Jahresbericht 2022

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.–31.12.2022

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

7. 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 01.01.2022–31.12.2022

Redaktionsschluss: 31.03.2023

Inhaltsverzeichnis

Vorwort

Am 19. Mai 2023 jährt sich der Todestag des heiligen Ivo, dem Schutzpatron des Katholischen Datenschutzzentrums, zum 720. Mal. Er soll sich in seinem Amt als Offizial und damit als Leiter des Kirchengerichts in seinem Bistum nicht von Interessen einer Gruppe hat leiten lassen, sondern seine Aufgaben unparteiisch und fair versehen haben[1]. Wir sind froh über die Wahl dieses Schutzpatrons für das Katholische Datenschutzzentrum durch die (Erz-)Diözesen, da dies auch die Erwartungen an die Arbeit unseres Hauses sehr gut wiedergibt.

Inhaltlich traten im dritten Jahr der Corona-Pandemie die pandemiebedingten datenschutzrechtlichen Themen mehr und mehr in den Hintergrund und die „normalen" Datenschutzthemen gewannen wieder an Bedeutung. Daher finden Sie in diesem Jahresbericht auch bekannte Themen aus der „Vor-Corona-Zeit" wieder.

Im Berichtszeitraum gab es eine rege gesetzgeberische Tätigkeit auf allen Ebenen, die direkt und indirekt Einfluss auf die datenschutzrechtliche Arbeit hat. Im Bericht stellen wir einige wichtige Neuerungen vor. Ebenso hat der Europäische Datenschutzausschuss im Berichtszeitraum viele Leitlinien zu wichtigen Fragestellungen und Auslegungsfragen verabschiedet. Auch hier greifen wir im Bericht einige für die Arbeit der kirchlichen Einrichtungen wichtige Punkte heraus.

Die Beratung der kirchlichen Stellen im Vorfeld der Verarbeitung von Daten und damit der Verhinderung von Gesetzesverstößen ist auch weiterhin der Schwerpunkt unserer Arbeit. Verstöße schon im Vorfeld zu verhindern ist für alle Beteiligten angenehmer als nachträglich mit den Mitteln einer Aufsicht Verstöße feststellen zu müssen. Daher stehen wir den kirchlichen Stellen gerne als Ansprechpartner für die datenschutzrechtlichen Themen zur Verfügung. Wir freuen uns, wenn dieses Angebot rege genutzt wird.

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

[1] Ausführlich zum Leben und Wirken des hl. Ivo: Michael Streck / Annette Rieck, St. Ivo (1247-1303) - Schutzpatron der Richter und Anwälte, 2007.

1 Entwicklungen im Datenschutzrecht

Mit der zunehmenden Bedeutung personenbezogener Daten als Wirtschaftsgut ergeben sich auf europäischer, nationaler und kirchlicher Ebene immer wieder Notwendigkeiten für neue oder geänderte gesetzliche und regulatorische Vorgaben zum Schutz und zum Umgang mit den personenbezogenen Daten. In diesem Abschnitt werden die gesetzgeberischen oder regulatorischen Initiativen zur Weiterentwicklung auf europäischer, nationaler und kirchlicher Ebene im Jahr 2022 auszugsweise beschrieben.

1.1 Gesetzgeberische Entwicklungen auf Ebene der Europäischen Union

Im Berichtszeitraum hat die Europäische Kommission erste Schritte zur Umsetzung ihrer europäischen Datenstrategie realisieren können. Diese und andere aus Sicht des Katholischen Datenschutzzentrums (KDSZ) datenschutzrechtlich relevante Vorhaben auf europäischer Ebene sollen nachfolgend kurz beleuchtet werden.

1.1.1 EU-Datengesetz

Die Europäische Kommission hat Anfang 2020 mit ihrer europäischen Datenstrategie[1] ein ehrgeiziges Vorhaben formuliert, mit dem sie die Digitalisierung in Europa vorantreiben möchte. Gleichzeitig sollen einheitliche Regelungen und Rechtsrahmen geschaffen werden, die den Datenaustausch zwischen Privatpersonen, Unternehmen und dem öffentlichen Sektor regeln. Als weitere Zielsetzung wird die bessere Nutzung vorhandener Daten angestrebt. Insbesondere bei Gesundheitsdaten möchte die Europäische Kommission einen stärkeren positiven Nutzen für die Allgemeinheit erreichen, indem für Forschungsvorhaben Gesundheitsdaten, deren Nutzung für Forscher bisher nicht möglich war, genutzt werden können. Aber auch insgesamt möchte die Kommission den Datenaustausch verbessern.

Als ein Mittel dazu soll neben weiteren Gesetzesvorhaben der geplante Data Act dienen. Diese Verordnung bezüglich eines verbesserten Datenaustauschs soll den Kontakt zwischen Anbietern und Nutzern verbessern und vereinfachen. Gleichzeitig sieht die Europäische Kommission viele derzeit nicht sinnvoll nutzbare Daten, welche sie nutzbar machen möchte. Sie erhofft sich mit den neuen Regelungen positive Auswirkungen zum einen für die Digitalisierung, aber auch für Forschungsergebnisse, die dem Nutzen der Allgemeinheit dienen.

Die EU-Kommission sieht weiter ein generelles Problem darin, dass Daten für den Gebrauch innerhalb der europäischen Wirtschaft unzureichend zur Verfügung stehen. Als Ursache werden ein Fehlen klarer Regeln bezüglich der Rechte an Daten, Verhandlungsungleichge-

[1] Zu Einzelheiten siehe https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

wichte, eingeschränkte Zugänge zu fairen und vertrauenswürdigen Cloud-Diensten sowie Schwierigkeiten bei einem sektorübergreifenden Datenaustausch gesehen.

Dem möchte die EU durch den Data Act begegnen, der die Rechtssicherheit bezüglich des Zugangs zu Daten erhöhen und den Missbrauch von vertraglichen Ungleichgewichten verhindern soll. Ebenso soll der Gebrauch von Wirtschaftsdaten durch den öffentlichen Sektor vereinfacht werden sowie der Wechsel zwischen vertrauenswürdigen Anbietern von Datenverarbeitungsdiensten.

Weiterhin soll für Nutzer und Anbieter eine bessere und umfangreichere Möglichkeit zur Kontrolle der Daten, die sie erschaffen, zur Verfügung stehen. Verstärkt werden soll auch ihre aktive Teilnahme an der Digitalwirtschaft.

1.1.2 Digital Services Act: Inhalt und Ziele der neuen EU-Regeln

„Zielsetzung des Digital Services Act (DSA) ist die Vereinheitlichung von Vorgaben für das Internet im Bereich der Mitgliedstaaten der Europäischen Union."

Zielsetzung des Digital Services Act (DSA) ist die Vereinheitlichung von Vorgaben für das Internet im Bereich der Mitgliedstaaten der Europäischen Union. Dabei sollen sowohl die Internetnutzer unter Beachtung der ihnen zustehenden Grundrechte geschützt, als auch die Verbreitung von illegalen Inhalten eingegrenzt und verhindert werden. Erreicht werden soll dies u. a. durch die Vorgabe verbindlicher Pflichten für die Anbieter digitaler Dienste. Der DSA zielt u. a. darauf ab, dass Anbieter stärker als bisher dazu verpflichtet werden, gegen rechtswidrige Inhalte vorzugehen. Derartige Inhalte sollen künftig schneller von den Seiten der digitalen Anbieter entfernt werden. Die Pflicht zum konsequenteren Löschen soll ab dem Zeitpunkt entstehen, sobald dem Anbieter eine Rechtsverletzung gemeldet wird oder er in sonstiger Weise Kenntnis erlangt.

Auch sollen Nutzer besser in die Lage versetzt werden, über ihre Daten zu verfügen und ihren etwaigen Widerspruch gegen eine Nutzung und Verarbeitung der von ihnen erzeugten Daten erforderlichenfalls in geeigneter Weise geltend machen zu können. Die Regelungen zielen insbesondere auf große Anbieter im Bereich sozialer Medien. Damit verbunden ist seitens der EU aber auch die Hoffnung, dass bessere Bedingungen für die Bereitstellung von digitalen Daten in den Märkten der Europäischen Union geschaffen werden.

Weiterhin soll durch den DSA eine weitergehende Transparenz in Bezug auf Werbeinhalte bei digitalen Angeboten geschaffen werden. Werbung im Internet soll künftig eindeutig als solche gekennzeichnet werden. Nutzer sollen auch erkennen können, wann Anwendungen von Profiling zur Analyse ihrer Nutzungen eingesetzt werden. Die Nutzer sollen dadurch besser feststellen können, warum ihnen eine bestimmte Werbung zur Verfügung gestellt wird.

Der DSA befindet sich damit auf einer Linie mit den auch durch andere Gesetzgebungsvorhaben angestrebten Zielen seitens der EU, mit geeigneten Gesetzen für Transparenz, Informations- und Rechenschaftspflichten im Bereich der digitalen Dienste zu sorgen. Dies gilt gleicher-

maßen für das Bestreben, illegale Inhalte bei digitalen Angeboten zu bekämpfen und die Wahrnehmung der Verantwortung von Anbietern zu regeln.

1.1.3 Chronologischer Überblick transatlantischer Datenabkommen mit den USA

Wie die DSGVO (Datenschutz-Grundverordnung) verbot schon deren Vorgängerrichtlinie 95/46/EG es grundsätzlich, personenbezogene Daten aus Mitgliedstaaten der Europäischen Union in Staaten zu übertragen, deren Datenschutz kein dem EU-Recht vergleichbares Schutzniveau aufwies. Zu diesen sog. Drittstaaten gehörten auch die Vereinigten Staaten. Das US-amerikanische Recht kennt jedenfalls auf Bundesebene keine ganzheitliche Regelung des Datenschutzrechts.

Damit personenbezogene Daten trotzdem in Übereinstimmung mit der europäischen Richtlinie 95/46/EG in die USA übertragen werden konnten, einigten sich die EU und die USA auf einen Katalog von Selbstverpflichtungen für US-Unternehmen, die einen Schutz von personenbezogenen Daten auf Niveau des EU-Rechts sicherstellen sollten. Diese Selbstverpflichtungen wurden „safe harbor principles" genannt. Die EU Kommission erkannte daraufhin mit Beschluss von Juli 2000 an, dass Unternehmen, die sich zu diesen Prinzipien verpflichtet hatten, einen ausreichenden Schutz für personenbezogene Daten böten.[2] Der Beschluss der Kommission wird auch als ***Safe-Harbor-Abkommen*** bezeichnet.

Der Europäische Gerichtshof (EuGH) erklärte das Safe-Harbor-Abkommen in seiner Schrems-I-Entscheidung als nichtig.[3]

Der Nachfolger von Safe Harbor war das ***Privacy-Shield-Abkommen***. Die Schrems-I-Entscheidung machte es notwendig, eine Nachfolgeregelung zu finden. Zwischenzeitlich hatten Unternehmen versucht, die Datenübertragung in die USA durch die Verwendung von Standardvertragsklauseln[4] so rechtssicher wie möglich zu gestalten.[5] Teil des Abkommens waren, wie bei Safe Harbor, Sicherheitsgarantien aufseiten der USA, mit denen versucht wurde, eine höhere Konformität mit dem damaligen Datenschutzregime der EU zu erreichen. Die USA richteten z. B. eine Stelle in ihrem Außenministerium zur Beilegung von Streitigkeiten in Datenschutzangelegenheiten ein.[6] Die Kommission beschloss am 12.07.2016, dass die Vorgaben des Privacy-Shield-Abkommens dem Datenschutzniveau der Europäischen Union entsprachen.[7]

---

[2] Der Angemessenheitsbeschluss der EU-Kommission ist abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32000D0520

[3] Die Entscheidung kann abgerufen werden unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0362

[4] Standardvertragsklauseln meint hier von der Kommission vorformulierte und genehmigte Vertragsklauseln. Diese Klauseln werden auch heute in einer aktualisierten Fassung verwendet.

[5] Die EU-Kommission hatte auf diese Vorgehensweise verwiesen. Die Pressemitteilung ist abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5782

[6] Die Maßnahmen werden in einer Pressemitteilung der Kommission detaillierter dargestellt: https://ec.europa.eu/commission/presscorner/detail/de/IP_16_433

[7] Der Angemessenheitsbeschluss kann abgerufen werden unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016D1250

Verschiedene Datenschützer beziehungsweise Datenschutzorganisationen übten Kritik an dem Privacy-Shield-Abkommen.[8] Am 16.07.2020 erklärte der EuGH auch den Angemessenheitsbeschluss der EU-Kommission über das EU-US Privacy Shield durch das Schrems-II-Urteil für nichtig.[9]

Im Anschluss an diese Entscheidung nahmen die USA und die EU-Kommission ***Verhandlungen für ein Nachfolgeabkommen*** auf. Eine Einigung über die grundsätzliche Ausgestaltung wurde aber erst Anfang 2022 getroffen.[10]

Um die Vorgaben aus der Schrems-II-Entscheidung zu erfüllen, haben die USA zu Reformen selbstverpflichtet, um den Schutz von Privatsphäre und bürgerlichen Freiheiten bei der nachrichtendienstlichen Aufklärung zu stärken. Präsident Biden ordnete z. B. mit einem präsidialen Dekret vom 07.10.2022 einige Veränderungen in der geheimdienstlichen Datensammlung an. Der Zugang der US-Nachrichtendienste zu europäischen Daten soll z. B. auf das zum Schutz der nationalen Sicherheit notwendige und verhältnismäßige Maß beschränkt sein. Außerdem soll der „Data Protection Review Court" innerhalb des Justizministeriums eingerichtet werden. Dieser soll Entscheidungen des Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) überprüfen. Dabei wird aber weiterhin an der Massenüberwachung festgehalten.[11]

An diesem Dekret beziehungsweise den darin normierten Sicherheitsgarantien wurde bereits zahlreich Kritik geübt.[12]

Die EU-Kommission scheint von der Qualität der getroffenen Maßnahmen allerdings überzeugt zu sein und hat den Annahmeprozess für einen Angemessenheitsbeschluss gestartet.[13]

Zu hoffen bleibt, dass die Kommission diesmal einen Angemessenheitsbeschluss beschließt, der den Rechtsanwendern eine langfristige Rechtssicherheit bieten kann. Es bleibt abzuwarten, ob dem EuGH die vereinbarten Sicherheitsgarantien dieses Mal ausreichen oder ob er einen eventuellen Angemessenheitsbeschluss wieder für nichtig erklärt.[14]

[8] So z. B. die Artikel-29-Gruppe. Die Stellungnahme der Gruppe ist abrufbar unter: https://ec.europa.eu/newsroom/article29/items/640157/en

[9] Die Entscheidung kann abgerufen werden unter: https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18. Für eine Darstellung der Entscheidung und der aufgestellten Vorgaben an ein DSGVO-konformes Abkommen siehe den Jahresbericht 2020, Abschnitt 2.1.1.

[10] Pressemitteilung der EU-Kommission abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/en/statement_22_2043

[11] Das Dekret des US-Präsidenten kann abgerufen werden unter: https://noyb.eu/sites/default/files/2022-10/Biden%20EO%20on%20Surveillance%2C%20Structured.pdf

[12] So z. B. von der Organisation NOYB. Max Schrems ist Vorsitzender der Organisation. Abrufbar unter: https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law

[13] Die Pressemitteilung der EU-Kommission ist abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7631

[14] Eine Klage gegen die neuen Regelungen ist wohl zu erwarten.

1.2 Gesetzgeberische Entwicklungen in der Bundesrepublik Deutschland

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

1.2.1 Vorratsdatenspeicherung

Die Vorratsdatenspeicherung ist und bleibt ein Dauerthema in der rechtlichen und politischen Diskussion. Mit seiner Entscheidung vom 20.09.2022[15] hat der Europäische Gerichtshof noch einmal deutlich gemacht, dass das Recht der Europäischen Union einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten entgegensteht. Ausnahmen können lediglich in Fällen ernster Bedrohungen für die nationale Sicherheit eines Staates gegeben sein.

Die bisherige Gesetzeslage in der Bundesrepublik Deutschland sah vor, dass Telekommunikationsanbieter einer gesetzlichen Pflicht unterlagen, Daten ihrer Kunden zu speichern und für einen gewissen Zeitraum aufzubewahren. Zu diesen Daten gehörten insbesondere die Verbindungs-, Verkehrs- und Standortdaten. Die Aufbewahrung dieser Daten sollte sicherstellen, dass im Falle des Bedarfs bei einer Strafverfolgung diese Daten noch zur Verfügung stehen und durch die betreffenden Behörden ausgewertet werden können. Das zur Begründung herangezogene Bedrohungsszenario betraf insbesondere die Situation terroristischer Anschläge. Mittels der aufbewahrten Daten können Bewegungsprofile erstellt werden beziehungsweise Bewegungen nachvollzogen werden, sodass ermittelt werden kann, wer sich zu welcher Zeit an welchem Ort aufgehalten hat. Auf diese Weise besteht aus Sicht von Strafverfolgungsorganen die Chance, die betreffende Person mit einer an dem Ort begangenen Straftat in Verbindung zu bringen.

Die Erfassung dieser Daten sowie deren Speicherung und Auswertung führt zu einem Konflikt mit dem Recht auf informationelle Selbstbestimmung. Daher ist das Thema wiederholt Gegenstand von gerichtlichen Entscheidungen, aber auch intensiven politischen und fachlichen Diskussionen gewesen. Mit dem derzeit geltenden Recht waren Entscheidungsträger in der Bundesrepublik Deutschland davon ausgegangen, dass eine rechtskonforme Lösung und eine tragfähige Grundlage geschaffen worden war.

Bereits die Schlussanträge des Generalanwalts der EU in dem oben genannten Verfahren zeigten, dass dies auf europäischer Ebene nicht so gesehen wird. Dies hat der EuGH nunmehr mit seiner Entscheidung bestätigt und seine Rechtsauffassung erneut klargestellt. Kritikpunkte des Gerichtshofs stellten insbesondere die Möglichkeiten zur anlasslosen Speicherung der Daten dar. Die damit verbundene Möglichkeit der Analyse des Privatlebens von betroffenen Bürgern und die Bildung von Profilen wurde durch den EuGH kritisiert. Er hat darin einen Verstoß gegen Art. 7 der europäischen Grundrechte Charta (Achtung des Privat- und Familienlebens) und von Art. 8 der Charta (Grundrecht auf Schutz

[15] Europäischer Gerichtshof, Urteil vom 22.09.2022, Rechtssachen C-793/19 und C-794/19, ECLI:EU:C:2022:702.

personenbezogener Daten) gesehen. Der EuGH hatte bereits in früheren Entscheidungen diese Auffassung deutlich zu erkennen gegeben und setzt sie nunmehr fort. Er führt dazu an, dass die Bevölkerung in der Furcht vor Auswertungen der Daten präventiv ihr Verhalten anpassen und sich in ihren eigenen Freiheiten beschränken würde. Dadurch würde in unangemessener Weise in die Rechte betroffener Personen eingegriffen. Dies darf entsprechend den Vorstellungen des Gerichts nicht geschehen.

Der EuGH hat allerdings auch Ausnahmetatbestände gesehen, in denen die Vorratsdatenspeicherung durchaus zulässig sein kann. Dies gilt insbesondere im Fall des Schutzes der nationalen Sicherheit, wenn sich der Mitgliedstaat einer ernsten Bedrohung für die nationale Sicherheit gegenübersieht. Unter Umständen kann auch eine Vorratsdatenspeicherung bei bestimmten Personengruppen oder an bestimmten Orten zulässig sein. Dabei denkt der EuGH an Fälle von bestimmter Kriminalität sowie von Orten, an denen ein erhöhtes Risiko für schwere Straftaten besteht und benennt dazu Flughäfen oder Bahnhöfe.

Die Bundesregierung ist nun gefordert, eine Änderung des Gesetzes vorzuschlagen, welche die Vorgaben des Europäischen Gerichtshofs berücksichtigt. Noch ist nicht abzusehen, in welcher Weise und mit welchen Inhalten die Bundesregierung die Vorgaben umsetzen will. Jedenfalls wird auch in Zukunft das Thema Vorratsdatenspeicherung Datenschützer, Gerichte und Politiker beschäftigen.

1.2.2 Hinweisgeberschutzgesetz

„Zielsetzung des Gesetzes ist ein besserer Schutz von Hinweisgebern in ihrem beruflichen Umfeld."

Der Deutsche Bundestag hat zum Ende des Berichtsjahres 2022 das „Gesetz für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" (Hinweisgeberschutzgesetz) beschlossen. Das Gesetz bedarf noch der Zustimmung des Bundesrates.

Der Gesetzentwurf sieht die Umsetzung der Hinweisgeberschutz-Richtlinie der Europäischen Union[16] vor. Diese Richtlinie hätte bereits bis zum 17.12.2021 in nationales Recht umgesetzt werden müssen.

Zielsetzung des Gesetzes ist ein besserer Schutz von Hinweisgebern in ihrem beruflichen Umfeld. So soll u. a. ein besserer Schutz vor möglichen Repressalien gewährleistet werden. Sofern betroffene Personen in einem zeitlichen Zusammenhang mit ihren Hinweisen eine Benachteiligung erfahren, soll vermutet werden, dass es sich dabei um eine Repressalie aufgrund des zuvor erteilten Hinweises handelt. Die Beweislast, dass dies nicht der Fall ist, trägt diejenige Person, welche die Benachteiligung veranlasst hat. Unter Umständen trifft den Verursacher eine Verpflichtung zum Schadenersatz. Jedoch kann auch den Hinweisgeber eine solche Pflicht treffen, sofern ein Schaden aufgrund einer vorsätzlichen oder grob fahrlässigen Meldung oder Offenlegung unrichtiger Informationen entstanden ist.

