Jahresbericht 2024

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.–31.12.2024

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

9. 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 01.01.2024–31.12.2024

Redaktionsschluss: 31.10.2025

Inhaltsverzeichnis

Vorwort

Die 2021 begonnene Evaluation des Gesetzes über den Kirchlichen Datenschutz (KDG) biegt auf die Zielgerade ein. Nach intensiver Arbeit der Facharbeitsgruppe konnte im Herbst 2024 ein Entwurf der Neufassung des KDG von der Arbeitsgruppe in das Beteiligungsverfahren gegeben werden. In diesem Verfahren haben neben den (Erz-)Diözesen auch verschiedenen Verbände und kirchliche Einrichtungen die Möglichkeit, zu den geplanten Änderungen im KDG Stellung zu nehmen und eigene Anregungen einzubringen. Damit steigt die Hoffnung, dass das Verfahren dann bis Ende 2025 beendet werden kann (vgl. Abschnitt 1.3.1). Die Novellierung des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (EKD) konnte im Berichtszeitraum bereits abgeschlossen werden (vgl. Abschnitt 1.4.2).

Andere gesetzliche Entwicklungen sind im Berichtszeitraum schon in Kraft getreten oder mussten erstmals angewendet werden. So wurden Ordnungen für den Betrieb einer Meldestelle nach dem Hinweisgeberschutzgesetz (HinSchG, vgl. Abschnitt 1.3.2) und weitere Regelungen zur Aufarbeitung der Fälle des Missbrauchs in der Kirche erlassen (vgl. Abschnitt 1.3.3). Auch die rasante Verbreitung von Anwendungen mit künstlicher Intelligenz schlug sich in neuen Regelungen nieder (vgl. Abschnitt 1.3.6).

Durch das vorzeitige Ende der Legislaturperiode des Deutschen Bundestages konnten einige gestartete Gesetzgebungsverfahren auf Bundesebene nicht mehr abgeschlossen werden und sind damit hinfällig geworden (vgl. Abschnitt 1.2.1). Damit blieb z. B. auch die Novellierung des Bundesdatenschutzgesetzes (BDSG) im Gesetzgebungsverfahren stecken, mit dem die Konferenz der Datenschutzaufsichten des Bundes und der Länder (DSK) gestärkt werden sollte.

Neben diesen gesetzlichen Entwicklungen gab es im Berichtszeitraum eine rege Rechtsprechung zum Datenschutz, die in diesem Bericht nur bruchstückhaft angerissen werden kann.

Die verschiedenen gesetzlichen Entwicklungen und die Rechtsprechung zeigen, dass im Datenschutzrecht vieles noch in Bewegung ist und es weiterhin spannend bleibt.

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

1 Entwicklungen im Datenschutzrecht

Das Datenschutzrecht bleibt ein sich ständig weiterentwickelnder Rechtsbereich. Dieser Abschnitt enthält eine auszugsweise Darstellung einiger Entwicklungen im Datenschutzrecht im Jahr 2024 – auf europäischer, nationaler und kirchlicher Ebene.

1.1 Entwicklungen auf Ebene der Europäischen Union

Im Rückblick auf das Jahr 2024 lassen sich wieder wichtige Entwicklungen im Bereich Datenschutz auf europäischer Ebene erkennen. Durch Entscheidungen des Europäischen Gerichtshofs und neue gesetzliche Vorgaben wurden einige Problemkreise geklärt. Einige der Vorhaben, die aus der Perspektive des Katholischen Datenschutzzentrums (KDSZ) im Bereich Datenschutz von Bedeutung sind, werden in diesem Abschnitt erläutert.

1.1.1 Auch die mündliche Übermittlung personenbezogener Daten kann in den Anwendungsbereich der DSGVO fallen

Am 07.03.2024 hat der Gerichtshof der Europäischen Union (EuGH) ein Urteil in der Rechtssache C-740/22 veröffentlicht. Gegenstand des Verfahrens war u. a. die Frage, ob die mündliche Weitergabe von Informationen als Verarbeitung i. S. d. Datenschutz-Grundverordnung (DSGVO) anzusehen ist.[1]

Der EuGH musste sich aufgrund einer Vorlagefrage eines finnischen Berufungsgerichts mit der Frage auseinandersetzen, ob eine mündliche Übermittlung der strafrechtlichen Vorgeschichte einer Person als Verarbeitung nach Art. 2 Abs. 1 und Art 4 Nr. 2 DSGVO zu werten ist. Im Kern ging es also um die Frage des Anwendungsbereiches der DSGVO auf mündliche Verarbeitungen. Grund für die Vorlage an den EuGH war das Begehren einer Prozesspartei im Ausgangsverfahren. Sie begehrte mündlich Auskunft über möglicherweise anhängige oder abgeschlossene Strafverfahren gegen eine natürliche Person aus dem Personenregister eines Gerichts, das Informationen über Strafurteile oder Delikte natürlicher Personen enthält. Problematisch war im vorliegenden Fall, ob der Verarbeitungsvorgang in Form der mündlichen Übermittlung den Anwendungsbereich der DSGVO eröffnet.

Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung ist gem. Art. 2 Abs. 1 DSGVO eröffnet, wenn es sich um eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten handelt sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Begriff der Verarbeitung wird in Art. 4 Abs. 2 DSGVO

[1] Über dieses Verfahren vor dem EuGH hat das KDSZ auch schon im Jahresbericht 2023 in Abschnitt 1.1.2 berichtet.

> **„Der EuGH hat den Begriff der Verarbeitung in seiner Entscheidung weit ausgelegt."**

definiert. Diese Definition legt auch die Offenlegung durch Übermittlung personenbezogener Daten als Verarbeitung fest. In der Definition ist allerdings nicht enthalten, ob die Übermittlung mündlich oder schriftlich geschehen muss. Daher ist fraglich, ob eine mündliche Übermittlung als nicht-automatisierte Verarbeitung mit Speicherung in einem Dateiensystem zu werten ist.

Der EuGH hat den Begriff der Verarbeitung in seiner Entscheidung weit ausgelegt. Auch mündliche Verarbeitungen fielen unter den Begriff der Verarbeitung aus Art. 4 Nr. 2 DSGVO, wenn die personenbezogenen Daten zumindest in einer Datei gespeichert sind oder gespeichert werden sollen. Für den vorgelegten Fall bedeutete dies, dass auch bei der mündlichen Übermittlung der strafrechtlichen Vorgeschichte einer Person der Anwendungsbereich der DSGVO eröffnet ist.

Hinweis für kirchliche Einrichtungen

In der Konsequenz können sich auch für katholische Einrichtungen Änderungen in ihrem Umgang mit mündlichen Verarbeitungen ergeben. Die Argumentation des EuGH kann auch auf die größtenteils deckungsgleichen Normen des Gesetzes über den Kirchlichen Datenschutz übertragen werden. Verantwortliche sollten zukünftig auch bei mündlichen Verarbeitungen genaustens auf die Einhaltung ihrer Verpflichtungen aus dem KDG achten.

1.1.2 Löschung von Taufbucheinträgen

Der belgische Märktegerichtshof hat dem Europäischen Gerichtshof erstmals Fragen zur Löschung personenbezogener Daten aus kirchlichen Taufbüchern vorgelegt. Hintergrund ist ein Verfahren, in dem das Bistum Gent gegen eine Entscheidung der belgischen Datenschutzaufsicht vorgeht. Diese hatte angeordnet, dass Einträge im Taufbuch – auf Antrag betroffener Personen – vollständig gelöscht werden müssen. Das Bistum verweigert, unter Hinweis auf kirchenrechtliche Bestimmungen, die Löschung und nimmt lediglich Randvermerke über den Kirchenaustritt vor.

Der Märktegerichtshof sieht zentrale Rechtsfragen zur Datenschutz-Grundverordnung als ungeklärt an, insbesondere das Verhältnis zwischen dem Recht auf Datenlöschung (Art. 17 DSGVO) und der Religionsfreiheit. Obwohl nationale Gerichte in anderen EU-Staaten (u. a. Irland, Slowenien, Frankreich) bisher zugunsten der Kirchen entschieden haben, hält der belgische Gerichtshof eine europarechtliche Klärung für notwendig.

Der EuGH soll nun über folgende Vorlagefragen entscheiden:[2]

- ob volljährige Personen ein Recht auf vollständige Löschung ihrer Daten aus einem Taufbuch haben,

[2] Die Fragen sind, unter Wahrung ihres Inhalts, aus Übersichtsgründen nur gekürzt dargestellt.

- ob das Recht auf Religionsfreiheit durch diesen Löschanspruch eingeschränkt wird,
- ob es Einfluss auf die Bewertung hat, dass das Taufregister ein physisches Buch ist und Einträge anderer Personen auf derselben Seite enthält,
- ob es relevant ist, dass das Taufbuch ein historisches Einzelstück darstellt und Daten auch aus Gründen des öffentlichen Interesses (Archiv, Forschung) gespeichert werden,
- ob anstelle einer Löschung ein Randvermerk über den Kirchenaustritt ausreicht, um das Löschrecht zu erfüllen.

