viele Endgeräte haben Sie in Betrieb? Um die Erfüllung datenschutzrechtlicher Anforderungen in Bezug auf Endgeräte wie Desktop-PCs, Laptops, Smartphones usw. nachweisen zu können (z. B. Zugangskontrolle und Patchmanagement), ist es zunächst erforderlich, diese aufzulisten. Bitte tragen Sie hier nur Zahlen (ggf. „0“) ein.

- Welche Speichermedien nutzen Sie im Alltagsbetrieb für die Speicherung personenbezogener Daten? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z. B. Aufbewahrung) haben.

- Führen Sie regelmäßig Datensicherungen durch?

- Wie oft führen Sie Datensicherungen durch?

- Warum führen Sie keine Datensicherungen durch?

- Auf welchen Speichermedien werden Ihre Datensicherungen gespeichert? Die Art der Speichermedien kann Einfluss auf die zu treffenden Maßnahmen zum Schutz dieser Medien (z. B. Lagerung) haben.

Virenscanner

- Setzen Sie Virenscanner ein?

- Wie oft wird der Virenscanner aktualisiert?

- Welche(n) Virenscanner setzen Sie ein?

Datenspeicher

- Wie viele externe/mobile Datenspeicher nutzen Sie?

- Wo und wie werden die Endgeräte und die externen Datenspeicher aufbewahrt, wenn diese nicht benutzt oder beaufsichtigt werden (insb. außerhalb der Dienstzeiten)?

- Nutzen Sie einen Server (intern oder extern) als zentrales System (z. B. zur Datenspeicherung oder für Anwendungen)? Werden z. B. Daten zentral auf einem Server gespeichert oder sind diese auf die eingesetzten Geräte „verteilt“?

- Durch wen wird der Server betrieben?

- Durch wen wird der Server gewartet?

Zugangsschutz

- Wie ist der Zugang zu den Betriebssystemen geschützt?

- Gibt es eine systemseitige Automatik für die Änderung der Passwörter für den Zugang zum Betriebssystem?

- Wie oft wird das Passwort geändert?

Verzeichnis von Verarbeitungstätigkeiten

- Ist für Ihre Einrichtung ein Verzeichnis von Verarbeitungstätigkeiten vorhanden?
- Wie stellen Sie die Aktualität des Verzeichnisses sicher?
- Wer führt das Verzeichnis von Verarbeitungstätigkeiten?
- Sofern eine Verarbeitung auf die Rechtsgrundlage der "Einwilligung" gestützt wird, wie wird die Einwilligungserklärung erteilt?
- Wie werden eingeholte Einwilligungen dokumentiert?

Informationssicherheit

- Wie kommen Sie Ihren Informationspflichten in Bezug auf Ihre Verarbeitungstätigkeiten nach?
    - Bitte erläutern Sie, wie Sie Ihren Informationspflichten im Einzelnen nachkommen.
- Sind die Mitarbeitenden zur datenschutzkonformen Verarbeitung personenbezogener Daten in Ihrem Arbeitsbereich sensibilisiert, geschult und verpflichtet worden?
- Zu welchem Zeitpunkt führen Sie normalerweise die Verpflichtung durch?
- Wie oft werden die Mitarbeitenden auf die Verarbeitung von personenbezogenen Daten hin sensibilisiert/geschult?

Datenschutzverletzungen

- Wenn bei uns Datenschutzverletzungen festgestellt werden, ...
    - führen wir ein internes Verfahren zur Erfassung und Bewertung durch. (J/N)
    - nehmen wir eine interne Dokumentation vor. (J/N)
    - melden wir den Vorfall an den Träger. (J/N)
    - melden wir den Vorfall an den betrieblichen Datenschutzbeauftragten. (J/N)
    - melden wir den Vorfall bei der Datenschutzaufsicht. (J/N)
        - » Bitte erläutern Sie, warum Meldungen bei der Datenschutzaufsicht nicht vorgesehen sind.