[16] Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

Der Schutz des Gesetzes soll sich auch auf Fälle beziehen, bei denen verfassungsfeindliche Äußerungen von Beamten gemeldet werden.

Weiterhin soll mittels der Einrichtung von sowohl internen als auch externen Meldestellen eine erleichterte Möglichkeit zur Verfügung gestellt werden, die Beobachtungen und Hinweise schildern zu können. Bei beiden Varianten ist eine vertrauliche Behandlung der Identität der hinweisgebenden Person vorgesehen. Eine Verpflichtung zur Ermöglichung der Abgabe anonymer Meldungen ist derzeit nicht vorgesehen. Gegenüber dem bisherigen Entwurf sind anonyme Meldungen, wenn solche bei den Meldestellen eingehen, jedoch zu bearbeiten.

Hinweis für kirchliche Einrichtungen

Die kirchlichen Stellen sollten sich schon jetzt informieren, welche Bestimmungen künftig zu beachten sein werden. Verantwortliche sollten durchaus vorbereitend das Thema in ihre Planungen und Überlegungen aufnehmen und die weiteren gesetzlichen Entwicklungen verfolgen. Sinnvoll ist dabei sicherlich, den eigenen betrieblichen Datenschutzbeauftragten wegen der Sicherstellung der Vertraulichkeiten im Rahmen der Umsetzungen einzubeziehen.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Auch im kirchlichen Bereich sind im Berichtszeitraum neue Regelungen beraten oder verabschiedet worden, die datenschutzrechtliche Vorgaben enthalten.

1.3.1 Personalaktenordnung für Kleriker und Kirchenbeamte

Die Deutsche Bischofskonferenz hat am 23.09.2021 eine bundesweite Standardisierung der Personalaktenordnung für Kleriker und Kirchenbeamte beschlossen.[17] Die PAO sollte in allen deutschen Bistümern (Erz-) Diözesen jeweils als diözesanes Gesetz möglichst wortlautidentisch in den Amtsblättern veröffentlicht werden und zum 01.01.2022 in Kraft treten. Alle (Erz-)Diözesen im Zuständigkeitsbereich des Katholischen Datenschutzzentrums haben diesen Beschluss auch umgesetzt. Anzumerken ist, dass nur ein kleiner Teil der Mitarbeitenden in den (Erz-) Diözesen von der neuen Personalaktenordnung betroffen ist. In ihren Geltungsbereich fallen grundsätzlich nur Kleriker, Kandidaten und Kirchenbeamte (Bedienstete). Das Bistum Essen hat aber beispielsweise die neue Personalaktenordnung auf alle seine Beschäftigten ausgedehnt.[18]

[17] Rahmenordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten (Personalaktenordnung), die Pressemitteilung ist abrufbar unter: https://www.dbk.de/themen/sexualisierte-gewalt-und-praevention/dokumente/offizielle-papiere

[18] Kirchliches Amtsblatt Bistum Essen vom 25.03.2022, Stück 3, S. 56.

Die Standardisierung soll u. a. eine mangelfreiere Personalaktenführung, insbesondere im Hinblick auf die Dokumentation von sexuellem Missbrauch, ermöglichen. In diesem Zusammenhang soll auch die Aufklärung von Sexualstraftaten durch Kleriker und Kirchenbeamte verbessert und die Rechte von Missbrauchsopfern sollen gestärkt werden. Alle Regelungen der PAO sind in datenschutzrechtlicher Hinsicht als Ergänzungen zum Gesetz über den Kirchlichen Datenschutz (KDG) zu verstehen und müssen mit diesem im Einklang stehen.

Für den Datenschutz sind vor allem die Normen über die Weitergabe von Personalakten und die Auskunft an Dritte von Interesse. Grundsätzlich ist die Weitergabe von Personalakten mit der Einwilligung des Bediensteten gemäß § 14 Abs. 1 PAO zulässig. In dieser Hinsicht ergeben sich keine Besonderheiten zum KDG. Hervorzuheben ist aber die Verpflichtung zur Weitergabe der Akte (oder einer Kopie) bei Wechsel des Bediensteten in den Dienst eines kirchlichen Rechtsträgers außerhalb seiner Inkardinationsdiözese und einer Umkardination. Zweck dieser Regelung ist die Vermeidung von Lücken in der Dokumentation von dienstlichem Verhalten des jeweiligen Bediensteten.

Der Auskunftsanspruch aus § 15 PAO ist als Transparenznorm zu verstehen, die aber ausdrücklich kein Akteneinsichtsanspruch ist. Dritte können gemäß § 15 Abs. 1 Auskunft aus Personalakten verlangen, wenn dies für die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder für den Schutz berechtigter, höherrangiger Interessen der oder des Dritten zwingend erforderlich ist. Ein berechtigtes, höherrangiges Interesse liegt nach § 15 Abs. 2 dann vor, wenn der Dritte glaubhaft macht, dass der Bedienstete Handlungen nach dem 13. Abschnitt des Besonderen Teils des Strafgesetzbuches begangen hat und der Dritte als Betroffener der Straftat oder dessen Angehörige ersten Grades auf konkrete Anfragen hin Auskunft begehren.

Die Akteneinsicht für Betroffene im Rahmen von kirchlichen Voruntersuchungen und durch die Kommissionen zur Aufarbeitung von sexuellem Missbrauch in den jeweiligen (Erz-)Diözesen richtet sich nach eigenständigen Regelungen.

1.3.2 Überarbeitung der Kirchlichen Archivordnung

Die derzeit geltende Kirchliche Archivordnung (KAO) ist noch nicht an die seit 2018 geltenden neuen datenschutzrechtlichen Regelungen des Kirchlichen Datenschutzgesetzes angepasst worden. In der Arbeit mit datenschutzrechtlichen Sachverhalten, die auch Fragen der Archivordnung betreffen, besteht dann – wie bei anderen spezialgesetzlichen Regelungen zu datenschutzrechtlichen Fragestellungen auch – manchmal der Anlass zur Prüfung nach § 2 Abs. 2 KDG nach dem Vorrang der spezialgesetzlichen Regelung. § 2 Abs. 2 KDG regelt, dass „soweit besondere kirchliche oder besondere staatliche Rechtsvorschriften auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, […] sie den Vorschriften dieses Gesetzes [vorgehen], sofern sie das Datenschutzniveau dieses Gesetzes nicht unterschreiten".

Bei Anwendung einiger Regelungen der KAO bestehen – auch vor dem Hintergrund von anderslautenden Regelungen z. B. des Landesarchivgesetzes NRW – nun Zweifel, ob diese Prüfung der Unterschreitung des Schutzniveaus des KDG noch zu Gunsten der KAO ausfallen kann. Diese Anmerkungen hat das Katholische Datenschutzzentrum in die Arbeit der im Berichtszeitraum auf Ebene des Verbandes der Diözesen Deutschlands gebildeten Arbeitsgruppe zur Evaluierung der kirchlichen Archivordnung adressieren können. Die Arbeitsgruppe hat noch keine Empfehlung zur Änderung der KAO vorgelegt.

1.3.3 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 auch im Berichtszeitraum weiter an einem Bericht zur Evaluation gearbeitet hat. Die Arbeit konnte noch nicht abgeschlossen werden.

1.4 Weitere datenschutzrechtliche Entwicklungen im kirchlichen Bereich, insbesondere in der Evangelischen Kirche in Deutschland

Im kirchlichen Bereich gab es im Berichtszeitraum weitere berichtenswerte Entwicklungen, von denen hier nur einige wenige erwähnt werden sollen.

1.4.1 Datenschutzaufsichten in der EKD veröffentlichen Entschließung zu Facebook-Fanpages

Die Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland (EKD) hat am 28.04.2022 eine Entschließung veröffentlicht, die sich mit der Nutzung von Facebook-Fanpages durch kirchliche und diakonische Stellen befasst.

Die Konferenz nimmt dabei zunächst Bezug auf die bereits früher von ihr verfasste „Gemeinsame Stellungnahme der Konferenz der Beauftragten für den Datenschutz in der EKD zur Datenübermittlung in die USA“[19] vom 15.05.2021. In dieser hatten die Mitglieder der Konferenz die rechtlichen Grundlagen für Drittstaatentransfers aus dem Bereich der Evangelischen Kirche aufgezeigt und sich zum „Schrems-II-Urteil“ und zu den diesbezüglichen Empfehlungen des Europäischen Datenschutzausschusses (EDSA) geäußert. Weiterhin verweist die Konferenz auf die zu dem Themenbereich ergangenen Veröffentlichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und führt dabei ausdrücklich den Beschluss der DSK vom

[19] https://datenschutz.ekd.de/wp-content/uploads/2021/10/GemeinsameStellungnahmeDatenuebermittlungUSA.pdf

23.03.2022[20] zur Taskforce Facebook-Fanpages auf. Zu dem von der Taskforce für die DSK erstellten Kurzgutachten vom 18.03.2022 erklärt die Konferenz, dass sie der darin dargelegten Bewertung zustimmt.

Aus dieser Einschätzung und der Übereinstimmung mit der Sicht der staatlichen Aufsichten formuliert die Konferenz dann ihre Anforderungen an die kirchlichen und diakonischen Stellen bei der Verwendung von Facebook-Fanpages. Die dabei verwendete Formulierung „haben danach nachzuweisen" verdeutlicht, dass die Mitglieder der Konferenz von den angesprochenen Stellen die Umsetzung der formulierten Vorgaben erwarten und sie nicht bloße Empfehlungen geben wollen.

„Der Datentransfer in Drittländer, für die kein Angemessenheitsbeschluss der Europäischen Kommission oder eine vergleichbare Bewertung vorliegt, stellt nach wie vor eine mit Risiken behaftete Übermittlung dar …"

Der Datentransfer in Drittländer, für die kein Angemessenheitsbeschluss der Europäischen Kommission oder eine vergleichbare Bewertung vorliegt, stellt nach wie vor eine mit Risiken behaftete Übermittlung dar, die sorgfältige Prüfungen und Abwägungen im Vorfeld erfordert. Dies gilt gleichermaßen für den auch bei katholischen kirchlichen Einrichtungen gern genutzten Einsatz von Facebook-Fanpages.

Die Entschließung der Konferenz auf evangelischer Seite bietet erneut Anlass, auf die Erfordernisse eines sorgfältigen Umgangs mit den Themen „Drittlandtransfer" sowie „Facebook-Fanpages" und auf die Beachtung der Empfehlungen des Europäischen Datenschutzausschusses hinzuweisen.

1.4.2 Eigenes Datenschutzrecht der Selbständigen Evangelisch-Lutherischen Kirche

Mit Urteil vom 30.11.2022 wies die 10. Kammer des niedersächsischen Verwaltungsgerichts in Hannover die Klage der Selbständigen Evangelisch-Lutherischen Kirche (SELK) ab und legte damit fest, dass die Religionsgemeinschaft kein eigenes Datenschutzrecht anwenden und auch keine eigene Aufsicht installieren darf, sondern der DSGVO und damit auch der Aufsicht der Landesbeauftragten (LfD) für Datenschutz in Niedersachsen unterliegt.

Dem gerichtlichen Verfahren war eine längere Auseinandersetzung über die Frage, ob die SELK eigenes Datenschutzrecht anwenden darf und welcher datenschutzrechtlichen Aufsicht die Religionsgemeinschaft unterliegt, vorausgegangen. Dabei standen sich die zwei Meinungen gegenüber, dass die SELK ihre eigene Datenschutzrichtlinie anwenden darf und einer eigenen Aufsicht unterliegt wie die Ansicht, dass die SELK der DSGVO und damit der Landesbeauftragten für Datenschutz in Niedersachsen unterliegt.

Durch Urteil vom 30.11.2022 wurde festgestellt, dass die SELK kein eigenes Datenschutzrecht anwenden und somit auch keine eigene Aufsicht installieren darf, da sie nicht von dem Bestandsschutz in Art. 91 Abs. 1 DSGVO profitiert. Die Kammer schloss sich der in der Literatur mittlerweile fast herrschenden Meinung an, dass die Privilegierung, eigenes Datenschutzrecht anzuwenden, nur dann infrage kommt, wenn bereits vor Inkrafttreten der DSGVO eigene umfassende Regelungen

[20] https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf

zum Datenschutz angewandt und diese bis zur Geltung der DSGVO an das in der Verordnung vorgegebene Schutzniveau angepasst wurden. Diese Voraussetzung wurde laut der Urteilsbegründung von der Religionsgemeinschaft nicht erfüllt, sodass der Bestandsschutz keine Wirkung entfaltet und die SELK der DSGVO und der Landesbeauftragten für Datenschutz in Niedersachsen unterfällt.

Einordnung der Entscheidung für die katholische Kirche

Die Entscheidung bringt für die Rechtsprechung in Bezug auf Art. 91 DSGVO wieder ein Stück mehr Klarheit. Es wurde einmal mehr gerichtlich festgestellt, dass bereits im Mai 2016 umfassende Regelungen zum Datenschutzrecht bestehen mussten, damit eine Religionsgemeinschaft von der Privilegierung eigenes Datenschutzrecht anzuwenden profitieren kann. Mit der Anordnung über den kirchlichen Datenschutz (KDO), welche bis zur Geltung der DSGVO im Mai 2018 angepasst wurde, bestand für die katholische Kirche eine solche umfassende Regelung. Durch das pünktlich in Kraft getretene KDG ist auch die Möglichkeit aus Art. 91 Abs. 2 DSGVO eröffnet und die katholische Kirche ist befugt eigene Datenschutzaufsichten zu installieren.

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss ist das in der Datenschutz-Grundverordnung vorgesehene Gremium, in dem sich die Datenschutzaufsichtsbehörden der Mitgliedsländer der EU beraten und u. a. gemeinsame Positionen und Vorgehensweisen beschließen. Nach Art. 70 DSGVO hat der Europäische Datenschutzausschuss insbesondere die Aufgabe, die einheitliche Anwendung der Verordnung sicherzustellen. Zu diesem Zweck kann der EDSA u. a. Leitlinien bereitstellen.[21] Da das kirchliche Datenschutzrecht im Einklang mit der DSGVO erlassen wurde, sollten auch die kirchlichen Stellen immer im Blick haben, mit welchen Themen sich der EDSA befasst.

Auswirkungen auf kirchliche Einrichtungen

Verantwortliche sollten die Entwicklungen im Bereich der Leitlinien des EDSA beobachten. Die Leitlinien sollen für eine europaweite Vereinheitlichung in der Rechtsanwendung der geltenden Gesetze sorgen. Auch wenn der EDSA seine Leitlinien in Bezug auf das staatliche Datenschutzrecht formuliert, wird das Katholische Datenschutzzentrum bei der Prüfung der Rechtsanwendung zum Auskunftsrecht die Vorgaben des EDSA nicht außer Acht lassen.

[21] Vgl. hierzu auch Abschnitt 1.1.1 des Jahresberichts 2018 sowie Abschnitt 1.5 des Jahresberichts 2019. Die Leitlinien können – ebenso wie Pressemitteilungen und weitere Materialien des Europäischen Datenschutzausschusses – über dessen Internetseite (https://edpb.europa.eu) abgerufen werden.

Der Europäische Datenschutzausschuss hat auch in diesem Berichtszeitraum eine Vielzahl an Leitlinien und Empfehlungen beschlossen. Nachstehend werden nur einige wenige Themen aus der Tätigkeit aufgegriffen.

1.5.1 EDSA Leitlinien 1/2022 zu den Rechten der betroffenen Person – Auskunftsrecht

Der Europäische Datenschutzausschuss hatte im Berichtsjahr einen vorläufigen Text für seine neuen „Leitlinien 1/2022 zu den Rechten der betroffenen Person – Auskunftsrecht Version 1.0“ im Rahmen eines Konsultationsverfahrens vorgestellt. Diese Leitlinien befassen sich mit den Rechten betroffener Personen mit dem Ziel, eine europaweit einheitliche Handhabung des Art. 15 DSGVO, der im katholischen Datenschutzrecht § 17 KDG entspricht, zu erreichen.

„Ein Ziel des Auskunftsrechts ist es nach den Darlegungen des EDSA, dem Einzelnen ausreichende, transparente und leicht zugängliche Informationen über die Verarbeitung seiner personenbezogenen Daten zur Verfügung zu stellen.“

Ein Ziel des Auskunftsrechts ist es nach den Darlegungen des EDSA, dem Einzelnen ausreichende, transparente und leicht zugängliche Informationen über die Verarbeitung seiner personenbezogenen Daten zur Verfügung zu stellen. Der Betroffene soll damit in die Lage versetzt werden, die Rechtmäßigkeit der Verarbeitung und die Richtigkeit der verarbeiteten Daten zu erkennen und zu überprüfen. Die beabsichtigten Leitlinien sollen neben der Vereinheitlichung innerhalb der Europäischen Union auch zu einer Vereinfachung für die Betroffenen führen.

Der EDSA unterteilt das Zugangsrecht in drei Bereiche, für die er die Bestätigung, ob Daten über die betroffene Person verarbeitet werden oder nicht, den Zugang zu diesen personenbezogenen Daten und den Zugang zu Informationen über die Verarbeitung benennt.

In diesem Zusammenhang zeigt der EDSA konkrete Prüfpflichten auf, die der für die Verarbeitung Verantwortliche durchführen muss. Dabei ist festzustellen, welche Auskunft konkret begehrt wird und welche Informationen für die Beantwortung erforderlich sind. Besondere Anforderungen an den Antrag des Betroffenen sollen nicht zu beachten sein. Die Verantwortlichen sollen geeignete und benutzerfreundliche Kommunikationskanäle bereithalten, sodass ein möglichst leichter Zugang für die Betroffenen zur Verfügung gestellt wird.

Der Umfang des Auskunftsrechts soll die Vorgaben bezüglich des Begriffs der personenbezogenen Daten, wie er in Art. 4 Nr. 1 DSGVO[22] festgelegt ist, berücksichtigen. Zu diesen Daten muss der Verantwortliche Zugang gewähren und auch zusätzliche Informationen über die Verarbeitung und die Rechte der betroffenen Person bereitstellen. Der EDSA weist darauf hin, dass neben den grundlegenden personenbezogenen Daten auch eine Vielzahl von anderen Daten unter die Definition subsumiert werden können. Dementsprechend soll die Frage nach dem Umfang der zur Auskunft gehörenden Daten nicht zu restriktiv ausgelegt werden. Auch wird beispielsweise darauf hingewiesen, dass die Kommunikationshistorie mit eingehenden und ausgehenden Nachrichten dazugehört. Erwartet wird auch, dass Verantwortliche zusätzliche Informationen über die Verarbeitung und über die Rechte der betrof-

[22] Entspricht § 4 Nr. 1 KDG.

fenen Personen bereitstellen. Im Zweifel soll ein Antrag so zu verstehen sein, dass er sich auf alle personenbezogenen Daten der betroffenen Person bezieht. Gegebenenfalls kann ein Verantwortlicher einen Betroffenen dazu auffordern, den Antrag konkreter zu fassen, sofern große Mengen an Daten verarbeitet werden.

Der EDSA setzt voraus, dass ein Verantwortlicher in allen IT-Systemen und nicht-IT-bezogenen Ablagesystemen nach den personenbezogenen Daten sucht, um keine der Auskunft unterliegenden Daten zu übersehen.

In den Leitlinien wird noch einmal deutlich herausgearbeitet, dass diejenigen Daten zu beauskunften sind, die im Zeitpunkt des Zugangs des Auskunftsbegehrens beim Verantwortlichen vorhanden sind. Zu berücksichtigen ist allerdings, dass die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden. Dies muss der Verantwortliche prüfen und sicherstellen sowie gegebenenfalls die Auskunft in geeigneter Weise unter Beachtung dieser Rechte und Freiheiten anderer umsetzen. Dies darf nach den Vorstellungen des EDSA allerdings nicht so weit gehen, dass der Verantwortliche mit der Begründung und dem Verweis auf die Rechte und Freiheiten anderer die Auskunft insgesamt deutlich reduziert oder ganz verweigert. Vielmehr ist nach geeigneten Lösungen zu suchen, um sämtlichen beteiligten Interessen zu genügen.

Der EDSA betont in den Leitlinien, dass die grundsätzlich vorgesehene gesetzliche Frist von einem Monat nach Eingang des Ersuchens für die Beantwortung einzuhalten ist. Nur erforderlichenfalls kann diese Frist um höchstens zwei weitere Monate verlängert werden, wenn die Komplexität und die Zahl der Anträge dies notwendig machen. In einem solchen Fall ist die antragstellende Person über den Grund für die Verzögerung zu informieren.

Dazu ist anzumerken, dass ein Verantwortlicher generell darauf achten sollte, sich und seine Einrichtung so zu organisieren und die erforderlichen Maßnahmen zu ergreifen, dass eine Beantwortung innerhalb des gesetzlich vorgesehenen Zeitraums erfolgen kann. Auch ist bei Daten, die nur über einen kurzen Zeitraum gespeichert werden, darauf zu achten, dass sie nicht gelöscht werden und zur Verfügung stehen, solange noch ein Auskunftsverfahren bezüglich der betroffenen Person anhängig ist.

Der EDSA spricht in seinen Ausführungen an, dass Art. 12 Abs. 5 DSGVO[23] zwar ermöglicht, Antragsbegehren, die offensichtlich unbegründet oder übertrieben sind, abzulehnen oder eine angemessene Gebühr für entsprechende Anträge zu verlangen. Er weist aber darauf hin, dass dies eng auszulegen ist. Dementsprechend ist die Möglichkeit, einen Antrag als offensichtlich unbegründet abzulehnen, eingegrenzt. Der EDSA empfiehlt, dass der Verantwortliche dafür Sorge tragen muss, einen offensichtlich unbegründeten oder übermäßigen Charakter eines Antrags nachweisen zu können. Der EDSA spricht auch an, dass Beschränkungen des Auskunftsrechts gegebenenfalls auf dem nationalen Recht der Mitgliedsstaaten beruhen können. Auch dazu macht der EDSA deutlich, dass die Voraussetzungen, die nach nationalem

„… ein Verantwortlicher [sollte] … darauf achten …, sich und seine Einrichtung so zu organisieren …, dass eine Beantwortung [des Auskunftsbegehrens] innerhalb des gesetzlich vorgesehenen Zeitraums erfolgen kann."