Die Entscheidung des EuGH könnte grundsätzliche Bedeutung für den kirchlichen Datenschutz in der gesamten EU haben und das Verhältnis von Betroffenenrechten zu institutioneller Religionsfreiheit klarstellen.

In Deutschland sind die Gerichte bisher vor dem Hintergrund der verfassungsrechtlich garantierten kirchlichen Selbstbestimmung der Argumentation der katholischen Kirche gefolgt, dass die Taufe als Sakrament nicht durch einen Kirchenaustritt gelöscht werden kann.[3] Damit bleibt die Eintragung in das Taufbuch als Dokumentation des Sakraments der Taufe auch nach einem Kirchenaustritt notwendig.

Der Vatikan hat im April 2025 in einer erklärenden Note „über das Verbot der Löschungen im Taufregister der Pfarrei" theologisch und kirchenrechtlich begründet, warum ein Eintrag im Taufregister nicht gelöscht werden darf.[4]

1.1.3 Befugnisse einer Aufsichtsbehörde zur Anordnung der Datenlöschung

Auf die Vorlagefrage eines ungarischen Gerichts hin, hat der Europäische Gerichtshof die Anordnungsbefugnisse nationaler Aufsichtsbehörden konkretisiert. In seiner Entscheidung vom 14.03.2024 (Az. C-46/23) hat der EuGH festgestellt, dass Aufsichtsbehörden gegenüber Verantwortlichen und deren Auftragsverarbeitern Löschungen von personenbezogenen Daten anordnen können, wenn diese nicht von der betroffenen Person beantragt gewesen sind.

Die ungarische Datenschutzbehörde ordnete die Löschung unrechtmäßig verarbeiteter Daten auch ohne Antrag der betroffenen Person an. Die von der Anordnung betroffene Verwaltung hielt dies für unzulässig und klagte. Während das oberste ungarische Gericht der Verwaltung zustimmte, hob das ungarische Verfassungsgericht dieses Urteil auf: Es erklärte die Datenschutzaufsichtsbehörde – gestützt auf eine Stellungnahme des Europäischen Datenschutzausschusses (EDSA) – für

[3] Vgl. z. B. VGH Bayern, Beschluss vom 16.02.2015 (Az. 7 ZB 14.357); VG München, Urteil vom 19.12.2013 (Az. M 22 K 12.106).

[4] Siehe https://press.vatican.va/content/salastampa/it/bollettino/pubblico/2025/04/17/0259/00486.html (Schreiben in italienischer Sprache). Zur Absicherung dieser Auslegung im kirchlichen Datenschutzgesetz soll im Rahmen der Novellierung des KDG (Stand der Beratungen zum Zeitpunkt der Erstellung des Berichts) eine entsprechende Regelung in das novellierte KDG eingefügt werden.

befugt, Löschungen auch von Amts wegen nach Art. 58 Abs. 2 DSGVO anzuordnen. Das vorlegende Gericht hatte allerdings immer noch Zweifel an der Befugnis der Behörde, entgegen eines (mutmaßlichen) Interesses der betroffenen Person, die Löschung von personenbezogenen Daten anordnen zu können.

„Der EuGH betont, dass nationale Datenschutzbehörden nach Art. 57 DSGVO die Anwendung der DSGVO überwachen und nötigenfalls Abhilfen ergreifen müssen."

Der EuGH betont, dass nationale Datenschutzbehörden nach Art. 57 DSGVO die Anwendung der DSGVO überwachen und nötigenfalls Abhilfen ergreifen müssen. Art. 58 Abs. 2 DSGVO erlaubt ihnen dabei teils Maßnahmen nur auf Antrag, teils auch von Amts wegen – darunter auch Löschungsanordnungen (Art 58 Abs. 2 lit. d) und g) DSGVO). Art. 17 Abs. 1 DSGVO enthält zwei eigenständige Löschungsfälle, sodass Behörden auch ohne Antrag tätig werden können, besonders wenn Betroffene gar nicht wissen, dass ihre Daten verarbeitet werden. Gestützt wird dies durch die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) und den Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 lit. a) DSGVO), wonach der Verantwortliche selbst für rechtmäßige Verarbeitung sorgen muss. Diese Grundsätze gelten unabhängig davon, ob Daten direkt oder über Dritte erhoben wurden.

Hinweis für kirchliche Einrichtungen

Für katholische Einrichtungen dürfte diese Entscheidung nur wenig verändern. In Deutschland war die Frage der Anordnung von Amts wegen, zumindest bisher, nicht umstritten. Verantwortliche sollten aber trotzdem beachten, dass Aufsichtsbehörden nicht an die Begehren von Beschwerdeführern gebunden sind.