Unter Datenschutzverletzungen im Sinne dieser Frage sind sämtliche "Datenpannen" (z. B. Versand von Unterlagen an den falschen Empfänger, Veröffentlichung vertrauenswürdiger Informationen, Veröffentli-

chung von Fotos ohne Einwilligung, Schadsoftwarebefall mit nachfolgendem Verlust personenbezogener Daten) zu verstehen, unabhängig von einer Meldepflicht an die Datenschutzaufsicht.

Private Endgeräte

- Benutzen Mitarbeitende private Endgeräte zu dienstlichen Zwecken?
    - Bitte erläutern Sie uns, wie Sie den datenschutzrechtlichen sicheren Betrieb der privaten Endgeräte für den dienstlichen Zweck sicherstellen.
- Welche Regelungen haben Sie zur Nutzung von privaten Endgeräten zu dienstlichen Zwecken getroffen? Regelungen könnten z. B. in Form von Dienstanweisungen oder Dienstvereinbarungen bestehen. Bitte fassen Sie den Inhalt eventueller Bestimmungen/Vereinbarungen stichwortartig zusammen.

Löschen von Daten

- Haben Sie für alle verarbeiteten Daten festgelegt, wie lange diese aufbewahrt werden müssen (gesetzliche oder betriebliche Gründe)?
- Haben Sie Regeln und Verfahren, wie Sie mit zu löschenden Daten umgehen?
- Existiert ein Löschkonzept, das auch das Löschen aus dem Langzeitregister (internes Archiv) und von Datensicherungen regelt?
    - Sofern Sie noch kein Löschkonzept haben, erläutern Sie bitte, nach welchen Kriterien Sie bisher Daten gelöscht oder vernichtet haben.
    - Sofern Sie bereits ein Löschkonzept haben, erläutern Sie bitte, wie Sie bisher mit in Langzeitregistern (oft als Archive bezeichnet) gelagerten Daten umgegangen sind und anhand welcher Kriterien die Daten gelöscht oder vernichtet wurden.
- Wie stellen Sie sicher, dass auf ausgemusterten Endgeräten keine personenbezogenen Daten mehr gespeichert sind?
    - Bitte erläutern Sie, wie Sie dauerhaft den Zugriff unberechtigter Dritter auf mögliche noch auf dem Endgerät gespeicherten personenbezogenen Daten verhindern.

Datensicherheit

- Sind alle Festplatten (interne und externe) Ihrer Einrichtung verschlüsselt?
    - Bitte erläutern Sie, wie Sie die Vertraulichkeit der auf Ihren Festplatten gespeicherten personenbezogenen Daten (z. B. Fotos), beispielsweise auch bei Diebstahl, sicherstellen und fügen Sie entsprechende Nachweise bei.

- Mit welcher Software führen Sie die Festplattenverschlüsselung durch?

- Sind alle weiteren digitalen Datenträger (z. B. USB-Sticks, SD-Karten) mit personenbezogenen Daten verschlüsselt?

    - Bitte erläutern Sie, wie Sie die Vertraulichkeit der auf diesen Datenträgern gespeicherten personenbezogenen Daten sicherstellen und fügen Sie entsprechende Nachweise bei.

- Warum sind die digitalen Datenträger mit personenbezogenen Daten nicht verschlüsselt?

    … Technisch zu aufwändig

    … Mit der aktuellen Hardware nicht umzusetzen

    … Eine Verschlüsselung ist nicht notwendig

    … Organisatorische Maßnahmen sind getroffen

    … Zu teuer

    … Technisch nicht möglich

    … Es ist in der Einrichtung nicht bekannt, wie das funktioniert

    … Sonstiges

- Kopieren Sie personenbezogene Daten auf externe Datenträger (Festplatten, USB-Sticks, SD-Karten)?