[23] Entspricht § 14 Abs. 5 KDG.

Recht bestehen, sorgfältig zu prüfen und einzuhalten sind. Er betont, dass keine darüber hinausgehenden Ausnahmen oder Abweichungen zulässig sind.

Gemäß Art. 12 Abs. 1 S. 1 DSGVO[24] muss die Auskunft in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erteilt werden. Nach Auffassung des EDSA muss der Verantwortliche geeignete Maßnahmen treffen, um die Beauskunftung im Sinne des Gesetzes realisieren zu können. Dazu müssten erforderlichenfalls die im Rahmen eines Auskunftsbegehrens zur Verfügung gestellten Daten zur besseren Verständlichkeit in geeigneter Weise aufbereitet und erläutert werden.

Bezüglich der Frage nach Kopien sieht der EDSA darin zunächst die hauptsächliche Form der Überlassung von Daten. Er kann sich aber auch andere Varianten vorstellen, z. B. durch Erteilung von Informationen oder durch einen Zugang zu Daten vor Ort. Auch die Bereitstellung von Informationen auf verschiedenen Ebenen ist aus Sicht des EDSA eine mögliche Option. Grundsätzlich sollen die Kopien der Daten und die zusätzlichen Informationen in einer dauerhaften Form zur Verfügung gestellt werden, was klassischerweise eine Übermittlung in schriftlicher Form bedeutet. Allerdings soll auch ein gängiges elektronisches Format möglich sein, sodass die betroffene Person die Informationen leicht herunterladen kann.

Soweit Bild- und Sprachaufnahmen betroffen sind, ist der betroffenen Person gemäß den Leitlinien eine Kopie der Bild- oder Sprachaufnahmen zur Verfügung zu stellen. Ausnahmen bestehen nur dann, wenn die Rechte und Freiheiten anderer Personen dadurch ansonsten beeinträchtigt werden. In diesen Fällen kann unter Umständen eine Schwärzung oder gegebenenfalls eine Beschreibung des Bildinhaltes sowie ein angemessen geschwärztes Transkript einer Tonaufnahme ausreichend sein.

1.5.2 Guidelines 9/2022 on personal data breach notification under GDPR

Mit den „Guidelines 9/2022 on personal data breach notification under GDPR" hat der EDSA im Oktober 2022 die ursprünglich in seiner ersten Plenarsitzung gebilligten „Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01" der Artikel-29-Gruppe aktualisiert. Im Zeitraum von Mitte Oktober bis Ende November 2022 fand eine öffentliche Konsultation zur geänderten Ziffer 73 der Leitlinien statt. Da sich der geänderte Absatz mit der Meldepflicht von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern, welche einen Vertreter in der Union benannt haben, befasst, sind Auswirkungen dieser Änderung auf den kirchlichen Bereich nicht ersichtlich. Daher bringt die Neufassung des bisherigen WP250 in Bezug auf den Umgang mit Verletzungen des Schutzes personenbezogener Daten keine Änderungen für die kirchlichen Einrichtungen und kann von den kirchlichen Stellen weiter als Hilfestellung herangezogen werden.

[24] Entspricht § 14 Abs. 1 KDG.

Die aktuellen Leitlinien erläutern die Anforderungen, welche die DSGVO an die Melde- und Benachrichtigungspflicht und die damit einhergehende Kommunikation stellt. Auch werden einige Beispiele dafür genannt, was die Verantwortlichen und Auftragsverarbeiter unternehmen können, um diesen Anforderungen gerecht zu werden.

Die Leitlinien beschäftigen sich zunächst mit der Definition (vgl. Art. 4 Nr. 12 DSGVO, vergleichbare Regelung im KDG ist § 4 Nr. 14 KDG) sowie einigen Arten von Verletzungen des Schutzes personenbezogener Daten und sodann mit deren Konsequenzen. Erläutert werden die Verletzung der Vertraulichkeit (Confidentiality breach), die Verletzung der Integrität (Integrity breach) und die Verletzung der Verfügbarkeit (Availability breach).

Anschließend setzt sich der EDSA mit der Meldepflicht an die zuständige Aufsicht auseinander. Insbesondere damit, wann eine solche zu erfolgen hat, wann eine Verletzung dem Verantwortlichen „bekannt" ist und welche Informationen bereitgestellt werden müssen.[25]

Darüber hinaus wird auf die Benachrichtigungspflicht der betroffenen Person eingegangen.[26] Auch hier stellen sich nämlich die Fragen, wann diese zu benachrichtigen ist, welche Informationen bereitgestellt werden müssen und wie dies zu erfolgen hat.

1.5.3 Leitlinien 3/2022 des Europäischen Datenschutzausschusses zu irreführenden Gestaltungen von Schnittstellen Social Media-Plattformen

Der Europäische Datenschutzausschuss hatte im März 2022 eine erste Version von Leitlinien zu irreführenden Gestaltungen der Schnittstellen sozialer Medienplattformen veröffentlicht. Nach der Auswertung der Rückmeldungen aus der Konsultationsphase hat der EDSA im Februar 2023 auf seiner Website die Leitlinien „deceptive design patterns in social media platform interfaces: how to recognise and avoid them" (täuschende Gestaltungsmuster in Interfaces sozialer Medienplattformen: Wie man sie erkennt und vermeidet) in der Version 2 nach der Konsultation veröffentlicht.[27] Die Leitlinien bieten praktische Empfehlungen für Anbieter, Verantwortliche, Entwickler und Nutzer von sozialen Medien um irreführende Gestaltungen sozialer Medien, die gegen die DSGVO verstoßen, zu vermeiden. Irreführende Gestaltungsmuster i. S. d. Richtlinie beschreiben solche Interfaces, die versuchen, die Nutzer derart zu beeinflussen, dass sie unbeabsichtigte, ungewollte und potenziell schädliche Entscheidungen bezüglich ihrer personenbezogenen Daten treffen. Diese Entscheidung geht häufig in eine Richtung, die sich gegen die Interessen der Nutzer und zugunsten der Interessen der sozialen Medienplattformen auswirkt. Die in den Leitlinien behandelten irreführenden Gestaltungsmuster werden in folgende Kategorien eingeteilt:

„Die Leitlinien bieten praktische Empfehlungen … um irreführende Gestaltungen sozialer Medien, die gegen die DSGVO verstoßen, zu vermeiden."

[25] Vgl. hierzu auch Art. 33 DSGVO und § 33 KDG.
[26] Vgl. hierzu auch Art. 34 DSGVO und § 34 KDG.
[27] Die Leitlinien können auf der Website des EDSA in englischer Sprache abgerufen werden: https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

1. **Overloading** (Überlastung) bedeutet, dass die Nutzer mit einer großen Menge von Anfragen, Informationen, Optionen oder Möglichkeiten konfrontiert werden, um sie zu veranlassen, mehr Daten preiszugeben oder ungewollt eine Verarbeitung personenbezogener Daten entgegen den Erwartungen der betroffenen Person zuzulassen.

2. **Skipping** (Überspringen) bedeutet, dass das Interface oder die Benutzerführung so ausgestaltet ist, dass die Benutzer nicht über alle Datenschutzaspekte nachdenken.

3. **Stirring** (Mitreißen) beeinflusst die Entscheidungen der Nutzer, indem es an ihre Gefühle appelliert oder sie visuell anregt (manchmal auch „**nudging**" genannt).

4. **Obstructing** (Behindern) bedeutet, dass der Informations- und Verwaltungsprozess der Nutzer bezüglich ihrer Daten erschwert oder unmöglich gemacht wird.

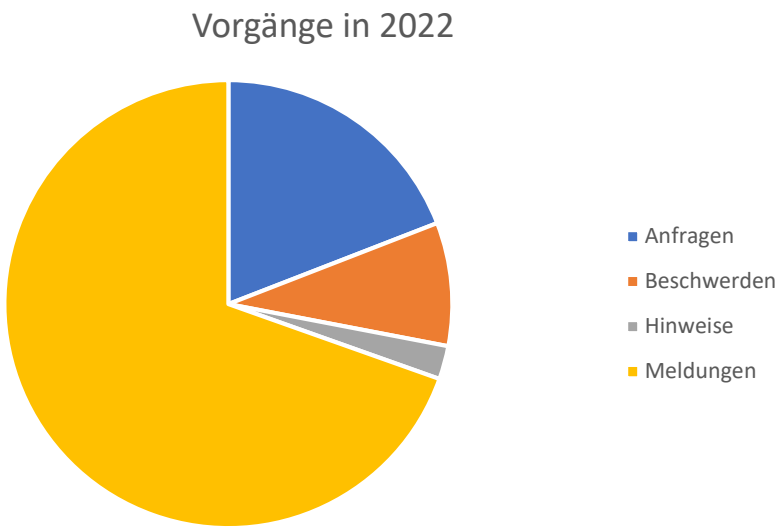
5. **Fickle** (Unbeständig) bedeutet, dass das Design des Interface uneinheitlich und unklar ist, sodass es für den Benutzer schwierig ist, sich in den verschiedenen Datenschutzkontrollinstrumenten zurechtzufinden und den Zweck der Verarbeitung zu verstehen.

6. **Left in the dark** (Im Dunkeln gelassen) bedeutet, dass ein Interface so ausgestaltet ist, dass Informationen oder Datenschutzkontrollinstrumente verborgen werden oder die Nutzer im Unklaren darüber gelassen werden, welche Kontrolle sie in Bezug auf die Ausübung ihrer Rechte haben können.

Die Leitlinien des EDSA orientieren sich an den gesetzlichen Vorgaben der DSGVO. Insbesondere an den Verarbeitungsgrundsätzen aus Art. 5 DSGVO (entspricht § 7 KDG), den Anforderungen für Einwilligungen nach Art. 7 DSGVO (entspricht § 8 KDG) und z. B. dem Grundsatz der Datensparsamkeit aus Art. 25 DSGVO (entspricht § 26 KDG). Neben Hinweisen zu den allgemeinen Datenschutzgrundsätzen enthalten die Leitlinien auch viele Anwendungsfälle und Beispiele für aus Sicht des EDSA (noch) datenschutzkonforme und nicht mehr datenschutzkonforme Umsetzungen von Schnittstellen. Die Leitlinien sollten auch von Verantwortlichen katholischer Einrichtung zur datenschutzkonformeren Ausgestaltung ihrer Plattformen verwendet werden.

2 Aus der Tätigkeit des Datenschutzzentrums

Im Berichtsjahr 2022 handelte es sich bei den meisten Eingaben an das Katholische Datenschutzzentrum erneut um Meldungen von Datenschutzverletzungen. Auch wenn die Anfragen und Beschwerden beziehungsweise Hinweise zahlenmäßig hinter den Meldungen zurückbleiben, so sind sie in der Bearbeitung der einzelnen Vorgänge oft zeitaufwendiger.



2.1 Beratungen und Anfragen

Die Beantwortung von Anfragen und ganz allgemein die Beratung kirchlicher Stellen sind wichtige Bestandteile der Arbeit des Katholischen Datenschutzzentrums. Mit dieser vom KDG mehrfach betonten Beratungstätigkeit 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 offene Fragen im Vorfeld zu klären, wurde im Berichtszeitraum auch weiterhin umfangreich genutzt.

„Die Beantwortung von Anfragen und ganz allgemein die Beratung kirchlicher Stellen sind wichtige Bestandteile der Arbeit des Katholischen Datenschutzzentrums."

2.1.1 Videoüberwachung

Auch im Jahr 2022 erreichten das Katholische Datenschutzzentrum wieder viele Anfragen bezüglich der datenschutzkonformen Ausgestaltung einer Videoüberwachung. Dabei stammte die überwiegende Anzahl der Anfragen von Gemeinden, deren Anliegen die Verhinderung von Vandalismus an und um ihre Gebäude beziehungsweise Grundstücke war.

Zur Erstellung eines validen Videoüberwachungskonzepts sollte die „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen" der Datenschutzkonferenz, des Gremiums der unabhängigen deutschen Datenschutzaufsichten des Bundes und der Länder, Beachtung finden. Neben der Erforderlichkeitsprüfung und der anzustellenden Interessenabwägung sind die Informationspflichten des Verantwortlichen und die Erstellung eines Verarbeitungsverzeichnisses unbedingt zu beachten.[28]

2.1.2 Weitergabe von Daten an Dritte ohne Einwilligung

Im Berichtsjahr wurde das Katholische Datenschutzzentrum auch mit Anfragen bezüglich der Weitergabe von personenbezogenen Daten an Dritte befasst. Rechtlich handelt es sich dabei um eine Offenlegung durch Übermittlung i. S. d. § 4 Nr. 3 KDG und mithin um eine Verarbeitung, für welche es eine Rechtsgrundlage braucht (vgl. § 6 KDG).

Eine Anfrage war darauf gerichtet, ob der Verantwortliche (die Einrichtung) auf Grundlage des § 117 Heilberufsgesetz NRW (HeilBerG) berechtigt beziehungsweise verpflichtet ist, die unter § 115 Abs. 6 Nr. 1 bis 6 HeilBerG genannten Angaben an die Pflegekammer NRW weiterzuleiten.

Eine Verpflichtung zur Übermittlung besteht nach dem Wortlaut der Norm, wenn die Einrichtung vom Errichtungsausschuss beziehungsweise der Pflegekammer zur Übermittlung aufgefordert wird. Daher stellte im angefragten Fall § 6 Abs. 1 lit. d) KDG i. V. m § 117 Abs. 1 S. 1 HeilBerG die Rechtsgrundlage für die Übermittlung der personenbezogenen Daten an den Einrichtungsausschuss und die Pflegekammer dar. Eine anlasslose Übermittlung ist von der Norm allerdings nicht umfasst.

Eine weitere Anfrage beschäftigte sich mit dem Antrag auf Gleichstellung mit einem schwerbehinderten Menschen nach § 2 Abs. 3 SGB IX. Gegenstand war eine Datenübermittlung, wenn der Verantwortliche durch die Agentur für Arbeit als Arbeitgeber zur Situation im Arbeitsalltag der betroffenen Person befragt wird.

Derartige Anfragen, bei denen staatliche Behörden bei den kirchlichen Stellen Informationen anfragen, erfolgen häufig mit kurzer Fristsetzung. Jedoch kann eine spontane und stichhaltige Auskunft aufgrund der Vielzahl von Gesetzen nicht immer gewährleistet werden. Im beschriebenen Fall war die Übertragung aufgrund einer Einwilligung der betroffenen Person möglich. Dabei sollten aber die Grundsätze des § 53 KDG beachtet werden, d. h., es sollte insbesondere auf die Freiwilligkeit der Erklärung geachtet werden.

[28] Für eine detaillierte Darstellung der Problematik und der anzustellenden Überlegungen rund um den Themenkreis Videoüberwachung siehe Abschnitt 2.8 des Jahresberichts 2021.

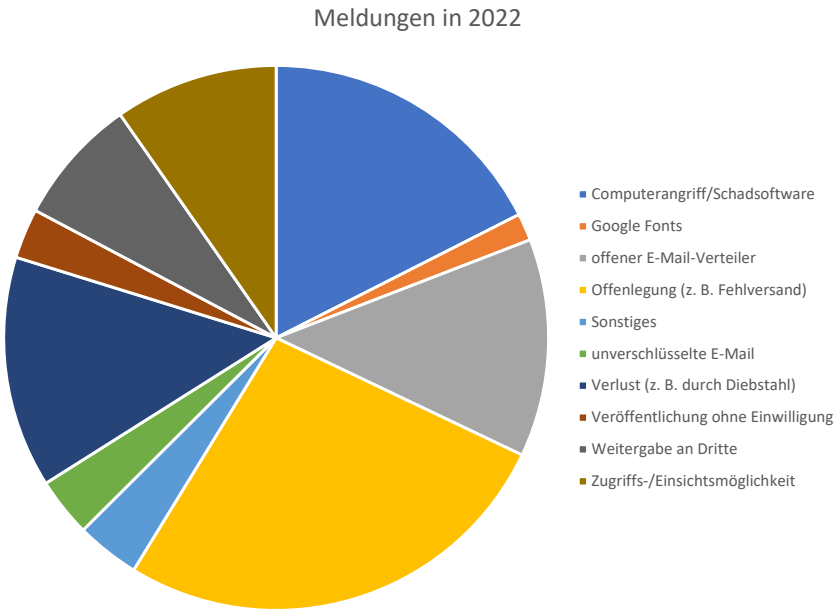
Hinweis für kirchliche Einrichtungen

Grundsätzlich ist den Verantwortlichen zu raten, bei Ersuchen von staatlichen Stellen nicht übereilt personenbezogene Daten herauszugeben, bevor unzweifelhaft geklärt ist, auf welcher rechtlichen Grundlage welche Daten von der anfordernden Stelle verlangt werden können. Da die anfragende Stelle wissen sollte, auf welcher rechtlichen Grundlage sie die Daten anfordert, lohnt bei Unklarheiten stets eine Rückfrage, um kein unnötiges Risiko einzugehen.

2.2 Meldungen von Datenschutzverletzungen

Die Anzahl der im Jahr 2022 an das Katholische Datenschutzzentrum gerichteten Meldungen von Datenschutzverletzungen nach § 33 KDG war weiterhin sehr hoch, im Vergleich zum Vorjahr stieg die Zahl leicht.

Die nachfolgende Darstellung zeigt eine grobe thematische Einordnung der eingegangenen Meldungen im Berichtszeitraum. Einzelne Themen werden im Folgenden aufgegriffen.



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.

2.2.1 Ransomware-Angriffe auf Dienstleister

2022 haben Cyberangriffe in Form von Ransomware auch Dienstleister (Auftragsverarbeiter gemäß § 29 KDG) der katholischen Kirche befallen. Das KDSZ zeigt in diesem Bericht exemplarisch zwei Fälle.

Zwei zentrale Rechenzentrumsdienstleister wurden erfolgreich mit Ransomware angegriffen. Die Verschlüsselung von Filesystemen, Datenbanken und ganzer Server brachte den Betrieb zum Erliegen. Vertragsgemäß meldeten die Dienstleister diese Datenschutzverletzung dem Verantwortlichen der wiederum gemäß §33 KDG eine Meldung über eine Datenschutzverletzung beim Katholischen Datenschutzzentrum durchführte. Da beide Dienstleister auch als Verantwortliche im Sinne der DSGVO arbeiten, wurde die Datenschutzverletzung ebenfalls bei der zuständigen staatlichen Datenschutzaufsicht gemeldet. In der weiteren Bearbeitung tauschten sich die staatliche Datenschutzaufsicht und das Katholische Datenschutzzentrum über die Vorfälle aus.

Nach einer ersten Analyse bei den betroffenen Dienstleistern stellte sich heraus, dass personenbezogene Daten in großem Umfang betroffen waren. Durch die eingeschalteten IT-Forensiker wurde festgestellt, dass einmal rund 7 GB und in dem anderen Fall über 20 GB an komprimierten Daten abgeflossen sind. Beide Dienstleister haben direkt nach Bekanntwerden des Vorfalls die betroffenen Systeme vom Netzwerk getrennt.

Bei einem Dienstleister konnten die Systeme aus Backups wieder hergestellt und damit der Betrieb wieder aufgenommen werden. Durch die Verantwortlichen, die dem KDG unterliegen, wurden beim Dienstleister nur pseudonymisierte Daten verarbeitet, sodass die Risikobewertung in diesem Einzelfall ergab, dass eine Benachrichtigung der Betroffenen nicht notwendig war. Die Angreifer hatten dem Dienstleister gedroht, alle erbeuteten Daten auf einer Plattform im Darknet zu veröffentlichen. Kurz vor dem angekündigten Veröffentlichungsdatum gab es seitens des Dienstleisters eine Entwarnung, dass die Bedrohung durch eine Veröffentlichung nicht mehr gegeben ist. In diesem Falle ist davon auszugehen, dass es eine Einigung zwischen den Angreifern und dem Dienstleister gegeben hat. Eine Veröffentlichung der Daten im Darknet hat laut Aussage des betroffenen Dienstleisters nicht stattgefunden.

Beim zweiten Dienstleister ist nicht der komplette Datenbestand des Dienstleisters verschlüsselt worden. Die Einrichtungen der katholischen Kirche, die ihre Daten dort hosten, sind angabegemäß nicht von diesem Vorfall betroffen gewesen. Der Dienstleister hat neben den Hostingdaten auch Zugangsdaten für Supportdienstleistung bei Verantwortlichen gespeichert. Direkt nach Bekanntwerden des Vorfalls wurden die Verantwortlichen benachrichtigt und die Supportzugänge des Dienstleisters deaktiviert. Für Supportdienstleistungen waren neben den Zugangsdaten zum Netzwerk des Verantwortlichen auch Zugangsdaten für Server- und Datenbanksysteme beim Dienstleister gespeichert. Bei den Verantwortlichen wurden keine Zugriffe über die Zugangsdaten des Supports erkannt. Gemeinsam mit dem Dienstleister wurden Server- und Datenbankpasswörter beim Verantwortlichen geändert und die betroffenen Applikationen beim Verantwortlichen wieder in Betrieb genommen. Nach der Wiederherstellung der Systeme beim Dienstleister wurden die Zugangsdaten der Supportzugänge geändert und für

den Dienstleister wieder freigegeben. Auch in diesem Fall konnten die betroffenen Systeme neu aufgebaut und aus Backups wieder hergestellt werden. Eine angedrohte Veröffentlichung der erbeuteten Daten durch den Angreifer ist laut Aussage des betroffenen Dienstleisters ausgeblieben.