1.1.4 Europäische Union verabschiedet Verordnung zur künstlichen Intelligenz

Die Europäische Union hat mit der Verordnung (EU) 2024/1689[5] einen wegweisenden Regulierungsrahmen für künstliche Intelligenz (KI) geschaffen. Die KI-Verordnung trat am 01.08.2024 in Kraft und soll ab dem 02.08.2026 vollständig angewendet werden.

Die Verordnung verfolgt u. a. das Ziel, „vertrauenswürdige KI" zu fördern, die die Grundrechte der EU-Bürger schützt – darunter Demokratie, Rechtsstaatlichkeit und Umweltschutz. Die VO verfolgt dabei einen risikobasierten Ansatz und enthält besondere Regelungen für „verbotene Praktiken" (Art. 5 KI-VO) und „Hochrisiko-KI-Systeme" (Art. 6 KI-VO).

Wie schon das KDG legt auch die KI-VO besonderen Wert auf Transparenz. So ist vorgeschrieben, dass Menschen erkennen können müssen, dass sie z. B. mit einem KI-gestützten Chatbot interagieren (Art. 50 Abs. 1 S. 1 KI-VO). Für manipulierte Inhalte, sog. Deepfakes, gilt zudem eine Offenbarungspflicht (Art. 50 Abs. 4 KI-VO).

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401689

Für Hochrisiko-KI-Systeme normiert die Verordnung besondere Anforderungen hinsichtlich Validierung, Konformitätsprüfung, Datenqualitätsanforderungen, menschliche Aufsicht und laufendes Monitoring.

Hinweis für kirchliche Einrichtungen

Bei der Verarbeitung personenbezogener Daten mithilfe von KI-gestützten Systemen bleibt das KDG auch weiterhin neben der KI-VO anwendbar. Da gemäß Art. 2 Abs. 7 KI-VO die KI-VO nicht die Vorschriften der DSGVO berührt, bleiben diese anwendbar. Damit ist im kirchlichen Bereich auch die Anwendung der Normen des KDG für datenschutzrechtliche Sachverhalte aus dem Anwendungsbereich der KI-VO zu prüfen. Die kirchlichen Stellen sollten hier aber die Diskussion zur Umsetzung der KI-Verordnung zur Klärung evtl. noch offener Fragen verfolgen.

Außerdem sollten die kirchlichen Einrichtungen Wert auf die Vermittlung von KI-Kompetenz gemäß Art. 4 KI-VO legen, da dies die Beschäftigten über Chancen und Risiken der KI-Nutzung informiert und sensibilisiert.

1.1.5 EuGH äußert sich zum "berechtigten Interesse"

Der Europäische Gerichtshof hat am 04.10.2024 im Verfahren C-621/22 (Koninklijke Nederlandse Lawn Tennisbond vs. Autoriteit Persoonsgegevens) eine wichtige Entscheidung zur Auslegung von „berechtigten Interessen“ nach Art. 6 Abs. 1 lit. f) DSGVO gefällt.

Der niederländische Tennisverband hatte personenbezogene Daten seiner Mitglieder (u. a. Name, Adresse) gegen Entgelt an Sponsoren (einen Sportwarenhändler und einen Glücksspielanbieter) ohne vorherige Einwilligung der Mitglieder weitergegeben. Die niederländische Datenschutzaufsichtsbehörde stufte die kommerzielle Weitergabe solcher Daten ohne Einwilligung als nicht zulässig ein.

In dem anschließenden Gerichtsverfahren sollte der EuGH daher die Frage beantworten, wie der Begriff des „berechtigten Interesses“ im Sinne des Art. 6 Abs. lit. f) DSGVO auszulegen ist. So bestand Streit darüber, ob zum „berechtigten Interesse“ nur gesetzlich festgelegte Interessen gehören oder jedes Interesse, sofern es nicht einem Gesetz zuwiderläuft.

Der EuGH stellt in seiner Entscheidung klar, dass auch rein wirtschaftliche beziehungsweise kommerzielle Interessen grundsätzlich „berechtigte Interessen“ im Sinne von Art. 6 Abs. 1 lit. f) DSGVO sein können. Um sich auf das „berechtigte Interesse“ zu stützen, müssen dabei drei Voraussetzungen erfüllt sein:

- Das verfolgte Interesse muss rechtskonform sein.
- Die Verarbeitung muss notwendig für dieses Interesse sein – es darf kein ebenso wirksames, weniger eingreifendes Mittel geben.