Technische und organisatorische Maßnahmen

- Welche Vorkehrungen sind zur Zutrittskontrolle zum Gebäude getroffen? Hierunter versteht man Maßnahmen, die den Zutritt zu den Räumlichkeiten der Datenverarbeitung beschränken und kontrollieren.

- Welche Vorkehrungen sind zur Zugangskontrolle zu den Rechnern/Endgeräten (Anmeldung) beziehungsweise zur Zugriffskontrolle auf die Anwendungsdaten (Berechtigungen) getroffen? Dies sind Maßnahmen, die auf der zweiten Stufe den Zugang zu Datenverarbeitungssystemen verhindern, nachdem die erste Stufe der Zutrittskontrolle überwunden wurde, sowie Maßnahmen, die Nutzern den Zugriff auf oder die Löschung von bestimmten Daten erlauben. (Mehrfachauswahl möglich, bitte geben Sie nur die bereits umgesetzten Maßnahmen an.)

- Wie wird die Weitergabe von Daten kontrolliert? Gemeint sind Maßnahmen, die die Integrität und Vertraulichkeit personenbezogener Daten sowohl bei elektronischen Übermittlungsvorgängen als auch beim Transport der Datenträger sicherstellen.

- Wird die Tätigkeit von Auftragsverarbeitern kontrolliert? (Bitte nennen Sie nur bereits umgesetzte Maßnahmen.)

- Wie kontrollieren Sie die Eingabe und das Löschen von personenbezogenen Daten? Dies sind Maßnahmen, die nachträgliche Feststellungen ermöglichen, ob und durch wen personenbezogene Daten in Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind. (Mehrfachauswahl möglich, bitte nennen Sie nur bereits umgesetzte Maßnahmen.)

- Wie wird die permanente Verfügbarkeit beziehungsweise die Wiederherstellung der Daten sichergestellt? Gemeint sind Maßnahmen zur Verhinderung eines ungewollten Datenverlustes sowie zur Wiederherstellung von Daten.

4.3 Beschlüsse und Veröffentlichungen der Konferenz der Diözesandatenschutzbeauftragten

4.3.1 Betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

vom 04.01.2021

betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG

Geltungszeitraum des Beschlusses: 01.01.2021 bis längstens 30.04.2021

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands beschließt

- vor dem Hintergrund der speziellen Anforderungen des Kirchlichen Datenschutzgesetzes der (Erz-)Diözesen (KDG) aus § 29 Abs. 11 KDG,
- auf Grund des Endes der Übergangsphase zum 31.12.2020 zum Austritt des Vereinigten Königreiches von Großbritannien und Nordirland aus der Europäischen Union,
- auf der Basis des Abkommens zwischen der Europäischen Union und dem Vereinigten Königreich vom 24.12.2020 („TRADE AND COOPERATION AGREEMENT BETWEEN THE EUROPEAN UNION AND THE EUROPEAN ATOMIC ENERGY COMMUNITY, OF THE ONE PART, AND THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, OF THE OTHER PART", **nachfolgend „Handelsabkommen"**), vorläufig in Kraft getreten zum 01.01.2021,
- vorbehaltlich der Ablehnung oder etwaiger Änderungen des oben genannten Handelsabkommens durch das Europäische Parlament zur noch erforderlichen Genehmigung des Handelsabkommens,
- zur Vermeidung von Nachteilen katholischer Einrichtungen gegenüber außerkirchlichen Einrichtungen durch die Formulierung des § 29 Abs. 11 KDG,
- betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG im Geltungsbereich des Handelsabkommens,

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

dass sie durch das Handelsabkommen, Abschnitt FINPROV.10A,

- für den Zeitraum vom 01.01.2021 bis zur Wirksamkeit einer Entscheidung der Europäischen Kommission nach Artikel 45 Abs. 3 DSGVO (Verordnung (EU) 2016/679) bezüglich des Vereinigten Königreichs von Großbritannien und Nordirland oder bis zum 30.04.2021, je nachdem, welches Ereignis eher eintritt und
- soweit und solange die in Abschnitt FINPROV.10A des Handelsabkommens aufgestellten Voraussetzungen erfüllt werden,