Bei beiden Dienstleistern wurde beim Wiederaufbau der IT-Systeme mithilfe von externem IT-Consulting und IT-Forensikern auf zuvor erstellte Backups zurückgegriffen. In beiden Fällen ist die Ursache für den Angriff mit Ransomware nicht mit Sicherheit zu bestimmen. Mit hoher Wahrscheinlichkeit ist aber durch eine E-Mail mit einem manipulierten Anhang der Initiator der Schadsoftware ins Unternehmen gelangt.

Ein funktionierendes und getestetes Backup- sowie Anti-Malware-Konzept in Verbindung mit sensibilisierten, geschulten Mitarbeitenden bieten einen guten Schutz gegen Angriffe mit Ransomware.

„Ein funktionierendes und getestetes Backup- sowie Anti-Malware-Konzept in Verbindung mit sensibilisierten, geschulten Mitarbeitenden bieten einen guten Schutz gegen Angriffe mit Ransomware."

2.2.2 Cyberangriff auf einen Dienstleister der Wohnungswirtschaft

In der zweiten Jahreshälfte 2022 gingen beim KDSZ zahlreiche Meldungen bezüglich einer Datenschutzverletzung bei einem Auftragsverarbeiter ein.

Ein Dienstleister der Wohnungswirtschaft wurde ab Mitte Juli 2022 Opfer eines Cyberangriffs. Es handelte sich um eine Lösegeld-Attacke, bei welcher sich die Angreifergruppe Zugang zu den IT-Systemen des Dienstleisters verschaffte, eine Vielzahl von Systemen verschlüsselte, Daten von Fileservern kopierte und diese später im Darknet veröffentlichte.

Der Dienstleister der Wohnungswirtschaft war in den gemeldeten Fällen Auftragsverarbeiter für u. a. Heizkostenabrechnungen. Bei dem Angriff wurden auch personenbezogene Daten von ehemaligen und teilweise wohl auch aktuellen Mietern aus den Verantwortungsbereichen kirchlicher Einrichtungen veröffentlicht. Bei den Daten handelte es sich um ein Archiv aus den Jahren 2006 bis 2012. Enthalten sind die Adresse, Liegenschaftsnummer, Verbrauchsdaten (Heiz-, Warm- und Kaltwasserverbrauch), Nutzername, Nutzernummer sowie die beheizte Fläche.

Da es sich bei dem betroffenen Dienstleister um ein Unternehmen im Zuständigkeitsbereich der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI) handelt, erfolgte die initiale Meldung eines Datenverlustes bei der LDI.

Im Rahmen von Analysen wurde dem Dienstleister am 18.08.2022 bekannt, dass auch Auftragsdaten von Kunden in Deutschland abgegriffen und im Darknet veröffentlicht worden waren. Zu diesen Kunden gehörten auch die meldenden Einrichtungen aus dem Zuständigkeitsbereich des Katholischen Datenschutzzentrums. Trotz der gesetzlichen Vorgabe des § 33 Abs. 2 KDG, dass der Auftragsverarbeiter, dem eine Verletzung des Schutzes personenbezogener Daten bekannt wird, diese unverzüglich dem Verantwortlichen zu melden hat, erfolgten

> **„... die Bearbeitung einer Datenschutzverletzung [ist] nicht mit der Meldung an die Datenschutzaufsicht abgeschlossen ...“**

einige Meldungen erst über 30 Tage nach dem Bekanntwerden. Insofern sollten die Verantwortlichen ihre Auftragsverarbeiter dazu anhalten, Datenschutzverletzungen wirklich zeitnah zu melden.

Im Rahmen der Bearbeitung der Meldungen wurde zudem ersichtlich, dass viele Verantwortliche offenbar davon ausgehen, dass die grundsätzliche Meldung eines Vorfalls genügt und weitere, erst später bekannt werdende Einzelheiten nicht mehr nachzumelden sind. Ganz im Gegenteil ist es jedoch so, dass die Bearbeitung einer Datenschutzverletzung nicht mit der Meldung an die Datenschutzaufsicht abgeschlossen ist. Vielmehr ist der Verantwortliche gemäß § 33 Abs. 4 KDG dazu verpflichtet, die in Absatz 3 genannten Informationen unaufgefordert und ohne unangemessene weitere Verzögerung schrittweise zur Verfügung zu stellen.

In vielen Fällen fehlte es u. a. an der Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen nach § 33 Abs. 3 lit. d) KDG. Lediglich in einem Fall trat der meldende betriebliche Datenschutzbeauftragte wiederholt an das KDSZ heran, lieferte im Rahmen des Möglichen ergänzende Informationen und suchte den Austausch.

Für die weitere Bearbeitung der Meldungen war mithin ein Austausch zwischen dem KDSZ und der LDI erforderlich. Ein solcher Austausch ist immer wünschenswert, sollte jedoch nicht notwendig sein, um an die benötigten, vom Verantwortlichen zu liefernden Informationen zu gelangen.

2.2.3 Datenschutz-Vorfall in einem Rechenzentrum

Zu Beginn des Jahres gingen Meldungen zu einer Datenschutzverletzung im Bereich des kirchlichen Meldewesens ein.

Aufgrund eines Fehlers in der Softwareentwicklung bei einem Rechenzentrum, welcher sich durch ein übereiltes Einspielen des Updates ohne Freigabekonzept im Produktivsystem auswirkte, kam es Ende Januar für einen Zeitraum von Freitag gegen 22 Uhr bis Samstag gegen 11:30 Uhr dazu, dass es allen registrierten Nutzern zweier betroffener Anwendungen möglich war, lesend auf alle Meldedaten der 15 angeschlossenen (Erz-)Diözesen zuzugreifen. Betroffen waren personenbezogene Daten der Datenschutzklassen II und III. Durch die Zugriffe war das Schutzziel der Vertraulichkeit verletzt.

Da aufgrund der Vielzahl an betroffenen (Erz-)Diözesen die Zuständigkeit verschiedener Aufsichten gegeben war, führte die für das Rechenzentrum örtlich zuständige Aufsicht eine Vor-Ort-Prüfung durch, während die anderen Aufsichten – unter ihnen auch das Katholische Datenschutzzentrum – die Meldungen der betroffenen (Erz-)Diözesen in ihrem jeweiligen Zuständigkeitsbereich bearbeiteten. Die Aufsichten stimmten sich laufend über ihre Ergebnisse ab.

Bereits kurze Zeit später kam es trotz der infolge des ersten Vorfalls ergriffenen Maßnahmen Mitte Mai erneut zu einem weiteren Vorfall in dem Rechenzentrum. Aufgrund eines anders gelagerten Fehlers bei der

Softwareentwicklung haben in einem Zeitraum von ca. fünf Tagen 17 Nutzer einer Anwendung personenbezogene Daten von 28 Betroffenen unberechtigt abgerufen. Aufgrund einer fehlerhaften Zuordnung wurden die betroffenen Personen nicht nur ihrer Stammgemeinde zugeordnet, sondern zusätzlich und fälschlich einer zusätzlichen Gemeinde. Hierdurch konnten die Mitarbeitenden dieser anderen Kirchengemeinden ebenfalls auf die Daten zugreifen.

Daraufhin fanden weitere Gespräche zwischen dem Katholischen Datenschutzzentrum, dem Rechenzentrum und einer der betroffenen Diözesen aus dem Zuständigkeitsbereich des KDSZ statt, um den Vorfall aufzuklären und über Folgemaßnahmen zu entscheiden. Die Aufarbeitung der Vorfälle dauert noch an. Das Katholische Datenschutzzentrum steht weiterhin im Austausch mit den Verantwortlichen und den anderen Aufsichten.

2.2.4 Weitergabe von Daten an Dritte ohne Einwilligung

Im Bereich der Meldungen von Verletzungen des Schutzes personenbezogener Daten nach § 33 KDG stellt die unbefugte Offenlegung einen stetigen Problemfall dar.

So führte der Versand eines Arztbriefes an einen möglichen weiterbehandelnden Arzt ohne die erforderliche schriftliche Dokumentation einer Einwilligungserklärung in der Folge zu Beweisproblemen.

Einen Fall mit weitreichenderen Folgen für die handelnde Person gab es infolge einer Corona-Infektion einer Ärztin. Da sie ihre Patientin anscheinend nicht selbst über ihre Erkrankung informieren wollte oder konnte, gab sie die Kontaktdaten einer ihrer Patientinnen an ihren Ehemann weiter, damit dieser die Patientin (über den Umweg über deren Arbeitgeber) kontaktieren konnte, um sie über eine mögliche Ansteckungsgefahr in Kenntnis zu setzen. Zwar war die Absicht des Infektionsschutzes eine gute, allerdings war das Handeln der Ärztin aufgrund des Fehlens einer Rechtsgrundlage datenschutzrechtlich äußerst problematisch. Zudem kann ein solches Handeln, abgesehen von den datenschutzrechtlichen Folgen, auch arbeits- und strafrechtliche Konsequenzen nach sich ziehen.

In einigen Einrichtungen wurde angesichts der Corona-Pandemie ein Krisenstab zur Koordinierung, Einführung und Abstimmung von Maßnahmen eingerichtet. Ein Verantwortlicher zeigte sich jedoch lernresistent bezüglich der Offenlegung von personenbezogenen Daten gegenüber dem Krisenstab. Für die Erfüllung seiner ihm übertragenen Aufgaben benötigte der Krisenstab lediglich die Anzahl der aktuell an Corona erkrankten Mitarbeitenden. Dennoch wurden mehrfach aufgrund von Unachtsamkeiten und unzureichender Kommunikation die Namen der erkrankten Mitarbeitenden mit übermittelt. Erst nach dem dritten Verstoß innerhalb kurzer Zeit konnte dieser Mangel abgestellt werden.

Zu einem ähnlichen Vorfall kam es, indem eine Stationsleitung auf eine vorausgegangen Informations-E-Mail zum Meldeweg bei Covid-Fällen dem gesamten E-Mail-Verteiler antwortete und so die Erkrankung einer

Mitarbeitenden, sowie deren Geburtsdatum, private Anschrift, Telefonnummer und Berufsbezeichnung offenlegte. Unabhängig davon, ob für die Meldung tatsächlich alle offengelegten personenbezogenen Daten erforderlich waren, ist ein solcher Datenschutzverstoß ausschließlich auf mangelnde Aufmerksamkeit zurückzuführen, weshalb eine regelmäßige Sensibilisierung auch ohne eine explizite gesetzliche Verpflichtung angezeigt erscheint.

Dass eine fortlaufende Sensibilisierung der Mitarbeitenden erforderlich ist, zeigte auch die Meldung eines Vorfalls aus einer Pflegeeinrichtung. Dort hatte ein Mitarbeiter des Nachtdienstes eine private Bodycam während des Dienstes im Einsatz. Anlass hierfür war die Sorge vor Beweisschwierigkeiten, wenn es zu Vorfällen mit Bewohnern kommen sollte, da er meist alleine im Dienst war. Auch wenn dieser Gedanke nachvollziehbar erscheint, steht er im Widerspruch zu den datenschutzrechtlichen Vorgaben.

Eine weitere Meldung einer unzulässigen Weitergabe von personenbezogenen Daten hatte auch eine Beschwerde zur Folge. In diesem Fall verweigerte die betroffene Person mehrfach die Unterzeichnung einer Einwilligungserklärung zum Zwecke der Datenübermittlung an eine Abrechnungsfirma. Nachdem die betroffene Person im Nachgang nicht auf eine E-Mail mit der Ankündigung der beabsichtigten Datenübermittlung reagierte, wurden die personenbezogenen Daten an den Dienstleister übermittelt.

Die betroffene Person hatte in die Verarbeitung ihrer personenbezogenen Daten zum Zwecke der Weitergabe für eine Rechnungserstellung nicht wirksam eingewilligt. Eine Einwilligung ist wirksam, wenn die betroffene Person mit einer abgegebenen Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Willensbekundung muss für den bestimmten Fall in informierter Weise freiwillig und unmissverständlich sein. Vor allem die Freiwilligkeit ist prägende Voraussetzung für die Wirksamkeit der Einwilligung.

Es lag schon keine Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung vor. Zwar ist es richtig, dass eine betroffene Person nach der oben genannten Definition im jeweiligen Kontext auch durch eine Verhaltensweise ihre Einwilligung erklären kann. Diese Verhaltensweise muss allerdings wie jede andere Erklärung i. S. d. Norm eindeutig sein. Die betroffene Person hat unstreitig die Unterzeichnung des Behandlungsvertrags und der Einwilligungen zur Datenübermittlung an Dritte mehrfach verweigert. In diesem Zusammenhang konnten das Verhalten und die Aufforderung zur Rechnungsstellung per E-Mail nicht als eindeutig bestätigende Handlung für eine Weitergabe der personenbezogenen Daten verstanden werden. Hier musste die Erklärung der betroffenen Person viel eher so verstanden werden, dass diese die Rechnungsstellung unmittelbar durch die verantwortliche Stelle wünschte.

Auch die ausgebliebene Reaktion der betroffenen Person auf die E-Mail konnte nicht als eindeutig bestätigende Handlung ausgelegt werden. Stillschweigen stellt keine eindeutig bestätigende Handlung dar. Das ergibt sich bereits aus dem Willen des Gesetzgebers zur Daten-

schutz-Grundverordnung. In Erwägungsgrund 32 der DSGVO wird ein Stillschweigen als bestätigende Handlung explizit ausgeschlossen. Zur Auslegung des KDG können die Erwägungsgründe der DSGVO auch herangezogen werden, da das KDG gemäß Art. 91 Abs. 1 DSGVO mit dieser in Einklang stehen muss.

Ob eine Ausnahme vom Schriftformerfordernis gemäß § 8 Abs. 2 KDG vorliegt, brauchte im vorliegenden Fall nicht entschieden zu werden, da bereits die Voraussetzungen für eine wirksame Einwilligung nicht vorlagen.

2.2.5 Hacker-Angriffe/Phishing-Mails

Datenschutz-Vorfälle durch Phishing-Angriffe auf E-Mail-Postfächer sind ein stetiger Teil der Arbeit des Katholischen Datenschutzzentrums.

Besonders ärgerlich sind jedoch Fälle wie aus diesem Berichtsjahr, bei dem der private E-Mail-Account einer Mitarbeitenden gehackt wurde. Dieser Account beinhaltete entgegen den gesetzlichen Vorgaben des § 20 KDG-DVO (Durchführungsverordnung zum KDG) auch dienstliche E-Mails mit Inhalten der Datenschutzklasse III gemäß § 13 KDG-DVO. Neben dem Verstoß gegen das Verbot der Nutzung privater IT zu dienstlichen Zwecken wurde im Rahmen dieses Vorfalls zum einen die Meldefrist nicht eingehalten, da die Inhaberin des E-Mail-Accounts den Vorfall zunächst herunterspielte. Zum anderen wurde auch das erforderliche Schutzniveau III nicht eingehalten. Die Übermittlung der personenbezogenen Daten durch die Weiterleitung der dienstlichen E-Mails auf den privaten E-Mail-Account erfolgte entgegen den Vorgaben aus § 13 Abs. 2 i. V. m. § 12 Abs. 2 lit. e) KDG-DVO unverschlüsselt.

Besonders problematisch an diesem Fall ist, dass dem Verantwortlichen durch die Nutzung privater IT zu dienstlichen Zwecken ein Großteil seiner Einflussmöglichkeiten genommen wird, für eine sichere Verarbeitung der personenbezogenen Daten zu sorgen. Auch wird es ihm erschwert, nach einer erfolgten Datenschutzverletzung den Vorgang umfassend aufzuklären und entsprechende Abhilfemaßnahmen zu ergreifen.

Auch Dienstleister waren von Hacker-Angriffen betroffen. So wurde etwa ein Druck- und Logistikdienstleister gehackt und es wurden die auf dem Server liegenden Daten verschlüsselt. Ob ein Datenabfluss erfolgte, konnte in diesem Fall nicht mit Sicherheit ausgeschlossen werden. Der in unserem Zuständigkeitsbereich befindliche Verantwortliche war von diesem Vorfall insofern betroffen, als dass Lohn- und Gehaltsabrechnungen, welche durch den Dienstleister ausgedruckt und postalisch versandt werden sollten, betroffen waren. Zugangspunkt für den Angriff war eine E-Mail mit kompromittiertem Anhang, welcher in einem bereits stattfindenden E-Mail-Verkehr versteckt wurde. Dies macht ein Erkennen für den Anwender besonders schwer.

Bei einem anderen Vorfall haben Angreifer den Terminalserver eines Caritasverbands verschlüsselt und dann versucht den Verband zu erpressen. Betroffen waren u. a. Gesundheitsdaten von Patienten und Klienten sowie personenbezogene Daten von Mitarbeitenden. Auch

hier konnte weder die Veröffentlichung noch der Abfluss von Daten mit Sicherheit festgestellt, aber auch nicht ausgeschlossen werden. Ebenso konnte nicht mehr bestimmt werden, wie der Zugriff auf den Server erfolgte. Naheliegend ist auch in diesem Fall, dass die Ransomware durch eine E-Mail mit einem manipulierten Anhang in die Einrichtung gelangte.

Als Sofort-Maßnahme durch den Verantwortlichen erfolgte eine physische Trennung der Systeme, eine Kontaktaufnahme zur Versicherung und die Einschaltung eines IT-Forensikers. Zudem wurde eine fristgerechte Meldung gemäß § 33 KDG an das KDSZ als zuständige Datenschutzaufsicht abgegeben und Strafanzeige bei der Polizei gestellt.

Zeitnah wurde eine Fachfirma beauftragt, um die Arbeitsfähigkeit des Verbandes wiederherzustellen. Auf Entscheidung des Vorstandes wurde das gesamte System „zurückgesetzt", d. h., es wurden z. B. alle Server und Rechner komplett neu installiert, Passwörter neu vergeben und die Daten in Gänze bereinigt, bevor sie wieder nutzbar waren. Die wesentlichen Maßnahmen erfolgten alle im Vier-Augen-Prinzip und wurden dokumentiert. Zeitgleich wurde mit der schriftlichen Benachrichtigung der betroffenen Personen begonnen.

Darüber hinaus wurden zahlreiche weitere Maßnahmen ergriffen, um das System für die Zukunft sicherer zu gestalten (vgl. dazu auch Beitrag „Ransomware-Angriffe auf Dienstleister")[29].

2.2.6 Unverschlüsselte E-Mail

Eine größere Anzahl der Meldungen von Datenschutzverletzungen im Berichtzeitraum drehen sich um Themenkomplexe rund um E-Mails. Datenschutzverletzungen bezüglich E-Mails sind auch in der Vergangenheit besonders häufig aufgetreten beziehungsweise gemeldet worden.[30] Innerhalb dieses Problemkomplexes kommt es oft zum unverschlüsselten E-Mail-Versand besonders schützenswerter personenbezogener Daten. Am häufigsten sind Gesundheitsdaten gem. § 4 Nr. 2 und Nr. 17 KDG betroffen.

Verantwortliche sind nach § 26 Abs. 1 KDG 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. Dort wird auch die Verschlüsselung als geeignete technische Maßnahme aufgeführt. 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 Versand personenbezogener Daten per E-Mail.

[29] Siehe hierzu Abschnitt 2.2.1 dieses Jahresberichts.
[30] Siehe z. B. Abschnitt 3.7.3 im Jahresbericht 2020 zu dem Thema offener E-Mail-Verteiler.

Nach § 12 Abs. 2 lit. e) KDG-DVO hat die Übermittlung personenbezogener Daten (des Schutzniveaus II) außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) grundsätzlich verschlüsselt zu erfolgen. Das Verschlüsselungsverfahren ist dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen auszuwählen.[31] Die wohl verbreitetsten Public-Key-Infrastruktur (PKI)[32] Verschlüsselungsmethoden für E-Mails sind die S/MIME- und PGP-Standards.[33] Die Verschlüsselung von E-Mails garantiert die Einhaltung der Schutzniveaus II und III gem. §§ 12 und 13 KDG-DVO. Das umfasst z. B. auch den Versand von Gesundheitsdaten.

Der Versand personenbezogener Daten ohne Verschlüsselung oder vergleichbare gleichwertige Schutzmaßnahmen stellt eine Verletzung des in § 7 Abs. 1 lit. f) und § 26 Abs. 1 lit. b) KDG normierten Schutzziels der Vertraulichkeit und mithin eine meldepflichtige Datenschutzverletzung dar. Das Schutzziel Vertraulichkeit gewährleistet den Schutz vor unberechtigter und unbefugter Verarbeitung.

Die Ursachen für die gemeldeten Datenschutzverletzungen sind zahlreich. Wiederholt kam es zum Versand unverschlüsselter E-Mails, weil Mitarbeitende katholischer Einrichtungen das Schutzniveau der personenbezogenen Daten zunächst falsch eingeschätzt hatten oder schlicht nicht (ausreichend) für die Problematik sensibilisiert wurden. Nicht selten kommt es auch zum rein versehentlichen unverschlüsselten Versand, obwohl die Problematik bekannt ist. Denkbar ist auch, dass eine Verschlüsselung von E-Mails als zu umständlich betrachtet wird. An dieser Stelle sei daher darauf hingewiesen, dass die Möglichkeit zu einer Einwilligung in unverschlüsselte (E-Mail) Kommunikation grundsätzlich besteht.[34]

2.2.7 Verlust von personenbezogenen Daten

Der Verlust von personenbezogenen Daten stellt eine der im Berichtszeitraum am häufigsten gemeldeten Datenschutzverletzungen dar. Dabei ist der Verlust ein Sammelbegriff für Fallkonstellationen vom Einbruchsdiebstahl und dem schlichten Verlieren von Papierakten bis hin zur Ransomware-Attacke.