- Bei der Abwägung müssen die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden und dürfen nicht überwiegen.

Das Gericht weist darauf hin, dass im vorliegenden Fall genau zu prüfen sei, ob die Mitglieder des Verbandes vernünftigerweise vorhersehen konnten, dass ihre Daten gegen Entgelt an kommerziell handelnde Sponsoren weitergegeben werden. Außerdem sei bei der Interessenabwägung zu beachten, dass die Datenübermittlung an einen Glücksspielanbieter sich auf die Betroffenen unter dem Gesichtspunkt der Entwicklung einer Spielsucht nachteilig auswirken könne.

Der EuGH weist die Auslegung zurück, dass ein berechtigtes Interesse gesetzlich normiert sein müsse. So sei es nicht erforderlich, dass das Interesse in einem Gesetz verankert ist, solange es „gesetzlich zulässig" ist.

Das vorlegende Gericht muss daher sorgfältig prüfen, ob weniger eingreifende Maßnahmen möglich sind. Das Gericht muss ferner bei der Bewertung auch die „vernünftigen Erwartungen" der Betroffenen sowie das Ausmaß und die Auswirkungen der Datenverarbeitung berücksichtigen.

„Der EuGH weist die Auslegung zurück, dass ein berechtigtes Interesse gesetzlich normiert sein müsse. So sei es nicht erforderlich, dass das Interesse in einem Gesetz veranktert ist, solange es ‚gesetzlich zulässig' ist."

Hinweis für kirchliche Einrichtungen

Diese Entscheidung ist auch für den kirchlichen Bereich von Bedeutung, da § 6 Abs. 1 lit. g) KDG von seinem Wortlaut im Wesentlichen dem Art. 6 Abs. 1 lit. f) DSGVO entspricht.

Auch die kirchlichen Einrichtungen können daher Verarbeitungen personenbezogener Daten auch bei rein wirtschaftlichen beziehungsweise kommerziellen Interessen auf ein „berechtigtes Interesse" im Sinne von § 6 Abs. 1 lit. g) KDG stützen, soweit sie die Anforderungen des EuGH an die Prüfung eines „berechtigten Interesses" erfüllen. Es ist aber nicht ausreichend, ein berechtigtes Interesse nur zu behaupten – es muss eine nachvollziehbare Prüfung stattfinden, ob die Verarbeitung wirklich notwendig ist und die Rechte der Betroffenen gewahrt sind. Diese Prüfung ist nachvollziehbar zu dokumentieren.

1.1.6 Aufgaben der Aufsichtsbehörde

In einer weiteren Entscheidung hat der EuGH die Aufgaben der Aufsichtsbehörden konkretisiert. In der Rechtssache C-768/21 ging es darum, ob eine Aufsichtsbehörde bei einem festgestellten Datenschutzverstoß (eigene) Abhilfemaßnahmen ergreifen muss, oder ob sie durch den Verantwortlichen ergriffene Maßnahmen als ausreichend und abschließend bewerten kann.

Im ursächlichen Streitfall griff eine Sparkassenmitarbeiterin unbefugt auf Kundendaten zu. Die Sparkasse meldete den Vorfall der Aufsichtsbehörde, informierte aber den Kunden nicht, da sie kein hohes Risiko sah und disziplinarische Maßnahmen ergriff. Der Kunde beschwerte sich nach Art. 77 DSGVO und verlangte eine Geldbuße gegen die Spar-

kasse. Die Aufsichtsbehörde verhängte kein Bußgeld, da, so die Aufsicht, kein hohes Risiko für die Rechte des Kunden bestanden und keine Weitergabe oder missbräuchliche Nutzung der Daten vorgelegen habe und die Mitarbeiterin bereits disziplinarisch belangt worden war.

Der EuGH entschied: Aufsichtsbehörden sind verpflichtet, bei Datenschutzverstößen geeignete Abhilfemaßnahmen nach Art. 58 Abs. 2 DSGVO zu ergreifen, wenn dies erforderlich und verhältnismäßig ist. Sie müssen jedoch nicht zwingend Geldbußen verhängen. Ein Untätigbleiben ist möglich, wenn der Verstoß bereits abgestellt wurde, geeignete Maßnahmen ergriffen wurden und keine Wiederholung droht. Die DSGVO erlaubt ausdrücklich, bei geringfügigen Verstößen oder unverhältnismäßiger Belastung auf eine Geldbuße zu verzichten.

„Aufsichtsbehörden sind verpflichtet, bei Datenschutzverstößen geeignete Abhilfemaßnahmen … zu ergreifen, wenn dies erforderlich und verhältnismäßig ist."