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

Begründung

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

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

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

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

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

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

Beschluss vom 04.01.2021

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

4.3.2 Betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG (Verlängerung)

Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

vom 22.04.2021

betreffend Datenverarbeitungen von Auftragsverarbeitern katholischer Einrichtungen im Vereinigten Königreich von Großbritannien und Nordirland im Sinne von § 29 Abs. 11 KDG

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

Beschluss vom 22.04.2021

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

4.3.3 Zur Beurteilung von Messenger- und anderen Social Media-Diensten

Konferenz der Diözesan-datenschutzbeauftragten der Katholischen Kirche Deutschlands

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 15.09.2021)

Beurteilung von Messenger- und anderen Social Media-Diensten

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

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

Vorbemerkung

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

Kriterien, die ein Dienst aus Sicht des Datenschutzes erfüllen muss

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

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

Der Verantwortliche muss sich also überzeugen, dass die Rechtmäßigkeit der Verarbeitung durch Vorliegen mindestens einer dieser Bedingungen gegeben ist.
Die Überprüfung der Rechtmäßigkeit der Verarbeitung in einem Drittland führt dabei in jedem Fall zu einem deutlich größeren Aufwand bei der Einrichtung des Verfahrens im Vergleich zu einem Betrieb in einem EU-Mitgliedsland. Schon aus diesem Grund sowie

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

wegen des permanenten Risikos, dass die Rechtmäßigkeit durch Änderung z.B. der Gesetzeslage im Drittland oder Änderung der Anerkennungssituation entfällt, raten wir grundsätzlich von der dauerhaften Verarbeitung in einem Drittland ab, selbst wenn formal die Rechtmäßigkeit der Verarbeitung zum aktuellen Zeitpunkt gegeben wäre.

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

  Nach § 26 KDG hat der Verarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten. Als geeignete Maßnahme wird unter anderem die Verschlüsselung personenbezogener Daten ausdrücklich genannt. Auch in § 6 Abs. 1 lit. b KDG-DVO wird Verschlüsselung als geeignete Maßnahme zum Schutz personenbezogener Daten bei deren Übertragung aufgeführt und in § 12 Abs. 2 lit e KDG-DVO für Daten der DSK II explizit gefordert. § 27 KDG fordert überdies, die Sicherheitsoptionen so zu gestalten, dass bereits durch die Voreinstellung das angemessene Schutzniveau gewahrt wird. Verschlüsselung darf deshalb nicht „optional zuschaltbar“ sein, sondern sollte per Default vorgegeben werden. Die Sicherheit der Daten sollte auch nicht nur auf dem Transport, also auf dem Weg vom Endgerät des Senders über den zentralen Server bis zum Endgerät des Empfängers gewährleistet werden, sondern auch, wenn die Daten auf dem Endgerät angekommen sind, durch eine sichere Datenhaltung in der Applikation, die die Daten z.B. gegen ungewolltes Ausspähen durch andere Applikationen auf dem gleichen Endgerät schützt. Dem aktuellen Stand der Technik (im Jahr 2020) entsprechen Transport- und Inhaltsverschlüsselungen nach den Standards TLS mindestens in der Version 1.2 idealerweise mit Perfect Forward Secrecy[1] oder AES 128 und größer, idealerweise mit der Betriebsart GCM bzw. bei der Verwendung von EC-Verfahren eine Schlüssellänge von mindestens 250 Bit[2].

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

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

  Eine Beschränkung auf das für den Zweck der Verarbeitung notwendige Maß an personenbezogenen Daten wird in § 7 Abs.1 lit c) KDG gefordert. Die Beschränkung gilt für die Menge und den Zeitraum der Verarbeitung und Speicherung. Deshalb ist zu fordern, dass alle personenbezogenen Daten, also Inhalte und Verbindungsdaten der Kommunikation, sobald wie möglich gelöscht werden. Eine Speicherung von Inhalten der Kommunikation auf dem zentralen Server ist - genau wie ein Mitlesen durch den Serviceprovider - nicht akzeptabel.