Einbruchsdiebstähle sind eine der häufigsten Ursachen für den Verlust von personenbezogenen Daten. Einbrecher stehlen oftmals Laptops, Digitalkameras oder ähnliche Endgeräte aus den Einrichtungen. Besonders häufig sind davon Kindertageseinrichtungen betroffen.[35] Der Verlust durch Diebstahl beschäftigt das Katholische Datenschutzzentrum aber auch in vielfältigen anderen Konstellationen. Es wurde zum Beispiel der Diebstahl eines Fahrrads samt Satteltasche gemeldet, in der sich ein Arbeitsvertrag eines neuen Mitarbeiters befunden hat.

---

[31] Sollte eine Verschlüsselung nicht möglich sein, sind die in der E-Mail enthaltenen sensiblen Daten durch Passwörter zu schützen.

[32] Der Begriff PKI bezeichnet in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

[33] Das Katholische Datenschutzzentrum verwendet z. B. den S/MIME-Standard.

[34] Zur Thematik der Einwilligung in schlechtere TOM siehe Abschnitt 2.11 im Jahresbericht 2021.

[35] Eine genauere Darstellung siehe Abschnitt 2.6.2 im Jahresbericht 2021.

Es wurden auch Vorfälle gemeldet, in denen z. B Papieraktenordner oder Arbeitstaschen in öffentlichen Verkehrsmitteln oder an öffentlich zugänglichen Plätzen vergessen wurden. In einem Fall kam es sogar zu einem Verlust einer Patientenakte während des Transports des Patienten in eine andere Einrichtung.

Bei Ransomware-Attacken werden Daten z. B. auf Servern und Computern meist durch Trojaner verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Erfolgt die Zahlung des Lösegeldes nicht, wird oftmals mit der Veröffentlichung beziehungsweise dem Verkauf der Daten im Internet gedroht. Selten handelt es sich um gezielte Angriffe auf Einrichtungen. Dem KDSZ wurden solche Attacken sowohl auf kleine Einrichtungen als auch überregionale Verbände gemeldet. Dabei ist ein Anstieg der Häufigkeit dieser Attacken im Berichtszeitraum zu verzeichnen.[36]

Durch den Verlust personenbezogener Daten, unabhängig von ihrer Speicherung, werden potenziell die Schutzziele Verfügbarkeit und Vertraulichkeit verletzt. Das Schutzziel der Verfügbarkeit gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck der Verarbeitung, solange dieser besteht. Die Verfügbarkeit ist auch wichtig zur Erfüllung aller Betroffenenrechte, etwa der Informations- und Auskunftspflichten nach §§ 15–17 KDG. Die Verfügbarkeit ist zum Beispiel verletzt, wenn der Verlust der personenbezogenen Daten endgültig ist beziehungsweise diese nicht wiederhergestellt werden können. Das Schutzziel der Vertraulichkeit schützt die personenbezogenen Daten des Betroffenen vor unberechtigter Verarbeitung, insbesondere unberechtigter Einsichtnahme Dritter, und unterstützt damit den Grundsatz der Zweckbindung jeder Verarbeitung personenbezogener Daten. Dieses Schutzziel ist zum Beispiel verletzt, wenn ein gestohlener Laptop nicht mit einer Festplattenverschlüsselung versehen wurde.

Hinweis für kirchliche Einrichtungen

In den zu Beginn geschilderten Fallkonstellationen können durch geeignete technische und organisatorische Maßnahmen meldepflichtige Datenschutzverletzungen vermieden werden. Die Umstellung auf eine papierlose Verwaltung in Kombination mit verschlüsselten Endgeräten sind einfache Beispiele. Bezüglich Ransomware-Attacken können auch schlicht Sensibilisierungsmaßnahmen der Mitarbeitenden die Risiken hinsichtlich von Infektionen durch infizierte E-Mails stark vermindern.

2.3 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.

[36] Für eine detailliere Darstellung dieser Problematik siehe den Abschnitt 2.2.1 in diesem Jahresbericht.

Im Berichtszeitraum haben wieder viele Personen von dieser Möglichkeit Gebrauch gemacht. Neben Themen, die immer wieder auftauchen und schon in einem der letzten Jahresberichte oder in diesem Bericht an anderen Stellen erwähnt sind, werden nachfolgend exemplarisch einige Sachverhalte aufgegriffen.

2.3.1 Betroffenenrecht auf Auskunft

Im Berichtsjahr war das Betroffenenrecht auf Auskunft nach § 17 KDG erneut einer der häufigsten Beschwerdegegenstände, aber auch Anfragen betrafen dieses Thema.

Es fällt in der aufsichtsrechtlichen Praxis weiterhin auf, dass die Verantwortlichen mit dem Recht auf Auskunft und vor allem mit den damit verbundenen gesetzlichen Anforderungen überfordert sind und daher die Auskunftsersuchen oftmals unzureichend und verspätetet – teils auch nur nach Einschreiten der Aufsicht – beantwortet werden. Dies stellt einen groben Verstoß gegen die Datenschutz-Grundverordnung und im kirchlichen Bereich gegen das KDG dar. Sollte die Stärkung der Betroffenenrechte doch gerade zum Ziel haben, die Verarbeitungen personenbezogener Daten zu schützen und transparenter zu gestalten, gefährden nicht oder nicht gesetzeskonform beantwortete Auskunftsanfragen dieses Ziel.

Häufige Stolpersteine

1. Das Recht auf Auskunft steht grundsätzlich jeder betroffenen Person zu.

2. Die Auskunft ist unverzüglich, spätestens einen Monat nach Antragseingang zu gewähren. Dabei ist die Verlängerungsoption (Frist von drei Monaten) des § 14 Abs. 3 S. 2 KDG nur in den dort festgelegten Ausnahmefällen möglich.

3. Nichtbeauskunftete Schriftstücke/Informationen über personenbezogene Daten können nur innerhalb der gesetzlich vorgegebenen Bedingungen einbehalten werden.

Zu 1.
Jede natürliche Person hat das Recht, vom Verantwortlichen Auskunft über ihre der Verarbeitung unterliegenden personenbezogenen Daten zu erhalten, einschließlich einer Kopie dieser Daten. Hierbei ist es keine Voraussetzung, dass die betroffene Person einen ausformulierten Antrag nach § 17 Abs. 1 und 3 KDG stellt, sondern es ist nur wichtig, dass aus der Anfrage hervorgeht, dass die betroffene Person ihr Recht auf Auskunft geltend macht. Eine Nichtbeantwortung, weil nicht auf § 17 KDG Bezug genommen wurde, verstößt gegen datenschutzrechtliche Bestimmungen und untergräbt die Transparenz der Verarbeitung und damit auch das Recht auf Auskunft.

Zu 2.
In den allermeisten Fällen wird der Verantwortliche zwar nicht in der Lage sein, die Auskunft unverzüglich zu erfüllen, jedoch ist er verpflichtet, dies innerhalb eines Monats ab Eingang des Antrags zu gewährleis-

ten. Dies bedeutet, dass gerade bei umfangreicheren Verarbeitungen innerhalb der jeweiligen Organisation schon vorab genau festgelegt sein sollte, welche Schritte nach Eingang eines Antrags auf Auskunft nach § 17 KDG erledigt werden müssen, damit nach spätestens einem Monat die Auskunft erteilt werden kann. Zwar erlaubt das KDG in Ausnahmefällen die Monatsfrist auf drei Monate zu verlängern, wenn der Anfragende innerhalb der Monatsfrist über diesen Umstand und die Gründe für die Verzögerung informiert wird, jedoch ist dies nur unter den dort festgelegten Voraussetzungen möglich. Gerade ein wiederholtes Berufen auf diese Ausnahmeregelungen in gleichgelagerten Auskunftsanfragen zeigt eher, dass der Verantwortliche keinen (angemessenen) Prozess zur fristgerechten Beantwortung implementiert hat.

Zu 3.
Die Auskunftserteilung ist generell nur gesetzeskonform, wenn sie auch umfänglich und vollständig erfolgt. Beruft sich der Verantwortliche darauf, dass er teilweise nicht beauskunftet, weil zum Beispiel Rechte Dritter gefährdet werden könnten, hat er diesen Umstand darzulegen oder wenn möglich geschwärzte Kopien zur Verfügung zu stellen.

2.3.2 Weitergabe von Daten an Dritte ohne Einwilligung

Hinsichtlich der unbefugten Weitergabe von personenbezogenen Daten gingen im Berichtsjahr zahlreiche andere Beschwerden von Betroffenen ein.

In einem Fall wurde ohne Einwilligung der betroffenen Person eine Rund-E-Mail an über 100 Mitarbeitende versandt, in welcher die Tatsache, dass die betroffene Person gekündigt hatte und deren neue Arbeitsstelle, offengelegt wurden. Gemäß § 6 Abs. 1 lit. g) KDG ist eine Verarbeitung u. a. zur Wahrung der berechtigten Interessen des Verantwortlichen möglich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Vorliegend konnte sich der Beschwerdegegner (Verantwortliche) auf sein berechtigtes Interesse berufen, dass die Information, dass die betroffene Person die Einrichtung verlassen werde, für die dienstliche Organisation erforderlich war. Auch überwogen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht. Dass eine seitens der betroffenen Person gewünschte Absprache bezüglich der Art und Weise einer Bekanntmachung nicht erfolgt ist, wog im Vergleich zum Interesse des Verantwortlichen, einen möglichst reibungslosen Arbeitsübergang zu schaffen, nicht besonders schwer.

Anders stellte es sich hinsichtlich der übrigen offengelegten Informationen dar, für welche keine entsprechende Rechtsgrundlage gegeben war und welche daher rechtswidrig war.

In einem anderen Fall wurde die Tatsache einer Abmahnung gegenüber anderen Mitarbeitenden offengelegt, ohne dass diese zur Kenntnisnahme berechtigt gewesen wären. Dies geschah zwar in der Absicht, das Betriebsklima zu fördern, da vonseiten der Mitarbeitenden ein Handeln des Dienstgebers gegenüber der betroffenen Person gewünscht

war, jedoch entbehrte die Offenlegung jeglicher Rechtsgrundlage und war mithin rechtswidrig.

Problematisch wird es zudem insbesondere, wenn Datenübermittlungen erfolgen, ohne dass sich vorab Gedanken zu der Rechtsgrundlage gemacht werden. Im Rahmen einer Beschwerde stellte sich heraus, dass vonseiten des Verantwortlichen eine Einwilligung zur Übersendung eines ärztlichen Abschlussberichts, an den weiter behandelnden Arzt bei der betroffenen Person eingefordert wurde. Diese Einwilligung wurde in der Folge jedoch nicht erteilt. Der Verantwortliche verteidigte sich damit, dass eine Einwilligungsabfrage nicht dokumentiert worden sei, und präsentierte eine seiner Ansicht nach einschlägige Rechtsgrundlage.

Unabhängig davon, dass die Rechtsgrundlage im in Rede stehenden Fall äußerst fraglich war, war hier problematisch, dass nach dem Versuch der Einholung einer Einwilligung die Datenverarbeitung auf eine alternative, nachgeschobene Rechtsgrundlage gestützt werden sollte.

Indem die Daten verarbeitende Stelle bei der betroffenen Person eine Einwilligung einholt, signalisiert sie dieser, dass es für die Zulässigkeit einer Datenverarbeitung gerade auf das Einverständnis ankommen soll. Dann aber wäre es ein in sich widersprüchliches Verhalten, wie vorliegend im Falle der Verweigerung der Einwilligung, doch wieder auf einen alternativen Zulässigkeitstatbestand zurückzugreifen. Der betroffenen Person darf keine Entscheidungsmacht suggeriert werden, die so tatsächlich gar nicht besteht. In Einzelfällen kann eine alternative Rechtsgrundlage allenfalls dann eine Legitimationswirkung entfalten, wenn die betroffene Person bei Einholung der Einwilligung auf diesen weiteren Legitimationstatbestand hingewiesen wird.

Es gingen jedoch auch unbegründete Beschwerden beim Katholischen Datenschutzzentrum ein. Ein Beschwerdeführer wandte sich gegen die Übermittlung seiner personenbezogenen Daten an einen ambulanten Pflegedienst zum Zwecke der Nachsorge. Hierbei ließ er außer Acht, dass er im Rahmen einer wirksam erteilten Einwilligung ebenfalls in die Datenübermittlung zum Zwecke des Entlassungsmanagements eingewilligt hatte, wovon u. a. auch die Organisation einer Anschlussversorgung umfasst war. Dem Verantwortlichen kam es insofern zugute, dass die Einwilligung ordnungsgemäß dokumentiert war und vorgelegt werden konnte.

2.4 Prüfungen

Auch in diesem Berichtszeitraum gab es im Zuständigkeitsbereich des Katholischen Datenschutzzentrums Vor-Ort-Prüfungen.

Nachdem die Durchführung von Vor-Ort-Terminen pandemiebedingt für einige Zeit zurückgestellt werden musste, lief der Prüfbetrieb im Jahr 2022 wieder in gewohnten Bahnen. Es wurde sowohl anlasslos als auch anlassbezogen geprüft.

2.4.1 Prüfung einer Kindertageseinrichtung

Ausgangspunkt einer anlassbezogenen Prüfung war, dass das Katholische Datenschutzzentrum im Jahr 2019 eine Querschnittsprüfung von Kindertageseinrichtungen gestartet hatte.[37] Zunächst wurde mit einem Schreiben an alle Kindertageseinrichtungen im hiesigen Zuständigkeitsbereich auf die Problematik gestohlener Laptops, Fotoapparate und mobiler Datenträger (z. B. USB-Sticks oder SD-Karten) hingewiesen und die Querschnittsprüfung angekündigt. Anlass der Querschnittsprüfung war, dass sich in den meisten Fällen herausstellte, dass die auf den Geräten vorhandenen personenbezogenen Daten (z. B. Bildungsdokumentationen, Berichte an Jugendämter und Fotos) ohne oder ohne ausreichenden Schutz gespeichert waren.

In der Folge wurde die Prüfung mit einer Stichprobe aus den Kindertageseinrichtungen aller fünf nordrhein-westfälischen (Erz-)Diözesen durchgeführt. Wobei im ersten Teil online ein Fragebogen ausgefüllt werden musste. Dieser Fragebogen wurde von der in diesem Fall geprüften Kindertagesstätte zunächst noch ausgefüllt. Auf die folgenden Rückfragen wurde jedoch nicht mehr reagiert. Aus diesem Grund war eine Überprüfung der Gegebenheiten vor Ort erforderlich.

Die Prüfung wurde grundsätzlich prozessbezogen aufgebaut und orientierte sich am Verlauf der Betreuung der Kinder. Im Fokus stand somit insbesondere der Umgang mit den personenbezogenen Daten der Kinder von deren Eintritt an, über die Anwesenheit, bis hin zum Ausscheiden aus dem Kindergarten. In diesem Rahmen wurden vereinzelt auch weitere Aspekte aus anderen Feldern herausgegriffen.

„... sollte den Verantwortlichen bewusst sein, dass sie ... zur Unterstützung und Zusammenarbeit mit der Datenschutzaufsicht verpflichtet sind."

Im Ergebnis konnte festgestellt werden, dass das Datenschutzniveau in der Einrichtung besser war, als die Zusammenarbeit im Rahmen der Querschnittsprüfung zunächst befürchten ließ. Diesbezüglich sollte den Verantwortlichen bewusst sein, dass sie gemäß § 32 und § 44 Abs. 2 KDG zur Unterstützung und Zusammenarbeit mit der Datenschutzaufsicht verpflichtet sind.

Bei der o. g. Prüfung stellte sich insbesondere heraus, dass der Datenschutz in der täglichen Arbeit – bis auf kleinere Mängel – gut gelebt wird. Auf der anderen Seite zeigte sich aber auch, dass die Dokumentation zur Erfüllung der Rechenschaftspflichten aus § 7 Abs. 2 und § 26 Abs. 1 S. 1 KDG häufig unvollständig oder nicht vorhanden war.

2.4.2 Prüfung einer Kirchengemeinde

Das Katholische Datenschutzzentrum führt auch anlasslose Prüfungen durch. Bei den anlasslosen Prüfungen wird durch ein Zufallsprinzip eine Einrichtung beziehungsweise Gemeinde ausgewählt, deren Prozesse nicht vollständig, sondern themenbezogen datenschutzrechtlich vom KDSZ überprüft werden.

Die Prüfungen werden auch hier grundsätzlich prozessbezogen aufgebaut. In einem Fall orientierte sich die Prüfung an verschiedenen

[37] Siehe hierzu Abschnitt 3.11.2 des Jahresberichts 2019, Abschnitt 3.5 des Jahresberichts 2020 und Abschnitt 2.4.1 des Jahresberichts 2021.

Bereichen der Jugendarbeit der Gemeinde. Im Fokus stand insbesondere der Umgang mit den personenbezogenen Daten der Minderjährigen von deren Eintritt in die Gemeinde, ihre Beteiligung am Leben in der Gemeinde, bis hin zum Ausscheiden aus der Gemeinde. In diesem Rahmen wurden vereinzelt auch weitere Aspekte herausgegriffen.

Die Zusammenarbeit mit der Gemeinde im oben bezeichneten Fall gestaltete sich sehr produktiv. Angeforderte Dokumente wurden stets fristgerecht eingereicht und auf Nachfragen prompt reagiert. Im Rahmen der Prüfung traten keine größeren Mängel hervor. Die Prüfung läuft noch und wird 2023 abgeschlossen werden.

2.5 Einrichtungsbezogene Impfpflicht

Im Rahmen einer Änderung des Infektionsschutzgesetzes (IfSG) vom 12.12.2021 wurde u. a. der § 20a IfSG a. F. (alte Fassung) eingeführt. Dieser beinhaltete die sogenannte „Einrichtungsbezogene Impfpflicht", wonach die dort genannten Personen, die etwa in Krankenhäusern tätig sind, ab dem 15.03.2022 entweder geimpft oder genesen sein mussten.

In der Folge kam es insbesondere zu Anfragen, welche personenbezogenen Daten auf dieser Grundlage vom Arbeitgeber erhoben und gespeichert werden durften.

Der geschaffene § 20a IfSG a. F. schrieb in seinem Absatz 2 insofern lediglich eine Pflicht für die in Absatz 1 Satz 1 genannten Personen vor, „der Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens bis zum Ablauf des 15. März 2022" einen der genannten Nachweise vorzulegen. Nur für den Fall, dass dies nicht geschieht oder wenn Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises bestehen, hatte die Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens unverzüglich das Gesundheitsamt, darüber zu benachrichtigen und dem Gesundheitsamt personenbezogene Daten zu übermitteln.

Eine grundsätzliche Notwendigkeit oder Pflicht die vorgelegten Nachweise in Kopie vorzuhalten, zu speichern oder an das Gesundheitsamt weiterzuleiten, bestand demnach nicht.

Auch aus § 20a Abs. 5 IfSG a. F., wonach die in Abs. 1 Satz 1 genannten Personen dem zuständigen Gesundheitsamt auf Anforderung einen entsprechenden Nachweis vorlegen mussten, ergab sich keine Pflicht zur Übermittlung derselben durch die Leitung der Einrichtung.

Nach dem Grundsatz der Datenminimierung aus § 7 Abs. 1 lit. c) KDG müssen die personenbezogenen Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Aus Sicht des Katholischen Datenschutzzentrums war es ausreichend einen Vermerk über den Impf-/Genesungsstatus / das ärztliche Zeugnis (über eine medizinische Kontraindikation Impfung) und ggf. das Gültigkeitsdatum anzufertigen.

Anders als das EU-Zertifikat lief der Impfstatus selbst nicht ab. Ein Vermerk der verwendeten Impfstoffe und den Zeitpunkt dieser Imp-

fungen war zum damaligen Zeitpunkt demnach nicht erforderlich. Insofern genügte die Überprüfung, ob eine vollständige Impfung nach der jeweiligen Rechtslage vorlag und ein Vermerk, dass dieser Nachweis erbracht wurde.

Neben der Datenminimierung waren die übrigen datenschutzrechtlichen Schutzmaßnahmen in Bezug auf die Vermerke selbstverständlich ebenfalls einzuhalten.

Mit der Änderung des IfSG vom 01.01.2023 ist der § 20a IfSG a. F. weggefallen. Datenschutzrechtlich endet das Recht auf Aufbewahrung mit dem endgültigen Wegfall des Zweckes der Erhebung und dem Zeitpunkt, ab dem keine berechtigten Interessen des Verantwortlichen auf die Aufbewahrung mehr bestehen. In diesem Zusammenhang erhobene personenbezogene Daten waren in der Folge demnach zu löschen.

2.6 Datenschutzaufsicht zum Anfassen – das Katholische Datenschutzzentrum auf dem Katholikentag 2022 in Stuttgart

Unter dem Motto „Leben teilen" fand vom 25. bis zum 29.05.2022 der 102. Katholikentag in Stuttgart statt. Auf der Kirchenmeile, in der Nähe der Bistümer und Verbände, waren die fünf deutschen Datenschutzaufsichten der katholischen Kirche vertreten. In einem gemeinsamen Zelt sind Mitarbeitende der Datenschutzaufsichten vor Ort gewesen, um Fragen zu beantworten oder Auskunft und Hinweise zum kirchlichen Datenschutz in der katholischen Kirche zu geben. Als Sprecher der Konferenz der Diözesandatenschutzbeauftragten (DDSB) war der Leiter des Katholischen Datenschutzzentrums ebenso anwesend wie Referenten und Sachbearbeiter aus den Bereichen IT und Recht und weitere Diözesandatenschutzbeauftragte. Zu den Besuchern im Zelt zählten nicht nur Politiker und kirchliche Amtsträger. Auch Mitarbeitende der Kirche sowie Besucher des Katholikentages kamen mit Fragen, Hinweisen und Anregungen zum „Datenschutzzelt". Viele konkrete Fragen zum Datenschutz und zur Arbeit der Datenschutzaufsichten konnten von den Mitarbeitenden in Stuttgart beantwortet werden. Der Katholikentag in Stuttgart war eine gelungene Veranstaltung, auf der durch die Teilnahme der Datenschutzaufsichten der Datenschutz in der katholischen Kirche Präsenz gezeigt hat.