1.1.7 Gestaltung von Cookie-Bannern

Cookies sind kleine Textdateien, die von Internetseiten oder digitalen Diensten auf den Geräten der Internetseitenbesucher oder Dienstkonsumenten gespeichert werden. Sie dienen z. B. dazu, den Benutzer zu erkennen, um Einstellungen zu speichern oder um Statistiken zu erstellen.

Unterschieden werden Cookies in technisch notwendige Cookies und in technisch nicht notwendige Cookies. Technisch notwendige Cookies werden beispielsweise für die Warenkorbfunktion in Onlineshops oder die Spracheinstellung einer Homepage verwendet. Diese Cookies dürfen ohne eine Einwilligung der Nutzer auf dem Gerät abgespeichert und verwendet werden. Die Nutzer müssen über die Verwendung von Cookies gemäß den Informationspflichten aus dem KDG informiert werden. Die Informationspflichten werden regelmäßig über die Datenschutzhinweise der besuchten Internetseite realisiert.

Muss für das Setzen eines Cookies und der damit anschließenden Verarbeitung von personenbezogenen Daten eine Einwilligung vom Nutzer eingeholt werden, wird dies regelmäßig über Einwilligungsbanner, sogenannte Cookie-Banner, realisiert. Das Einwilligungsbanner erscheint in der Regel beim ersten Besuch der Internetseite, unabhängig davon, ob die Startseite oder eine Unterseite durch den Nutzer aufgerufen wird. Um eine informierte Einwilligung des Nutzers zu erheben, muss vor der Einwilligung eine konkrete Information über die einwilligungsbedürftige Verarbeitung gegeben werden. Durch einen Link im Einwilligungsbanner auf die entsprechenden Datenschutzhinweise wird dieser Informationspflicht in der Regel nachgekommen. Durch ein Einwilligungsbanner darf der Zugriff auf Impressum und Datenschutzhinweise nicht blockiert werden. Bevor durch eine aktive, zustimmende Handlung der Verarbeitung zugestimmt wird, dürfen keine Cookies auf das Gerät des Nutzers gespeichert oder Skripte ausgeführt werden.

Sobald der Nutzer seine Einwilligung durch eine aktive Handlung erteilt hat, darf mit dem Setzen der Cookies und der ggf. folgenden Verarbeitung von personenbezogenen Daten begonnen werden. Die aktive Handlung wird z. B. durch das Setzen eines Hakens ausgeführt. Vorausgewählte Checkboxen erfüllen nicht die Voraussetzungen für eine wirksame, informierte Einwilligung.

Um eine wirksame, informierte Einwilligung des Nutzers zu erhalten, muss es für den Nutzer ebenso möglich sein, der Verarbeitung von personenbezogenen Daten und damit auch dem Setzen von Cookies nicht zuzustimmen. Das Ablehnen der Verarbeitung und dem damit verbundenen Setzen von Cookies muss genauso einfach sein wie die Zustimmung. Die EDSA Cookie Banner Taskforce[6] geht in ihrem Bericht davon aus, dass das Gesetz keine bestimmte Art der Darstellung von Auswahlmöglichkeiten vorschreibt.

In einem Einwilligungsbanner ist es daher wichtig, dass die Alternative zur Zustimmung durch den Nutzer wahrgenommen werden kann. Die französische Datenschutzaufsicht CNIL[7] und auch die Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder (Datenschutzkonferenz – DSK)[8] haben sich zu diesen unter dem Begriff „Nudging" zusammengefassten Techniken geäußert. Als Techniken, die möglicherweise die Wirksamkeit einer Einwilligung aufheben, werden die folgenden genannt:

Die Ablehnen-Option

- wird in Form eines anklickbaren Links dargestellt, dessen Farbe, Schriftgröße und Schriftstil die Annehmen-Option unverhältnismäßig stark hervorhebt.
- ist so in den Text eingebettet, dass sie nicht ohne Weiteres erkennbar ist.
- ist ohne einen angemessenen Abstand neben anderen Absätzen platziert, um sie visuell nicht von anderen Optionen unterscheiden zu können.
- wird im Einwilligungsbanner nur ein Mal und in nicht expliziter Form angeboten, während die Zustimmen-Option mehrfach angezeigt wird.

Die Verwendung der hier vorgestellten Nudging-Techniken muss nicht zwingend die Wirksamkeit der Einwilligung aufheben, deutet aber stark darauf hin. Einwilligungsbanner werden daher immer in Einzelfallprüfungen analysiert und bewertet.