  Eine extreme Datenminimierung zusammen mit einer starken Ende-zu-Ende-Verschlüsselung führt dazu, dass der Provider selbst unter Zwang (z.B. durch staatliche

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

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

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Behörden) technisch nicht in der Lage ist, Daten herauszugeben. Ebenso laufen illegale Angriffe auf die zentralen Server ins Leere.

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

  Personenbezogene Daten müssen rechtmäßig und für den Betroffenen in nachvollziehbarer Weise verarbeitet werden. (§ 7 Abs. 1 KDG). Der Betroffene hat nach den §§ 14 und 15 KDG umfassende Rechte auf Information über den Umfang und die Art der Verarbeitung seiner Daten. Dagegen verstößt regelmäßig die Ausspähung von Adressen und Kontaktdaten des Telefonbuches durch allzu neugierige Applikationen. Manche Anbieter versuchen über die AGB, die Verantwortung für die Einholung einer Einwilligung der Dritten in die Weitergabe ihrer Daten dem Nutzer aufzubürden, was dieser in der Praxis aber nie leisten kann.

Weitere Kriterien

Zu dem erweiterten Kriterienkreis gehören zum einen die Kosten: Der Entscheider sollte prüfen, ob die Nutzung des Produktes idealerweise für den privaten Nutzer kostenfrei und für die nicht-private Nutzung, also z.B. durch eine kirchliche Einrichtung, relativ erschwinglich ist.

Bei einer Beurteilung einer Messenger-Lösung ist ferner die Verfügbarkeit des Quellcodes (Open Source) zu berücksichtigen und ggf. positiv zu bewerten. Der Quellcode erlaubt es unabhängigen Experten, einerseits die Korrektheit von Herstellerangaben zu verifizieren und eröffnet diesen andererseits die Möglichkeit, Schwachstellen im Programmcode zu identifizieren.

Darüber hinaus sind die Bedingungen der Lizenzvergabe zu prüfen, die meistens in den AGB geregelt werden. Manche Anbieter untersagen die nicht-private Nutzung, andere untersagen lediglich die kommerzielle Anwendung. Während das Produkt im ersten Fall auch durch ehrenamtliche Non-Profit-Organisationen nicht genutzt werden darf, können diese im zweiten Fall – abhängig von den Formulierungen der AGB – doch von einer bestimmungsgemäßen Nutzung ausgehen. Nicht-privaten Nutzern wird manchmal eine spezielle „Business-Lösung“ angeboten, die aber oft mit höheren Lizenzkosten verbunden ist als die Privat-Anwendung. Einige Anbieter fordern ein Mindestalter der Nutzer von 16 oder sogar 18 Jahren, andere Anbieter stellen ihr Produkt nur für Nutzer mit Wohnsitz in bestimmten Staaten zur Verfügung.

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

15.09.2021

Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: ddsb@kdsz.de, Tel. 0231 / 138 985 – 0; Fax 0231 / 138 985 - 22

4.3.4 Technische Hilfen zu Windows 10

Die technischen Empfehlungen zum datensparsamen Betrieb von Windows 10 wurden vom Arbeitskreis Technik der Konferenz der Diözesandatenschutzbeauftragten erarbeitet und von der Konferenz der Diözesandatenschutzbeauftragten herausgegeben.