2.7 Digitalisierung in Schulen

Die Notwendigkeit des Einsatzes alternativer Lerntechniken und der dazu erforderlichen Software wurde auch durch die verschiedenen Formen des Distanzunterrichtes in den Jahren 2020 und 2021 deutlich. Gerade durch den dringenden Bedarf der Schulen, digitalen Unterricht zu ermöglichen und die damit verbundenen Unterrichtsstunden per Videokonferenz abzuhalten, sind einige Schulen auf Produkte ausgewichen, die nach dem Urteil des Europäischen Gerichtshof in der Sache C-311/18 vom 16.07.2020 (sog. Schrems-II-Entscheidung) aufgrund eines nicht zu unterbindenden Transfers personenbezogener Daten in ein Drittland, datenschutzrechtlich bedenklich sind. Die Landesdaten-

schutzbeauftragten verfolgten hier durchaus unterschiedliche Ansätze, inwiefern beziehungsweise wie lange man dies als Übergangslösung für die Nutzung dieser Software in Schulen gelten lassen kann, da das Urteil des EuGH in dieser Rechtssache eindeutige Hinweise gegeben hat, die es zu beachten gilt.

Auch die zahlreichen bischöflichen Schulen in NRW sind größtenteils dem Digitalisierungsvorhaben gefolgt und setzen auch nach der Notwendigkeit des Distanzunterrichtes weiterhin Software zum digitalen Lernen ein.

Datenschutzrechtlich ist der Einsatz des Großteils dieser Softwarelösungen kritisch zu beurteilen, da nach dem EuGH-Urteil vom 16.07.2020 feststeht, dass zusätzlich zu den Standardvertragsklauseln geeignete Maßnahmen getroffen werden müssen, um die Drittlandsübermittlung datenschutzkonform gestalten zu können. Diese zusätzlichen Maßnahmen stellen die Verantwortlichen vor eine schwierige Aufgabe, da nicht eindeutig feststeht, ob und wie diese Maßnahmen überhaupt zu einem datenschutzkonformen Verarbeiten der Daten führen können.

Um diese Probleme der Drittlandsübermittlung abzumildern oder zu beseitigen, wurde teilweise durch Einschaltung eines deutschen beziehungsweise europäischen Dienstleisters versucht, eine datenschutzkonforme Lösung zu finden. Einen dieser Lösungsansätze hat sich das KDSZ zusammen mit dem betreffenden Bistum näher angeschaut.

In der kirchlichen Einrichtung sollte ein bekanntes Office-Produkt in der Cloud-Variante mit einem zwischengeschalteten Dienstleister eingesetzt werden, wobei der Dienstleister zur Verwaltung der Geräte wiederum eine Software einsetzt, die eine (weitere) Drittlandsübermittlung beinhaltet.

Da es sich bei dem betrachteten Projekt um eines im schulischen Bereich handelt, wurde versucht, die Anzahl der personenbezogenen Daten durch die organisatorische Vorgabe zu reduzieren, dass bei der Verwendung des Office-Produktes keine personenbezogene Daten von Personen aus dem Schulleben, von Eltern oder anderen Verwandten und Freunden in den Dokumenten genutzt werden dürften. Außerdem sollten die Nutzerdaten (Anmeldename) aus einem Pseudonym bestehen, sodass die Kenntnis, wer sich mit dem Pseudonym angemeldet hat, für den Office-Anbieter nicht automatisch auf eine bestimmbare Person verweist.

Auch mit diesen Schutzmaßnahmen bleibt die Schwierigkeit, dass diese Maßnahme nicht mehr wirksam ist, sobald weitere Dienste, die mit dem Office-Produkt in Verbindung stehen oder die Anmeldedienste des Anbieters des Office-Produktes verwenden, mit der richtigen E-Mail-Adresse des Anwenders verwendet werden. Über die Telemetriedaten der Geräte und der Software kann dann eine Zusammenführung der Daten und deren De-Pseudonymisierung möglich sein. Auch das Speichern von Dokumenten mit personenbezogenen Inhalten würde die Pseudonymisierung aufheben.

Nach Herstellerangaben werden die erhobenen Telemetriedaten zwar pseudonymisiert, jedoch liegt die Kontrolle dessen beim Hersteller. Dieser kann jederzeit die Pseudonymisierung aufheben.

Die als weitere Schutzmaßnahme vom Hersteller des Office-Produktes angebotene „Hold Your Own Key" Option bietet eine Verschlüsselung der Daten mit einem kundeneigenen Schlüssel an. Die Verschlüsselung der in der Cloud gespeicherten Daten ist aber nur dann auch gegenüber dem Office-Anbieter wirksam, wenn nicht die vom Anbieter verwendeten Verschlüsselungsmethoden verwendet werden. Der Hersteller behält sich, trotz der „Hold Your Own Key" Funktion vor, einen Master-Key zu behalten, falls der Kunde seinen Schlüssel nicht mehr nutzen kann.

Die im Projekt vorgeschlagenen technischen und organisatorischen Maßnahmen sind in der Umsetzung und vor allem in der konsequenten Einhaltung in der Praxis anspruchsvoll.

Im April 2022 veröffentlichte der Landesbeauftragte für Datenschutz und die Informationsfreiheit Baden-Württemberg eine Pressemitteilung[38] zu diesem Thema, in der er ankündigte, dass er von den Schulen erwarte, zum neuen Schuljahr (Sommer 2022) Alternativen zum Cloud-Dienst MS 365 anzubieten. Dieser Forderung war vorausgegangen, dass seine Behörde zusammen mit dem Kultusministerium nach einer datenschutzkonformen Möglichkeit zur Nutzung des Cloud-Dienstes gesucht hat und dies nicht gelungen sei. Daher verwies der LfD explizit auf andere digitale Lern-Tools, welche vom Ministerium kostenlos zur Verfügung gestellt würden. Sollten einzelne Schulen sich dort trotzdem für den Einsatz von MS 365 entscheiden, haben diese ihre Rechenschaftspflicht zu erfüllen und nachzuweisen, dass der Einsatz datenschutzkonform erfolgen kann.

Auch das KDSZ stand im Berichtszeitraum mit unterschiedlichen Schulen beziehungsweise Schulträgern im Austausch zu diesem schwierigen Thema. Eine abschließende Bewertung konnte jedoch in 2022 nicht ergehen.

2.8 Abmahnungen Google Webfonts

Im Sommer/Herbst 2022 häuften sich die Meldungen zu Abmahnungen aufgrund der nicht datenschutzkonformen Einbindung von Google Webfonts (Schriftarten) auf Webseiten. Die Abmahnungen betrafen kirchliche und staatliche Einrichtungen, Unternehmen, aber auch Vereine und andere gemeinnützige Organisationen.

Google Webfonts dürfen kostenlos auf Webseiten eingesetzt werden. Google bietet in seiner Bibliothek dazu über 1.400 Schriften als Open Source unter der Open Fonts License (OFL) für die Benutzung an.

Wie kam es zu den Abmahnungen? Das Landgericht München I[39] hat einem Nutzer 100,00 Euro Schadenersatz zugesprochen, weil ein Web-

[38] Die Pressemitteilung ist abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/nutzung-von-ms-365-an-schulen/

[39] LG München I - Urteil vom 20.01.2022, Az. 3 O 17493/20.

seitenbetreiber Google Webfonts dynamisch von den Google Servern in seiner Webseite eingebunden hat. Beim Aufruf der Webseite wurde so die IP-Adresse des Nutzers an Google übermittelt, um die passende Schriftart zu laden und anzuzeigen. Der Nutzer wurde nicht informiert und es wurde keine Einwilligung eingeholt. Laut einem BGH-Urteil[40] vom 16.05.2017 stellt die dynamische IP-Adresse für den Anbieter von Online-Mediendiensten ein personenbezogenes Datum dar. Diese wird bei der Weitergabe an Google unerlaubt verarbeitet und wird in der Abmahnung als Verletzung des allgemeinen Persönlichkeitsrechts dargestellt.

Unabhängig von der rechtlichen Bewertung im Einzelfall, ob ein im Wege der Abmahnung geltend gemachter Anspruch berechtigt ist, hat das Katholische Datenschutzzentrum den kirchlichen Stellen geraten, die Verwendung von Google Webfonts auf den eigenen Internetseiten zu prüfen.

Hinweis für kirchliche Einrichtungen

Alle Webseitenbetreiber sollten ihre Webseite daher überprüfen, ob Google Webfonts verwendet werden. Die Webfonts können dynamisch beim Aufruf der Webseite vom Google Server eingebunden werden oder alternativ können die Schriften lokal auf dem Webserver der Webseite abgelegt werden. Die lokale Einbindung verhindert die Übermittlung der IP-Adressen der Nutzer an Google. Google selbst stellt Hilfsmittel für die lokale Einbindung der Webfonts zur Verfügung.

Dabei ist Google Webfonts aber nur ein Beispiel von vielen Diensten, die in einer Webseite eingebunden sein können und Daten an Dritte weitergeben. Es empfiehlt sich, die Webseite auf Tools und Dienste Dritter zu überprüfen. Übermitteln diese Tools Daten an Dritte, ist die Information der Nutzer sicherzustellen und ggf. eine Einwilligung vor der Verwendung einzuholen. Auf Webseiten wird die Einwilligung und die Information der Nutzer beispielsweise durch sogenannte Consent-Banner (oder auch Cookie-Banner) und die passenden Datenschutzhinweise realisiert.

„Es empfiehlt sich, die Webseite auf Tools und Dienste Dritter zu überprüfen."

[40] Bundesgerichtshof, Urteil vom 16.05.2017, Az. VI ZR 135/13.

2.9 Aktualisierung des Beschlusses zur Einwilligung in schlechtere TOM

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche in Deutschland hat ihren Beschluss von 2019 zur Einwilligung in schlechtere technische und organisatorische Maßnahmen (TOM) mit Beschluss vom 15.06.2022[41] aufgehoben und ihre Stellung zu dem Thema angepasst.[42] Die Änderung des Beschlusses erfolgte, nachdem die Datenschutzkonferenz ihren Beschluss zu dem Thema im November 2021 veröffentlichte.[43]

Der neu gefasste Beschluss der Diözesandatenschutzbeauftragten vertritt nunmehr den Standpunkt, dass Verantwortliche sicherstellen müssen, dass ein in jedem Fall entsprechendes Schutzniveau für personenbezogene Daten gewährleistet wird und auf Betroffenenseite in das Nichtanwenden von einzelnen technischen und organisatorischen Schutzmaßnahmen gemäß § 6 Abs. 1 lit. b) bzw. § 11 Abs. 2 lit. a) KDG auf informierte Weise eingewilligt werden kann. Diese Dispositionsbefugnis ist nur gegeben, 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 bringen würde.

2.10 Austausch zwischen altem und neuem Arbeitgeber bzw. Dienstgeber über wechselnde Mitarbeitende – nicht immer eine gute Idee

Auch bei Personalwechseln in kirchlichen Einrichtungen kommt es vor, dass der bisherige Dienstgeber sich mit dem neuen über die wechselnde Mitarbeiterin oder den Mitarbeiter austauscht. Dieses Vorgehen kann – je nach den Umständen des Einzelfalls – arbeitsrechtlich, aber auch datenschutzrechtlich problematisch sein, wie ein aktuelles Urteil des Landesarbeitsgerichts Rheinland-Pfalz im Berichtszeitraum beispielhaft zeigt.

Im Berichtsjahr war die Frage nach der Zulässigkeit des Austauschs von Informationen zwischen bisherigem und künftigem Arbeitgeber bezüglich einer Arbeitnehmerin Gegenstand einer Entscheidung des Landesarbeitsgerichts Rheinland-Pfalz[44]. Arbeitgeber haben aus ihrer Sicht häufig das Interesse, so viele Informationen wie möglich über ihre künftigen Mitarbeitenden zu erhalten. Von daher besteht für sie immer die Versuchung, von den bisherigen Arbeitgebern die gewünschten personenbezogenen Informationen in Erfahrung zu bringen.

---

[41] Der neue Beschluss aus 2022 kann auf der Internetseite des Katholischen Datenschutzzentrums im Bereich Infothek ⇨ Beschlüsse der Konferenz der Diözesandatenschutzbeauftragten abgerufen werden. Der Beschluss ist in diesem Bericht auch in Abschnitt 4.3.1 abgedruckt.

[42] Für eine detailliertere Darstellung des Themas und der verschiedenen Ansichten siehe Abschnitt 2.11 im Jahresbericht 2021.

[43] Der Beschluss der DSK ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

[44] LAG Rheinland-Pfalz, Urteil vom 5. Juli 2022, Az.: 6 Sa 54/22.

Im konkreten Fall hatte die frühere Arbeitgeberin und Beklagte der neuen Arbeitgeberin Informationen über die Klägerin mitgeteilt. Die Klägerin hatte daraufhin auf Unterlassung geklagt und das Begehren mit Äußerungen des Geschäftsführers der Beklagten gegenüber der neuen Arbeitgeberin der Klägerin begründet. Der Geschäftsführer der Beklagten hatte bei der neuen Arbeitgeberin der Klägerin angerufen und u. a. mitgeteilt, dass der Lebenslauf der Klägerin eine unwahre Angabe hinsichtlich ihrer Vorbeschäftigung enthalten habe, Fehlverhalten während des Beschäftigungsverhältnisses vorgekommen sei und dass sich aus seiner Sicht ein schwerwiegender Datenschutzverstoß ereignet habe

Die Klägerin hatte nach erfolglosem außergerichtlichen Antrag auf Abgabe einer Unterlassungserklärung im Hinblick auf die getätigten Äußerungen des Geschäftsführers Unterlassungsklage beim Arbeitsgericht Kaiserslautern erhoben. Das mit der Klage verfolgte Unterlassungsbegehren bezog sich unter anderem darauf, dass die Beklagte nicht auf potenzielle künftige Arbeitgeber der Klägerin zugehen und nicht die in der Klageschrift näher aufgelistete Behauptungen aufstellen dürfe.

Das erstinstanzliche Arbeitsgericht hat die Beklagte in seinem Urteil vom 25.01.2022 zu den im Urteilstenor aufgeführten Unterlassungen verurteilt. Das Bestehen des Unterlassungsanspruchs hat das erstinstanzliche Gericht mit § 1004 Abs. 1 i. V. m. § 823 Abs. 1 BGB i. V. m. dem von Artt. 1 und 2 GG garantierten Persönlichkeitsrecht begründet. Zwar sei der Arbeitgeber nicht grundsätzlich daran gehindert, Auskünfte über Leistung und Verhalten von Arbeitnehmern während des Arbeitsverhältnisses auch gegen den Willen des ausgeschiedenen Arbeitnehmers zu erteilen. Dies könne auch erfolgen, um andere Arbeitgeber bei der Wahrung von deren Belangen zu unterstützen. Jedoch bedürfe es im Einzelfall einer Güter- und Interessenabwägung, um zu klären, ob dem Persönlichkeitsrecht des Arbeitnehmers gleichwertige und schutzwürdige Interessen des Arbeitgebers gegenüberstünden. Das Gericht hat dazu ausgeführt, dass die insoweit vorzunehmenden Überlegungen auch von den Wertungen des Datenschutzrechts bestätigt werden. Im zu entscheidenden Verfahren kommt das Arbeitsgericht zu dem Ergebnis, dass der Beklagten der Klägerin ein Anspruch auf Unterlassung im Urteilstenor aufgeführten Fall zusteht.

Das LAG Rheinland-Pfalz hat die Berufung der Beklagten und die Anschlussberufung der Klägerin gegen das erstinstanzliche Urteil für zulässig erachtet, jedoch in der Sache als unbegründet zurückgewiesen. Das LAG bestätigt die Auffassung des vorinstanzlichen Arbeitsgerichts und führt aus, dass dieses zu Recht davon ausgegangen war, dass die Beklagte verpflichtet sei, es zu unterlassen, auf potenzielle Arbeitgeber der Klägerin zuzugehen und die aus dem erstinstanzlichen Tenor ersichtlichen Behauptungen aufzustellen, wobei ein solcher Anspruch im Hinblick auf einen weiteren Aspekt des Unterlassungsantrags der Klägerin nicht bestehe. Soweit die Unterlassungsklage begründet ist, besteht auch nach Auffassung des Berufungsgerichts zugunsten der Klägerin ein Unterlassungsanspruch nach §§ 1004, 823 Abs. 1 BGB i. V. m. Artt. 1, 2 GG.

In seinen Ausführungen zu den Urteilsgründen legte das LAG unter Verweis auf Rechtsprechung des Bundesarbeitsgerichts dar, dass Arbeitnehmer bei objektiv rechtswidrigen Eingriffen in Persönlichkeitsrechte

einen Anspruch auf Unterlassung weiterer Eingriffe geltend machen können. Das berufliche Wirken eines Betroffenen ordnet das LAG dessen Individualsphäre zu, sodass durch einen Eingriff darin eine Verletzung des Persönlichkeitsrechts vorliegt. Weiterhin führt das LAG aus, dass das durch Artt. 1 und 2 GG gewährleistete allgemeine Persönlichkeitsrecht einen Arbeitnehmer nicht nur vor einer zu weitgehenden Kontrolle und Ausforschung seiner Persönlichkeit schütze, sondern davon auch der Schutz vor der Offenlegung personenbezogener Daten umfasst sei. Dabei komme es nicht darauf an, dass der Arbeitgeber in zulässiger Weise von den Daten Kenntnis erlangt habe.

Das LAG erläutert in seiner Entscheidung das Recht auf informationelle Selbstbestimmung sowie dessen Inhalte und Umfang und setzt sich auch mit den Schranken dieses Rechts auseinander. Es verweist darauf, dass Eingriffe durch die Wahrnehmung überwiegend schutzwürdiger Interessen gerechtfertigt sein können. Insofern bedürfe es einer Güter- und Interessenabwägung im Einzelfall. Unter Verweis auf Rechtsprechung des Bundesarbeitsgerichts legt das LAG dar, dass der Arbeitgeber aus dem Gesichtspunkt der nachwirkenden Fürsorgepflicht gehalten sein kann, über die Erteilung eines Zeugnisses hinaus im Interesse des ausgeschiedenen Arbeitnehmers Auskünfte über diesen an solche Personen zu erteilen, mit denen der Arbeitnehmer in Verhandlungen über den Abschluss eines Arbeitsvertrages steht. Dabei könne er solche Auskünfte auch gegen den Willen des Arbeitnehmers erteilen. Wie bereits die Vorinstanz legt das LAG Wert auf die Durchführung einer Interessenabwägung unter Gewichtung der sich entgegenstehenden Interessen von Arbeitnehmer und Arbeitgeber.

In seiner Wertung kommt das LAG Rheinland-Pfalz zum Ergebnis, dass im vorliegenden Fall kein das Interesse der Klägerin übersteigendes Interesse der Beklagten an der Verbreitung der von der ersten Instanz für berechtigt festgestellten streitgegenständlichen Behauptungen besteht. Die von der Beklagten angeführten Begründungen für die Datenweitergabe hält das Gericht für nicht überwiegend. Demgegenüber habe die Klägerin ein berechtigtes Interesse daran, den Verlauf des vorangegangenen Arbeitsverhältnisses entsprechend ihrer persönlichen Wahrnehmung zu schildern und nicht befürchten zu müssen, dass subjektive Wahrnehmungen der Beklagten ihren Ruf schädigen. Auch bezüglich des Vorwurfs des Verstoßes gegen Datenschutzbestimmungen verneint das LAG ein überwiegendes Interesse der Beklagten an der Weitergabe der vorgenommenen Informationen an die neue Arbeitgeberin in diesem Fall

Auswirkungen auf kirchliche Einrichtungen

Kirchliche Arbeitgeber sollten neben der datenschutzrechtlichen auch die arbeitsrechtliche Rechtsprechung beobachten. Wie der Beispielsfall zeigt, kann auch eine arbeitsgerichtliche Entscheidung sich auf Sachverhalte beziehen, die datenschutzrechtliche Themen berühren.

Aus der Entscheidung kann die Erkenntnis gewonnen werden, dass Arbeitnehmer grundsätzlich vor einer unzulässigen Offenlegung ihrer personenbezogenen Daten aufgrund des informationellen Selbstbestimmungsrechts geschützt sind. Nur in Ausnahmefällen kann eine Zulässigkeit der Datenweitergabe gegeben sein, sofern nach einer durchzuführenden Abwägung zwischen sich gegenüberstehenden Interessen der Beteiligten so gravierende Gründe aufseiten des Arbeitgebers bestehen, dass die geschützten Interessen des Arbeitnehmers zurücktreten müssen. Die vorliegende Entscheidung zeigt aber, dass selbst berechtigte Interessen des Arbeitgebers nicht ausreichend sein können, um ein Überwiegen des Arbeitgeberinteresses feststellen zu können. In diesen Fällen besteht dann der klageweise geltend gemachte Unterlassungsanspruch zu Recht.

Kirchliche Arbeitgeber sollten daher vor der Anfrage bei einem vorherigen Arbeitgeber oder bei der Weitergabe von Daten als vorheriger Arbeitgeber eine sorgfältige Abwägung der Interessen vornehmen, um bei der Übermittlung der Daten keinen Datenschutzverstoß zu verursachen.