In aktuellen Browsern kann der Nutzer einstellen, wie mit Cookies umgegangen werden soll. Cookies können beispielsweise durch den Browser immer abgelehnt werden oder es ist möglich, alle Cookies beim Beenden des Browsers zu löschen.

„In aktuellen Browsern kann der Nutzer einstellen, wie mit Cookies umgegangen werden soll. Cookies können beispielsweise ... immer abgelehnt werden oder es ist möglich, alle Cookies beim Beenden des Browsers zu löschen."

[6] EDPB Cookie Banner Taskforce: https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf
[7] CNIL zu Ablehnen-Funktionen: https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers
[8] DSK OH Telemedien: https://www.datenschutzkonferenz-online.de/media/oh/20221130_OH_Telemedien_2021_Version_1_1.pdf

1.1.8 Der EuGH äußert sich zu den Grenzen von Betriebsvereinbarungen

In seinem Urteil vom 19.12.2024 (Rs. C-65/23) hat sich der Europäische Gerichtshof zu datenschutzrechtlichen Rahmenbedingungen von Betriebsvereinbarungen geäußert. Das Gericht führt in seinem Urteil aus, dass nationale Rechtsvorschriften über die Verarbeitung personenbezogener Daten für die Zwecke von Beschäftigungsverhältnissen nicht nur die in Art. 88 Abs. 2 DSGVO genannten Kriterien erfüllen, sondern dass auch die allgemeinen Grundsätze des Datenschutzes aus den Art. 5, Art. 6 Abs. 1 und Art. 9 Abs. 1 und 2 DSGVO von diesen Regelungen eingehalten werden müssen.

Nationale Rechtsvorschriften über die Verarbeitung personenbezogener Daten für die Zwecke von Beschäftigungsverhältnissen können also nur dann als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten herangezogen werden, wenn sie die Anforderungen der DSGVO erfüllen.

Die Datenverarbeitung ist daher auch in diesen Regelungen auf das für den Zweck absolut notwendige Maß zu beschränken. Übermäßige oder pauschale Datenverarbeitungen sind nicht möglich. Die ausgehandelte Regelung muss die Rechte der Beschäftigten ausreichend schützen und nachvollziehbar regeln.

Hinweis für kirchliche Einrichtungen

Die Ausführungen des EuGH zu Art. 88 DSGVO und den Rahmenbedingungen für Betriebsvereinbarungen sind auch auf das KDG und die kirchliche Mitbestimmung übertragbar.

Kirchliche Einrichtungen müssen ihre Dienstvereinbarungen auf die Einhaltung sämtlicher datenschutzrechtlicher Vorgaben überprüfen und erforderlichenfalls anpassen.

Dienstvereinbarungen müssen hinreichend klare und präzise Regelungen zur Datenverarbeitung enthalten. Dazu gehören insbesondere die Art der verarbeiteten Daten, der konkrete Zweck der Verarbeitung, die betroffenen Beschäftigtengruppen und eine genaue Beschreibung der Datenverarbeitungen.

Die datenschutzrechtlichen Prinzipien der Transparenz, Verhältnismäßigkeit und Zweckbindung müssen dabei beachtet und umgesetzt werden.

1.2 Datenschutzrechtliche Entwicklungen in der Bundesrepublik Deutschland

Im Berichtsjahr gab es nicht nur auf europäischer Ebene datenschutzrechtliche Entwicklungen, sondern auch auf nationaler Ebene, von denen in diesem Abschnitt nur einige Themen dargestellt werden können.

1.2.1 Nicht-verabschiedete gesetzliche Initiativen auf Bundesebene

Im Berichtszeitraum 2024 waren mehrere gesetzliche Initiativen zum Datenschutz im Bundestag in der Beratung. Durch die vorzeitigen Neuwahlen zum Deutschen Bundestag im Februar 2025 konnten einige der Vorhaben aber nicht mehr vor Ende der – verkürzten – Wahlperiode das Gesetzgebungsverfahren bis zum Ende durchlaufen. Dadurch sind die Initiativen aufgrund der Diskontinuität der Beratungsgegenstände des Bundestages am Ende einer Wahlperiode ohne Ergebnisse erledigt worden. Die Vorhaben müssten – sofern der neugewählte Bundestag sie wieder aufgreifen wollte – erneut als Gesetzentwurf in den Bundestag eingebracht werden.