Derzeit sind neben dem Manteldokument / datensparsamer Betrieb von Windows 10 noch verfügbar:

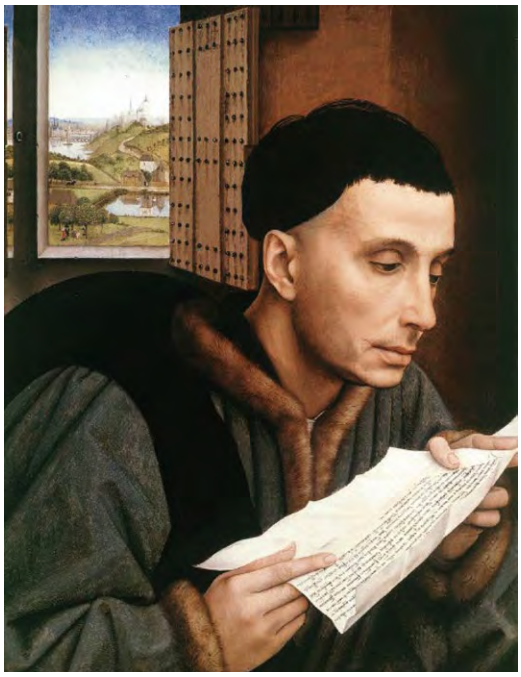
- Technische Hinweise für Windows 10 – Windows 10 Suchfunktion,
- Technische Hinweise für Windows 10 – Windows 10 Installation,
- Technische Hinweise für Windows 10 – Entfernung von automatisch installierten Applikationen,
- Technische Hinweise für Windows 10 – Online Spracherkennung und
- Technische Hinweise für Windows 10 – Webbrowser.

Die Technischen Hinweise für Windows 10 sind auf der Internetseite des Katholischen Datenschutzzentrums (Infothek ⇨ Arbeits- und Formulierungshilfen) abrufbar.

Abkürzungsverzeichnis

AVO	Aufarbeitungsverordnung (Gesetzesvertretende Verordnung des Rates der Evangelischen Kirche in Deutschland zur Änderung des EKG-Datenschutzgesetzes und dienstrechtlicher Regelungen zum Zwecke der institutionellen Aufarbeitung sexualisierter Gewalt)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BAG	Bundesarbeitsgericht
beBPo	besonderes elektronisches Behördenpostfach
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
DDSB	Diözesandatenschutzbeauftragte/r
DOK	Deutsche Ordensobernkonferenz
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz)
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EKD	Evangelische Kirche in Deutschland
e-Privacy-Verordnung	Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
GO-EKD	Grundordnung der Evangelischen Kirche in Deutschland
IDSG	Interdiözesanes Datenschutzgericht
IfSG	Infektionsschutzgesetz
ISMS	Information Security Management System (Managementsystem für Informationssicherheit)

JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
KAO	Kirchliche Archivordnung (Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche)
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDG-VDD	KDG für den Verband der Diözesen Deutschlands
KDM	Kirchliches Datenschutzmodell
KDS-VwVfG	Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
KRITIS	Kritische Infrastrukturen
NOYB	none of your business (Nichtregierungsorganisation; Europäisches Zentrum für digitale Rechte)
OH	Orientierungshilfe
OVG	Oberverwaltungsgericht
PatDSO	Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen
PIMS	Personal Information Management Services (Systeme, die natürlichen Personen mehr Kontrolle über ihre personenbezogenen Daten geben)
SCC	Standard Contractual Clauses (Standardvertragsklauseln)
SDM	Standard-Datenschutzmodell
Seelsorge-PatDSG	Gesetz zum Schutz von Patientendaten bei der Seelsorge in katholischen Einrichtungen des Gesundheitswesens
SGB	Sozialgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz)
USA	Vereinigte Staaten von Amerika
VDD	Verband der Diözesen Deutschlands
VG	Verwaltungsgericht



Hl. Ivo

Der heilige Ivo ist der Schutzpatron des Katholischen Datenschutzzentrums.
Er lebte im 13. Jahrhundert im heutigen Frankreich und setzte sich dort unter anderem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein.
Das Bildnis des heiligen Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums. Sein Gedenktag ist der 19. Mai.

Bild: Joachim Schäfer – www.heiligenlexikon.de

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel.: 0231/13 89 85 – 0
Fax: 0231/13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de