2.11 Auch Vorbekanntes vom Auskunftsanspruch umfasst

Anfragen und Beschwerden rund um das Auskunftsrecht nach § 17 KDG[45] nehmen immer noch einen größeren Anteil der Vorgänge ein, die an das Katholische Datenschutzzentrum herangetragen werden. Die Frage nach dem Umfang der Auskunft im Rahmen der Geltendmachung des Rechts auf Auskunft nach Art. 15 DSGVO beschäftigt Verantwortliche regelmäßig. Der Wortlaut dieser Vorschrift sowie der Inhalt des vergleichbaren § 17 KDG lässt Interpretationsspielräume zu. Ein Aspekt dabei ist das Thema derjenigen Daten, die dem Anfragenden bereits bekannt sein müssten. Es stellt sich bei Auskunftsbegehren immer wieder neu die Frage, welche der zur Auskunft gehörigen Informationen dem Fragesteller bereits bekannt sind und ihm vorliegen. Die weitere Frage ist dann, ob diese Informationen im Rahmen der Auskunft mit aufgeführt werden müssen oder ob darauf verzichtet werden kann, weil diese Informationen bereits bekannt sein müssten. Verantwortliche entscheiden sich dabei oft zur Verringerung des Aufwands dafür, dass diese Informationen bei der Antwort auf das Auskunftsbegehren nicht aufgeführt werden, zumindest aber im Rahmen der Erteilung von Kopien nicht mit übersandt werden. Der Beschluss des Landgerichts Bonn[46] bietet Anhaltspunkte für eine klarere Festlegung zu den Inhalten und Umfängen der Auskünfte.

[45] Siehe hierzu Abschnitt 2.3.1 dieses Jahresberichts.
[46] LG Bonn, Beschluss vom 24.05.2022, Az.: 9 O 158/21.

Dem Beschluss des LG Bonn lag ein Auskunftsbegehren zugrunde, in der die Klägerin Auskunft bezüglich ihrer Daten bei einer Krankenversicherung begehrt hatte. Zwar hatte die Versicherung eine Auskunft gegeben. Diese wurde aber nach Auffassung des LG Bonn nicht vollständig erteilt.

Das LG Bonn hat in seinem Beschluss festgestellt, dass durch die Klägerin betreffende Abrechnungsdaten nicht vollständig beauskunftet worden seien. Diese Informationen gelten nach Auffassung des Gerichts als personenbezogene Daten im Sinne der DSGVO und sind im Rahmen der Auskunft aufzuführen. Auch Schreiben der Klägerin an die beklagte Versicherung und umgekehrt sind nach den Ausführungen des Gerichts ihrem gesamten Inhalt nach als personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO anzusehen. Das Gericht hat weiter ausgeführt, dass auch interne Vermerke oder interne Kommunikation bei der Beklagten Informationen über die Klägerin enthalten können.

Das Gericht hat den Einwendungen der Versicherung, wonach bestimmte Informationen der Klägerin bereits bekannt und deswegen vom Auskunftsrecht nicht erfasst seien, entgegengehalten, dass die Bekanntheit von Schreiben und Rechnungen für sich genommen den datenschutzrechtlichen Auskunftsanspruch nicht ausschließe. Aus diesem Grund kommt das LG Bonn zu dem Ergebnis, dass das Auskunftsbegehren nicht vollständig erfüllt worden sei.

Mit seiner Rechtsauffassung folgt das LG Bonn den Vorgaben des Bundesgerichtshofs. Auch der Bundesgerichtshof hatte in seinem Urteil zum Auskunftsanspruch vom 15.06.2021[47] ähnlich entschieden. Nach Auffassung des BGH umfasst der Auskunftsanspruch auch Informationen aus bisheriger Korrespondenz sowie interne Vermerke über den die Auskunft beantragenden Kunden.

Auswirkungen auf kirchliche Einrichtungen

Aufgrund der Rechtsgrundlage des § 17 KDG sind kirchliche Rechtsträger dazu verpflichtet, in gesetzeskonformer Weise auf Auskunftsbegehren zu reagieren. Eine pauschale Verweigerung der Beauskunftung von Inhalten, die aus Sicht der kirchlichen Stelle der betroffenen Person schon bekannt sind, ist nicht möglich. Solange kein Missbrauch des Auskunftsrechts vorliegt, sind auch diese Angaben in die Auskunft einzuschließen.

[47] BGH, Urteil vom 15.06.2022, Az.: VI 576/19.

2.12 Aus der Rechenschaftspflicht des § 7 Abs. 2 KDG können sich im Einzelfall auch (neue) Compliance-Pflichten ergeben

In seinem Urteil vom 27.10.2022 (C-129/21)[48] beschäftigte sich der Europäische Gerichtshof u. a. mit der Vorlagefrage, ob Art. 5 Abs. 2 und Art. 24 DSGVO[49] dahingehend auszulegen sind, dass eine nationale Aufsichtsbehörde verlangen kann, dass ein Anbieter von Teilnehmerverzeichnissen als Verantwortlicher geeignete technische und organisatorische Maßnahmen ergreift, um weitere Verantwortliche, nämlich den Telefondienstanbieter, der ihm die personenbezogenen Daten seines Teilnehmers übermittelt hat, sowie die anderen Anbieter von Teilnehmerverzeichnissen, denen er selbst solche Daten geliefert hat, über den Widerruf der Einwilligung dieses Teilnehmers zu informieren.

Für ein grundlegendes Verständnis stark vereinfacht zusammengefasst, werden personenbezogene Daten eines Teilnehmers von einem Telefondienstanbieter an einen Anbieter von Teilnehmerverzeichnissen übermittelt. Dieser Anbieter veröffentlicht die Daten (vergleichbar mit einem Telefonbuch) und übermittelt sie wiederum an weitere Anbieter von Teilnehmerverzeichnissen. Rechtsgrundlage für die Veröffentlichung ist eine vom Teilnehmer gegenüber dem Telefondienstanbieter erklärte Einwilligungserklärung, auf die sich auch die weiteren Verantwortlichen in der Kette (Anbieter von Teilnehmerverzeichnissen) berufen.[50]

Nach Art. 6 Abs. 1 lit. a) DSGVO (vgl. hierzu § 6 Abs. 1 lit. b) KDG) ist eine Verarbeitung rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

Jedoch muss sich der Verantwortliche gemäß Art. 5 Abs. 1 lit. a) und Abs. 2 DSGVO (vgl. hierzu § 7 Abs. 1 lit. a) und Abs. 2 KDG) vergewissern, dass er nachweisen kann, dass die personenbezogenen Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Art. 24 DSGVO (vgl. hierzu § 26 KDG) verlangt seinerseits, dass der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt.

Der EuGH legt in seiner Entscheidung nunmehr u. a. fest, was von dem Anbieter eines Teilnehmerverzeichnisses verlangt beziehungsweise erwartet werden kann, wenn ein Teilnehmer diesem gegenüber die ursprünglich gegenüber einem Telefondienstanbieter erteilte Einwilligung widerruft.

In seinem Urteil schließt sich der EuGH zunächst den Ausführungen des Generalanwalts aus seinen Schlussanträgen an, dass „Art. 5 Abs. 2

[48] Europäischer Gerichtshof, Urteil vom 27.10.2022, Rechtssache C-129/21, ECLI:EU:C:2022:833.
[49] Entspricht § 7 Abs. 2 KDG und § 26 KDG.
[50] Eine tiefergehende Betrachtung der im konkreten Fall beurteilten Konstellation erfordert ggf. eine Auseinandersetzung mit den Spezifika der belgischen Rechtslage.

und Art. 24 DSGVO den für die Verarbeitung personenbezogener Daten Verantwortlichen eine allgemeine Rechenschaftspflicht sowie Compliance-Pflichten auf[-erlegen]. Insbesondere verpflichten diese Bestimmungen die Verantwortlichen, zur Wahrung des Rechts auf Datenschutz geeignete Maßnahmen zu ergreifen, um etwaigen Verstößen gegen die Vorschriften der DSGVO vorzubeugen."

In diesem Sinne sieht Art. 19 DSGVO (vgl. hierzu § 21 KDG) u. a. vor, dass der Verantwortliche allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen Daten nach Art. 17 Abs. 1 (vgl. hierzu § 19 Abs. 1 KDG) dieser Verordnung mitteilt, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

„Aus den allgemeinen Verpflichtungen nach Art. 5 Abs. 2 und Art. 24 DSGVO in Verbindung mit deren Art. 19 ergibt sich, dass ein für die Verarbeitung personenbezogener Daten Verantwortlicher […] geeignete technische und organisatorische Maßnahmen ergreifen muss, um die anderen Anbieter von Teilnehmerverzeichnissen, denen er solche Daten geliefert hat, über den an ihn gerichteten Widerruf der Einwilligung der betroffenen Person zu informieren. Unter Umständen […] muss ein solcher Verantwortlicher auch den Telefondienstanbieter, der ihm die personenbezogenen Daten übermittelt hat, informieren, damit dieser die Liste der personenbezogenen Daten, die er dem Anbieter von Teilnehmerverzeichnissen nach einem automatisierten Verfahren übermittelt, anpasst und die Daten seiner Teilnehmer herausfiltert, die ihren Willen bekundet haben, ihre Einwilligung zur Veröffentlichung dieser Daten zu widerrufen."

„Der EuGH stellt weiter fest, dass für den Fall, dass sich „verschiedene Verantwortliche auf eine einheitliche Einwilligung der betroffenen Person stützen" der Widerruf der Einwilligung durch die betroffene Person gegenüber irgendeinem der Verantwortlichen genügt."

Der EuGH stellt weiter fest, dass für den Fall, dass sich „verschiedene Verantwortliche auf eine einheitliche Einwilligung der betroffenen Person stützen" der Widerruf der Einwilligung durch die betroffene Person gegenüber irgendeinem der Verantwortlichen genügt. Um die Wirksamkeit des Art. 7 Abs. 3 DSGVO (vgl. hierzu § 8 Abs. 6 KDG) zu gewährleisten, „ist der Verantwortliche […] verpflichtet, jede Person, die ihm diese Daten übermittelt hat, sowie die Person, der er seinerseits die Daten übermittelt hat, über den Widerruf zu informieren. Die dementsprechend informierten Verantwortlichen sind dann ihrerseits verpflichtet, diese Informationen an die anderen Verantwortlichen weiterzuleiten, denen sie solche Daten übermittelt haben." Nur so ist die gesetzliche Vorgabe sichergestellt, dass der Widerruf so einfach wie die Erteilung der Einwilligung ist.

Abschließend beantwortet der EuGH die o. g. Vorlagefrage damit, dass Art. 5 Abs. 2 und Art. 24 DSGVO dahingehend auszulegen sind, dass eine nationale Aufsichtsbehörde verlangen kann, dass ein Anbieter von Teilnehmerverzeichnissen als Verantwortlicher geeignete technische und organisatorische Maßnahmen ergreift, um weitere Verantwortliche, nämlich den Telefondienstanbieter, der ihm die personenbezogenen Daten seines Teilnehmers übermittelt hat, sowie die anderen Anbieter von Teilnehmerverzeichnissen, denen er selbst solche Daten geliefert hat, über den Widerruf der Einwilligung dieses Teilnehmers zu informieren.

Zwar ist die Entscheidung zu einem speziellen Sachverhalt ergangen, der so im kirchlichen Bereich nicht auftreten wird. Mit der Entscheidung

macht der EuGH aber deutlich, dass in manchen Fällen aus der Weitergabe von Daten weitergehende Pflichten entstehen können, wenn die ursprüngliche Rechtsgrundlage für die Datenverarbeitung beim Verantwortlichen entfällt und dies auch Auswirkungen auf die Rechtsmäßigkeit der Daten beim Empfänger der Daten hat.

2.13 Mitarbeitervertretung muss eigene angemessene Schutzmaßnahmen vorsehen und nachweisen, wenn sie vom Arbeitgeber Auskunft über sensible Daten verlangt

Im Jahresbericht 2021 war von der Neuregelung des § 79a Betriebsverfassungsgesetz (BetrVG) berichtet worden. Der Bundesgesetzgeber hatte hier entschieden, dass Betriebsräte nicht Verantwortliche (Art. 4 Nr. 7 DSGVO / § 4 Nr. 9 KDG) im Sinne des Datenschutzrechts sind.[51]

Das Katholische Datenschutzzentrum hat diese Wertungsentscheidung des Bundesgesetzgebers für die eigene Beratungs- und Prüfpraxis auf die Situation im kirchlichen Bereich übertragen und deutlich gemacht, dass den Arbeitgeber damit die datenschutzrechtlichen Pflichten für den Zuständigkeitsbereich der Mitarbeitervertretung bei gleichzeitig eingeschränkten Kontroll- und Einflussmöglichkeiten treffen.[52]

Mit dieser Ausgangslage durfte sich das Landesarbeitsgericht Baden-Württemberg im Berichtszeitraum in einem Beschluss[53] im Zusammenhang mit dem Auskunftsbegehren eines Betriebsrates auseinandersetzen und hat sich zu Anforderungen bei der datenschutzrechtlichen Ausgestaltung der Organisation und zu den Vorgehensweisen von Betriebsräten im Umgang mit personenbezogenen Daten geäußert.

Gemäß den Ausführungen des LAG ist für ein zulässiges Auskunftsbegehren eines Betriebsrates ein konkreter Bezug auf dessen Aufgaben erforderlich. Sofern gesetzliche Anforderungen bestehen, welche dem Aufgabenkreis eines Betriebsrates zuzurechnen sind, steht diesem auch ein Anspruch auf Beauskunftung seiner Anfragen gegenüber dem Arbeitgeber zu. Nicht erforderlich ist dafür ein Vorbringen bezüglich einer konkreten besonderen geplanten Maßnahme.

Um berechtigter Empfänger von vertraulichen personenbezogenen Informationen zu sein, insbesondere wenn es sich um besondere personenbezogene Daten im Sinne des Art. 9 Abs. 1 DSGVO handelt, muss der Betriebsrat sicherstellen und erforderlichenfalls nachweisen können, dass er einen hinreichenden Datenschutz gewährleistet. Das Gericht entnimmt aus der Vorschrift des § 79a BetrVG, dass ein Betriebsrat im Rahmen seiner Verarbeitung personenbezogener Daten den erforderlichen Datenschutz zu gewährleisten hat. Dabei bleibt der Arbeitgeber für die Verarbeitung verantwortlich, wobei das Gesetz durch § 79a S. 1 und S. 2 BetrVG beiden Beteiligten eine gegenseitige Unterstützung auferlegt. Nach Auffassung des LAG gehören zum erfor-

> **„Um berechtigter Empfänger von vertraulichen personenbezogenen Informationen zu sein, … muss der Betriebsrat sicherstellen und erforderlichenfalls nachweisen können, dass er einen hinreichenden Datenschutz gewährleistet.“**

[51] Siehe Abschnitt 1.2.5 des Jahresberichts 2021.
[52] Siehe Abschnitt 1.2.5 des Jahresberichts 2021.
[53] LAG Baden-Württemberg, Beschluss vom 20.05.2022, Az.: 12 TaBV 4/21.

derlichen Datenschutz angemessene und spezifische Schutzmaßnahmen, einschließlich eines ausreichenden Schutzkonzepts.

Im konkreten Fall hatte der Betriebsrat dargelegt, dass bei Übergabe von physischen Unterlagen, wie Informationen in gedruckter Form, diese nur durch dazu benannte Personen entgegengenommen und in das Betriebsratsbüro verbracht werden dürfen, wobei sich dieses in einem abschließbaren Raum, zu dem ausschließlich Betriebsratsmitglieder Zutritt haben, befindet. Darüber hinaus werden Unterlagen in einem verschließbaren Schrank aufbewahrt, zu dem ausschließlich bestimmte Vertreter den Schlüssel besitzen. Unterlagen, die besonders sensible Daten enthalten, würden nur im Rahmen von Betriebsratssitzungen offengelegt. Für Übermittlungen von Daten per E-Mail konnte der Betriebsrat auf eine eigenständige E-Mail-Adresse und einen im Betriebsratsbüro stationär eingerichteten Desktop-PC verweisen. Der Zugang zum Betriebssystem dieses PCs war nach Angaben des Betriebsrates durch ein ausschließlich den Betriebsratsmitgliedern zur Verfügung stehendes Passwort gesichert. Weiter war die Löschung von nicht mehr benötigten Daten in geeigneter Weise vorgesehen.

Das LAG hat in seinem Beschluss den Antrag des Betriebsrates auf Auskunft aus § 80 Abs. 2 S. 1 BetrVG für begründet erklärt. Soweit zur Erfüllung des Auskunftsanspruchs die Übermittlung sensitiver Daten erforderlich ist, benennt das Gericht unter Verweis auf die Rechtsprechung des Bundesarbeitsgerichts die Voraussetzung, dass der Betriebsrat zur Wahrung der Interessen der von der Datenverarbeitung betroffenen Arbeitnehmer angemessene und spezifische Schutzmaßnahmen treffen muss. Wegen des besonderen Status eines Betriebsrates im Unternehmen kann nach den Darlegungen des Gerichts der Arbeitgeber die Erfüllung des in § 26 Abs. 3 S. 3 i. V. m. § 22 Abs. 2 BDSG (Bundesdatenschutzgesetz) geregelten Gebots angemessener und spezifischer Schutzmaßnahmen nicht unmittelbar realisieren, da er die Unabhängigkeit des Betriebsrates im Rahmen der gesetzlichen Vorgaben beachten muss. Aufseiten des Betriebsrates bestehe im Gegenzug die Verpflichtung, bei der Geltendmachung eines Anspruchs, der sich auf sensible besondere personenbezogene Daten richtet, darzulegen, welche Maßnahmen er ergriffen hat, um berechtigte Interessen der betroffenen Arbeitnehmer zu wahren. Das Gericht hat dazu ausgeführt, dass Maßnahmen zur Datensicherheit dazu gehören können, wie etwa das zuverlässige Sicherstellen des Verschlusses der Daten, die Gewähr begrenzter Zugriffsmöglichkeiten oder deren Beschränkung auf einzelne Betriebsratsmitglieder sowie die Datenlöschung nach Beendigung der Überwachungsaufgabe des Betriebsrates. Das Gericht hat auch aufgezeigt, dass eine mögliche Umsetzungsmaßnahme zur Gewährleistung der Datensicherheit darin liegen kann, freiwillig einen Datenschutz-Sonderbeauftragten für den Betriebsrat zu benennen, eine verpflichtende Grundschulung im Datenschutz für sämtliche Betriebsratsmitglieder zu organisieren sowie ein eigenes Datenschutzkonzept zu entwickeln, die Rechte der betroffenen Beschäftigten sicherzustellen und vor allem ein Löschkonzept vorzuhalten.

Im konkreten Fall hat das LAG festgestellt, dass nach seiner Auffassung mit den vom Betriebsrat geschilderten Maßnahmen ein ausreichendes Datenschutzkonzept vorliegt und somit ein hinreichender Datenschutz besteht, um den Auskunftsanspruch erfüllen zu können. Soweit es auf die Übermittlung konkreter personenbezogener Daten ankomme,

könne ein Betriebsrat nicht auf die Schutzmaßnahmen der Anonymisierung und Pseudonymisierung verwiesen werden. Er benötige gerade die konkreten personenbezogenen Daten, um die Betroffenen kontaktieren zu können.

Das Gericht hat in seinem Beschluss weiterhin ausgeführt, dass der Betriebsrat keinen eigenständigen Datenschutzbeauftragten beauftragen muss, da die Verpflichtung zu dessen Benennung sich nicht an den Betriebsrat richte, sondern an den Arbeitgeber. Eine Verarbeitung personenbezogener Daten im Geltungsbereich der DSGVO unterliege nach Auffassung des Gerichts der Überwachung durch den betrieblichen Datenschutzbeauftragten, weshalb dieser auch berechtigt sei, die Abläufe und den Datenschutz des Betriebsrates zu prüfen. Dabei sei zu beachten, dass der betriebliche Datenschutzbeauftragte in den Betriebsrat betreffenden Fällen eine besondere Vertraulichkeit wahrt.

Das LAG hat weiter ausgeführt, dass nicht verlangt werden könne, dass der Betriebsrat zur Präzisierung der Maßnahmen dazu verpflichtet sei, ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO zu führen und dort Verfahren zu dokumentieren. Das Gleiche gelte für eine gegebenenfalls erforderliche Datenschutz-Folgeabschätzung nach Art. 35 Abs. 1 DSGVO. Das Führen dieser Verzeichnisse bzw. Dokumentationen obliege der verantwortlichen Stelle im Sinne des Art. 4 Nr. 7 BDSG. Eine solche verantwortliche Stelle sei der Betriebsrat nach der Neuregelung des § 79a BetrVG gerade nicht.

Auswirkungen auf kirchliche Einrichtungen

Auch wenn die Regelungen für kirchliche Mitarbeitervertretungen mit denen für Betriebsräte nicht identisch sind, da es Unterscheidungen aufgrund der Besonderheiten des kirchlichen Arbeitsrechts und der entsprechenden Anforderungen gibt sowie Elemente des Personalvertretungsrechts in die Mitarbeitervertretungsordnungen eingeflossen sind, kann die Rechtsprechung zu den Betriebsräten bezüglich der Anforderungen an die Ausgestaltung der Betriebsratstätigkeiten und die Ausstattungen hier herangezogen werden.

Mitarbeitervertretungen sollten ebenso wie Betriebsräte so ausgestattet sein, dass sie die ihnen zur Verfügung gestellten Unterlagen sicher aufbewahren können. Dazu gehören u. a. abschließbare Schränke und abschließbare Räumlichkeiten bei gleichzeitiger Beschränkung des Zutritts auf die dazu berechtigten und notwendigen Personen. Auch die technische Ausstattung sollte so umgesetzt sein, dass vertrauliche, insbesondere besondere Kategorien personenbezogene Daten, sicher vor unberechtigten Zugriffen aufbewahrt werden können. Dies umfasst die auch im obigen Gerichtsverfahren angesprochene eigenständige E-Mail-Adresse mit Passwortschutz und die Limitierung der Zugriffsberechtigungen auf die notwendig damit zu befassenden Personen wie die Mitglieder der Mitarbeitervertretung. Mitarbeitervertretungen sollten entsprechend den Ausführungen im Beschluss Datenschutzkonzepte entwickeln und die Löschung nicht mehr benötigter sensibler Daten vorsehen. Auch wenn dies nicht ausdrücklich im Gesetz aufgeführt ist, empfiehlt es sich, dass auch Mitarbeitervertretungen den Rat des betrieblichen Datenschutzbeauftragten bei der näheren Ausgestaltung einholen.

2.14 Aufbewahrungsfrist zur Erfüllung der KDG-Nachweispflichten

Im KDG werden verschiedene Rechenschaftspflichten für Verantwortliche normiert. Eine Rechenschaftspflicht ist ein allgemeiner Grundsatz, der sicherstellen soll, dass Verantwortliche die gesetzlichen Anforderungen erfüllen. So muss sich jeder Verantwortliche gemäß § 7 Abs. 1 KDG an die allgemeinen Verarbeitungsgrundsätze halten. Die Einhaltung dieser Grundsätze muss ein Verantwortlicher auch in geeigneter Weise dokumentieren und nachweisen können. Diese Nachweispflicht ist z. B. für die allgemeinen Verarbeitungsgrundsätze in § 7 Abs. 2 KDG und für den Nachweis einer Verarbeitung aufgrund einer Einwilligung in § 8 Abs. 5 KDG geregelt.

Fraglich ist aber wie lange ein Verantwortlicher diese Nachweise erbringen beziehungsweise aufbewahren muss. Das KDG trifft dazu an keiner Stelle eine Regelung.[54] Vertreten werden könnte, dass ein Verantwortlicher die nötigen Nachweise ohne zeitliche Begrenzung aufbewahren muss.[55] Ein Anhaltspunkt für die zeitliche Begrenzung der Aufbewahrung könnte im Haftungsrisiko des Verantwortlichen zu finden sein. Ein Verstoß gegen die Rechenschaftspflichten kann durch die Datenschutzaufsicht gemäß § 51 KDG mit einem Bußgeld geahndet werden. Über § 25 Abs.1 KDS-VwVfG (Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz) finden die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) Anwendung bei der Verhängung von Bußgeldern durch die Datenschutzaufsicht. Ordnungswidrigkeiten verjähren gemäß § 31 Abs. 2 OWiG nach spätestens 3 Jahren. Nach dieser Zeit droht dem Verantwortlichen bei Verletzung seiner Rechenschaftspflichten beziehungsweise bei fehlendem Nachweis kein Bußgeld nach § 51 KDG mehr.[56] Diese Verjährungsfrist könnte daher als zeitliche Begrenzung der Aufbewahrungspflichten herangezogen werden.[57] Anders könnte das in Hinsicht auf die Verteidigung gegen zivilrechtliche Schadensersatzansprüche zu beurteilen sein. Diese unterliegen einer deutlich längeren Verjährungsfrist von 10 bis 30 Jahren gemäß § 199 Abs. 2 BGB.

An dieser Stelle ist noch das Verhältnis des Löschungsanspruchs des Betroffenen aus § 19 Abs. 1 KDG zu den oben beschriebenen Nachweispflichten zu erwähnen. Grundsätzlich kann eine betroffene Person vom Verantwortlichen die Löschung ihrer personenbezogenen Daten verlangen. Die Löschung muss allerdings nicht erfolgen, wenn die anhaltende Verarbeitung erforderlich ist. Diese Ausnahmetatbestände sind in § 19 Abs. 3 KDG normiert. Insbesondere ist die Verarbeitung erforderlich, wenn den Verantwortlichen gemäß Abs. 3 lit. b) eine rechtliche Verpflichtung zur Aufbewahrung trifft. Möglich ist auch, dass die Verarbeitung gemäß Abs. 3 lit. e) zur Ausübung oder Verteidigung von Rechten erforderlich ist.

Schließlich sollten Verantwortliche ihre Entscheidung für eine begrenzte Aufbewahrung, unabhängig von ihrer Länge, begründen und dokumentieren.

„Schließlich sollten Verantwortliche ihre Entscheidung für eine begrenzte Aufbewahrung, unabhängig von ihrer Länge, begründen und dokumentieren."

[54] Die gleiche Problematik existiert auch in der DSGVO.

[55] In der Literatur zum Art. 5 Abs. 2 DSGVO wird das auch vertreten. Siehe z. B. Reimer in: Sydow/Marsch, DS-GVO | BDSG, Rn. 59, 3. Auflage 2022.

[56] Andere Anordnungsbefugnisse durch die Datenschutzaufsicht sind von einer Verjährung nicht betroffen.

[57] Im Bereich der DSGVO wurde diese Ansicht vom Landesbeauftragten für den Datenschutz und Informationsfreiheit Thüringen vertreten. Siehe Jahresbericht des Landesbeauftragten 2021, S. 167 ff.; so auch in der Literatur zur DSGVO Voigt in: Taeger/Gabel, DSGVO - BDSG - TTDSG, 4. Auflage 2022, Art. 5, Rn. 41–46.

3 Die kirchliche Datenschutzaufsicht in den nordrhein-westfälischen (Erz-)Diözesen und beim Verband der Diözesen Deutschlands

3.1 Der gemeinsame Diözesandatenschutzbeauftragte

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. Im Zuständigkeitsgebiet leben fast 6,4 Millionen Menschen römisch-katholischen Glaubens (Stand 2021).

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands[58] 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 damit unter anderem auch 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.

Die Aufgaben des Diözesandatenschutzbeauftragten beziehungsweise des Verbandsdatenschutzbeauftragten des VDD als Datenschutzaufsicht sind im KDG beziehungsweise im KDG-VDD[59] 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. 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."[60]

Der Diözesandatenschutzbeauftragte, seine Stellvertreterin und die Mitarbeiterinnen und Mitarbeiter bringen ihre Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von

[58] Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter".
[59] Im Folgenden wird nicht immer explizit auf die gleichlautende Vorschrift des KDG-VDD verwiesen.
[60] Für eine ausführliche Darstellung der Aufgaben der Datenschutzaufsicht siehe Abschnitt 3.5 des Jahresberichts 2021.

kirchlichen Gremien und Arbeitsgruppen ein. Die Beratung der Gremien und Arbeitsgruppen ist Teil des gesetzlichen Auftrags der Datenschutzaufsichten.

3.2 Das Katholische Datenschutzzentrum

Das Katholische Datenschutzzentrum bildet als Körperschaft des öffentlichen Rechts den Rahmen für die Arbeit des Diözesandatenschutzbeauftragten und unterstützt diesen bei der Ausübung der Datenschutzaufsicht über die katholischen Einrichtungen in den fünf (Erz-)Diözesen Aachen, Essen, Köln, Münster und Paderborn und für den Verband der Diözesen Deutschlands. Eine Datenschutzaufsicht in den einzelnen (Erz-)Diözesen gab es parallel zu den staatlichen Datenschutzaufsichten auch bereits vor der Gründung des Katholischen Datenschutzzentrums.

Das Katholische Datenschutzzentrum in Dortmund ist als Umsetzung der Rechtsprechung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden als eigenständige und unabhängige Körperschaft des öffentlichen Rechts gegründet worden.[61] Der Diözesandatenschutzbeauftragte ist zugleich Leiter dieser Körperschaft und vertritt diese nach außen. 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.

Abb.: Das Katholische Datenschutzzentrum hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn. (Bild: Sozialinstitut Kommende Dortmund)

[61] 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.

Dem Diözesandatenschutzbeauftragten sind eine Vertreterin, Referenten und Sachbearbeiter zur Seite gestellt. 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.[62]

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 2022 sieht der Haushaltsplan für das Katholische Datenschutzzentrum ein Volumen in Höhe von 1.396.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben vor. Für das Folgejahr 2023 sinkt das genehmigte Budget leicht auf 1.364.000 Euro.

3.3 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 auch ein Schutzpatron von den (Erz-)Diözesen 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[63].

[62] 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.

[63] 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 (Bild: Katholisches Datenschutzzentrum)

3.4 Öffentlichkeitsarbeit

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

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.

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.

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.

Das Katholische Datenschutzzentrum ist mit einem eigenen „besonderen elektronischen Behördenpostfachs (beBPo)" an den elektronischen Rechtsverkehr angebunden.

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.

3.5 Antragsverfahren vor dem Interdiözesanen Datenschutzgericht

Im Berichtszeitraum sind sechs Verfahren aus 2022 beim Interdiözesanen Datenschutzgericht (IDSG) anhängig, bei denen das Katholische Datenschutzzentrum als Antragsgegner oder Beteiligter geführt wird.

Inhaltlich betreffen die Verfahren fast ausschließlich Beschwerdeverfahren, welche durch das KDSZ gemäß § 48 KDG bearbeitet wurden, das heißt, dass sich ein Betroffener mit einer datenschutzrechtlichen Eingabe an das Katholische Datenschutzzentrum gewandt hatte und anschließend gegen den Bescheid mittels gerichtlichen Rechtsbehelf vorgegangen wurde oder auch gegen den früheren Beschwerdegegner (in diesen Fällen wurde das KDSZ durch Verfügung des Gerichts zum Beteiligten). Dabei wenden sich die Antragsteller gegen die Verarbeitung ihrer personenbezogenen Daten in (ehemaligen) Beschäftigungsverhältnissen oder auch gegen die Art der Verarbeitung im Bewerbungsverfahren sowie gegen die Abfrage vom pandemiebedingten "3-G-Status" im Zusammenhang mit Veranstaltungen. Auch Fragestellungen im Zusammenhang mit der Personalakte und dem Auskunftsanspruch nach § 17 KDG sind Themen der anhängigen Verfahren aus 2022.

Da die Kirchliche Datenschutzgerichtsordnung (KDSGO) keinen Anwaltszwang vorschreibt, ist es den Antragstellern freigestellt, ob sie ihren Rechtsbehelf selbst verfolgen und sich selbst vertreten oder dies durch einen Rechtsanwalt vornehmen lassen. In den anhängigen Verfahren ist beides der Fall. Da es sich durchaus um wichtige und für die weitere datenschutzrechtliche Aufsichtspraxis relevante Fragestellungen handelt, werden die Entscheidungen des IDSG in 2023 mit Spannung erwartet.

3.6 Sprecher der Konferenz der Diözesandatenschutzbeauftragten

Nachdem der Diözesandatenschutzbeauftragte der nordrhein-westfälischen (Erz-)Diözesen und Leiter des Katholischen Datenschutzzentrums im Jahr 2019 bereits Sprecher der Konferenz der Diözesandatenschutzbeauftragten war, wählten ihn die anderen Diözesandatenschutzbeauftragten für das Jahr 2022 erneut zum Sprecher der Konferenz.

Mit dieser Funktion verbunden ist u. a. die Repräsentation der Konferenz in einigen Gremien, zu denen ein Vertreter der kirchlichen Datenschutzaufsichten eingeladen wird. So nimmt der Sprecher beratend an den Sitzungen des Gremiums teil, was auf Ebene des VDD die Entwicklung des Datenschutzrechts in der katholischen Kirche begleitet. Außerdem nahm der Sprecher im Berichtszeitraum an zwei Treffen der staatlichen Datenschutzaufsichten mit den Datenschutzaufsichten im Bereich der Medien und der Kirche teil. Diese Treffen sind Teil des wichtigen und kontinuierlichen Austausches, den die Diözesandatenschutzbeauftragten mit den staatlichen Datenschutzaufsichten und den Datenschutzaufsichten der Medien führen.

3.7 Zusammenarbeit mit der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder

In 2022 konnte die Beteiligung an den Arbeitskreisen der DSK ausgeweitet werden. Die katholischen Aufsichten werden seit längerem durch mindestens einen Vertreter in mehreren Arbeitskreisen, darunter der Arbeitskreis Technik und der Arbeitskreis Grundsatz, mit Gaststatus vertreten. In 2022 konnte dieser Status ebenfalls für die Arbeitskreise Gesundheit und Soziales sowie Medien erreicht werden.

Das KDSZ sieht die Teilnahme an den unterschiedlichen Arbeitskreisen als unbedingt notwendig an, da nur so ein einheitliches Datenschutzniveau bezogen auf die vielfältigen Themen, die auch in den kirchlichen Einrichtungen relevant sind, erreicht werden kann und nicht unterschiedlich mit datenschutzrechtlichen Fragestellungen umgegangen wird. Da eines der Ziele der DSGVO die Vereinheitlichung des europäischen Datenschutzniveaus ist, ist es elementar wichtig, dass auch die katholischen Aufsichten – ebenso wie die Aufsichten in der EKD – von den Entschließungen und den Beschlüssen der DSK nicht erst durch deren Veröffentlichung erfahren, sondern vielmehr an den Diskussionen und Denkprozessen beteiligt werden. Daher sieht das KDSZ den Fortschritt im Berichtsjahr als besonders positiv und erwähnenswert an.

4 Dokumentation

4.1 Die Datenschutzaufsicht in der katholischen Kirche

Die Datenschutzaufsicht für die (Erz-)Diözesen in der katholischen Kirche in Deutschland wird von fünf überdiözesanen Stellen wahrgenommen. Diese fünf Diözesandatenschutzbeauftragten sind jeweils für mehrere (Erz-)Diözesen 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 Einrichtungen. 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 (DOK), der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung der Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.

Zu den Aufgaben der Diözesandatenschutzbeauftragten 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

„Sie erreichen die Konferenz postalisch unter der Adresse des Katholischen Datenschutzzentrums in Dortmund oder per E-Mail unter mail@konferenz-ddsb.de."

den Konferenzen auch die von der Deutschen Ordensobernkonferenz bestellten Ordensdatenschutzbeauftragten für die päpstlichen Ordensgemeinschaften eingeladen.[64]

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 mail@konferenz-ddsb.de.

4.2 Veröffentlichungen des Katholischen Datenschutzzentrums – Auszug –

Im Berichtszeitraum hat das Katholische Datenschutzzentrum durch seine Veröffentlichungen die Praxis der letzten Jahre fortgeführt, 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 Band 3 – Festschrift zum 80. Geburtstag von Jupp Joachimski

Pünktlich zum Geburtstag des Jubilars, dem Diözesandatenschutzbeauftragten der bayerischen (Erz-)Diözesen Jupp Joachimski, konnte die ihm zu Ehren entstandene Festschrift mit dem Titel „Justiz die Pflicht – Datenschutz die Kür" fertiggestellt werden.

Die Festschrift beinhaltet sowohl private Einblicke in das aufregende Leben des Jubilars, als auch fachliche Auseinandersetzungen mit Themen rund um das kirchliche Datenschutzrecht, das Kirchenrecht und aus den vielfältigen Rechtsgebieten, in denen Jupp Joachimski während seines Berufslebens tätig war. Die Festschrift konnte deswegen so spannende und interessante Autoren für sich gewinnen, da die Herausgabe in Zusammenarbeit zwischen dem Katholischen Datenschutzzentrum und der Ordensdatenschutzbeauftragten Christine Haumer, die zugleich die Tochter des Jubilars ist, entstand. Bei der Lektüre wird dem interessierten Lesenden auffallen, dass der Jubilar vor seiner (kirchlichen) Datenschutzkarriere schon immer sehr technikinteressiert war und dies auch über seine Berufsjahre weitergegeben hat, wovon auch der kirchliche Datenschutz heute profitiert.

Die Festschrift erscheint als dritter Band der Schriftenreihe zum kirchlichen Datenschutzrecht. Wie die beiden ersten Bände ist auch diese Veröffentlichung über die Internetseite des Katholischen Datenschutzzentrums (Infothek ⇨ Publikationen) als PDF-Datei abrufbar.

[64] Ausführlich zur Konferenz der Diözesandatenschutzbeauftragten Steffen Pau zusammen mit Matthias Ullrich, Andreas Mündelein und Ursula Becker-Rathmair, Die Konferenz der Diözesandatenschutzbeauftragten – zwischen Unabhängigkeit und Zusammenarbeit, in: Justiz die Pflicht, Datenschutz die Kür – Festschrift zum 80. Geburtstag von Jupp Joachimski (Band 3 der Schriften zum kirchlichen Datenschutz des KDSZ), Dortmund 2022, S. 105–120; siehe auch die FAQ zur Konferenz im Abschnitt 4.1.3 im Jahresbericht 2021.

Abb.: Band 3 der Schriftenreihe zum kirchlichen Datenschutz
(Bild: Katholisches Datenschutzzentrum)

4.2.2 Handreichung zur Anbietung und Übergabe von Unterlagen an kirchliche Archive

Am 31.05.2022 hat das Katholische Datenschutzzentrum in Kooperation mit der Bundeskonferenz der kirchlichen Archive in Deutschland eine Handreichung veröffentlicht, die Fragen zur Anbietung und Übergabe von analogen und digitalen Unterlagen an die kirchlichen Archive beantworten und bisherige Unklarheiten beseitigen soll.[65]

Bei der Handreichung handelt es sich um einen Überblick über die Arbeit der Archive und welche Pflichten kirchliche Einrichtungen in Bezug auf die Anbietung und Übergabe ihrer Unterlagen haben. Dabei wird auch auf datenschutzrechtliche Aspekte im Umgang mit zu archivierenden Unterlagen, die personenbezogene Daten enthalten, eingegangen.

Abb.: Titelseite der Handreichung

[65] Die Handreichung kann auf der Internetseite des Katholischen Datenschutzzentrums im Bereich Infothek ⇨ Arbeits- und Formulierungshilfen abgerufen werden.

4.3 Beschlüsse und Veröffentlichungen der Konferenz der Diözesandatenschutzbeauftragten

4.3.1 Beschluss betreffend Dispositionsrecht zur Nichtanwendung von TOM

Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland

(Sitzung vom 15.06.2022)

Dispositionsrecht zur Einwilligung in die Nichtanwendung von technischen und organisatorischen Maßnahmen

Die Konferenz der Diözesandatenschutzbeauftragten hebt den Beschluss vom 19.09.2019 mit dem Titel *„Möglichkeit der Einwilligung in schlechtere technische und organisatorische Maßnahmen“* auf und ersetzt ihn durch:

In § 26 KDG sind die technischen und organisatorischen Maßnahmen geregelt, welche der Verantwortliche zu beachten hat. Dabei trifft ihn die Pflicht, diese zu implementieren, eine Absenkung dieser ist ihm nicht erlaubt.

Dem Sinn und Zweck dieser Pflicht nach ist es daher grundsätzlich nur möglich auf Betroffenenseite in das Nichtanwenden von einzelnen technischen und organisatorischen Schutzmaßnahmen gemäß § 6 Abs. 1 lit. b) bzw. § 11 Abs. 2 lit. a) KDG auf informierte Weise einzuwilligen. Diese Dispositionsbefugnis ist nur gegeben, 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 bringen würde. § 41 Abs. 1 KDG bleibt unberührt.

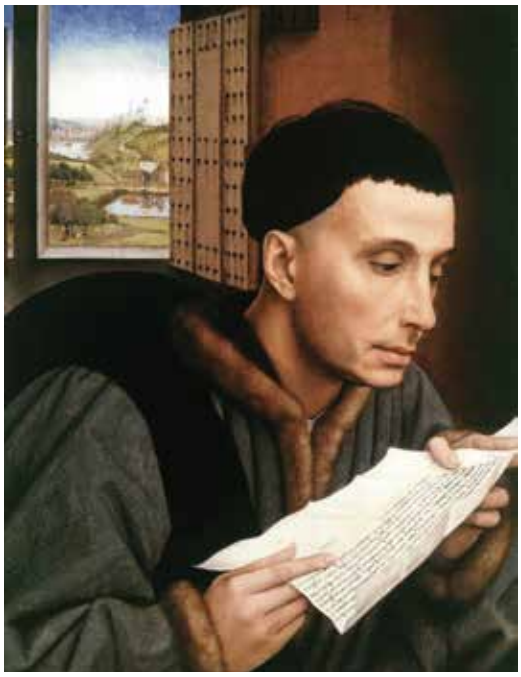
15.06.2022

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

Abkürzungsverzeichnis

beBPo	besonderes elektronisches Behördenpostfach
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGH	Bundesgerichtshof
CLPO	Civil Liberties Protection Officer (Beauftragter für den Schutz der bürgerlichen Freiheiten)
DDSB	Diözesandatenschutzbeauftragte/r
DOK	Deutsche Ordensobernkonferenz
DSA	Digital Services Act (Gesetz über digitale Dienste, GdD)
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EKD	Evangelische Kirche in Deutschland
EU	Europäische Union
EuGH	Europäischer Gerichtshof
HeilBerG	Heilberufegesetz NRW
IDSG	Interdiözesanes Datenschutzgericht
IfSG	Infektionsschutzgesetz
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
KDO	Anordnung über den kirchlichen Datenschutz
KDS-VwVfG	Gesetz über das Verwaltungsverfahren im kirchlichen Datenschutz
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
LAG	Landesarbeitsgericht
LDI	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfD	Landesbeauftragte/r für den Datenschutz
LG	Landgericht
NOYB	none of your business (Nichtregierungsorganisation, Europäisches Zentrum für digitale Rechte)
NRW	Nordrhein-Westfalen
OFL	Open Fonts License (Lizenz zur Lizenzierung von Schriftarten)
OWiG	Gesetz über Ordnungswidrigkeiten

PAO	Rahmenordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten (Personalaktenordnung)
PGP	Pretty Good Privacy (ein Programm zur Verschlüsselung und zum Unterschreiben von Daten)
PKI	Public-Key-Infrastruktur (System, das digitale Zertifikate ausstellen, verteilen und prüfen kann)
SELK	Selbständige Evangelisch-Lutherische Kirche
SGB	Sozialgesetzbuch
S/MIME	Secure / Multipurpose Internet Mail Extensions (Standard für die Verschlüsselung und das Signieren von E-Mails)
TOM	technische und organisatorische Maßnahmen
USA	Vereinigte Staaten von Amerika
VDD	Verband der Diözesen Deutschlands



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