Von den so erledigten Gesetzgebungsvorhaben sollen hier nur drei Initiativen genannt werden, die datenschutzrechtlichen Bezug hatten:

Novellierung des Bundesdatenschutzgesetzes
Im Jahresbericht 2023 hatte das Katholische Datenschutzzentrum schon auf den Referentenentwurf zur Novellierung des Bundesdatenschutzgesetzes in dieser Sache hingewiesen.[9] Auf Basis dieses Entwurfes wurde im Frühjahr 2024 ein Gesetzentwurf in den Bundestag eingebracht, der unter anderem vorsah, die Datenschutzkonferenz als Gremium der unabhängigen Datenschutzaufsichten des Bundes und der Länder zu stärken.[10] Mit diesem Schritt der Institutionalisierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und verbindlicheren Beschlüssen dieses Gremiums sollte auch eine einheitlichere Auslegung des Datenschutzrechts durch alle staatlichen Datenschutzaufsichtsbehörden erreicht werden.

Ob dieses Ansinnen in der neuen Wahlperiode noch einmal in dieser Form aufgegriffen wird, erscheint derzeit fraglich, da im neuen Koalitionsvertrag 2025 der Bundesregierung eher eine Zentralisierung der Zuständigkeiten für den nichtöffentlichen Bereich bei der Bundesdatenschutzbeauftragten in den Blick genommen wird und darüber eine einheitliche Auslegung der gesetzlichen Vorgaben erreicht werden soll. Gegen diese Zentralisierungstendenzen gibt es nicht nur von den Landesdatenschutzbeauftragten heftigen Widerstand.

Klarstellung im Bundesdatenschutzgesetz zur aufsichtlichen Zuständigkeit für öffentlich-rechtlich verfasste Kirchen, Religionsgemeinschaften und weltanschauliche Gemeinschaften ohne eigene Datenschutzaufsicht
In der Stellungnahme vom 22.03.2024 zum vorgenannten Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes[11] griff der Bundesrat eine Problematik auf, die zuvor in Fachkreisen angesprochen worden war und auch in einem Urteil des VG Hannover[12] relevant wurde.

Bei Kirchen, Religionsgemeinschaften und weltanschaulichen Gemeinschaften, die öffentlich-rechtlich verfasst sind und keine eigenen

[9] Siehe Abschnitt 1.2.2 im Jahresbericht 2023.
[10] Siehe Bundestags-Drucksache 20/10859 vom 27.03.2024.
[11] Siehe den Gesetzentwurf (Bundesrats-Drucksache 72/24 vom 09.02.2024) und die Stellungnahme im Beschluss (Bundesrats-Drucksache 72/24 (B) vom 22.03.2024).
[12] Urteil des VG Hannover vom 30.11.2022, Az. 10 A 1195/21.

Datenschutzregelungen im Sinne von Art. 91 DSGVO erlassen haben, ist offenbar ungeklärt, welche Datenschutzaufsichtsbehörde zuständig ist. In diesen Fällen greift mangels eigener kirchlicher Datenschutzregelungen Art. 91 Abs. 2 DSGVO nicht, sodass eine staatliche Datenschutzaufsicht zuständig ist.

Die öffentlich-rechtlich verfassten Kirchen, Religionsgemeinschaften und weltanschaulichen Gemeinschaften „sind keine öffentlichen Stellen des Bundes oder des Landes gemäß § 2 Absatz 1 bis 3 BDSG, da sie insbesondere nicht der Aufsicht des Landes unterstehen. Sie sind auch keine nichtöffentlichen Stellen im klassischen Sinne gemäß § 2 Absatz 4 BDSG, da sie keine juristischen Personen „des privaten Rechts" sind", wie der Bundesrat in seiner Drucksache ausführt.[13] Der Bundesrat hatte daher vorgeschlagen, dem § 2 BDSG folgenden Absatz anzufügen: „(6) Kirchen, Religionsgemeinschaften und weltanschauliche Gemeinschaften in der Rechtsform einer Körperschaft des öffentlichen Rechts gelten, soweit sie nicht nach Maßgabe von Artikel 91 der Verordnung (EU) 2016/679 eigene Regelungen zum Schutz natürlicher Personen bei der Verarbeitung von Daten erlassen haben, als nichtöffentliche Stellen im Sinne dieses Gesetzes."[14]

Änderung des Bundesmeldegesetzes

Mit dem Entwurf eines Dritten Gesetzes zur Änderung des Bundesmeldegesetzes (3. BMGÄndG)[15] sollte unter anderem die Regelung des § 42 Abs. 5 Bundesmeldegesetz gestrichen werden.

Diese Regelung sieht vor, dass eine Datenübermittlung an eine öffentlich-rechtliche Religionsgemeinschaft nur zulässig ist, wenn sichergestellt ist, dass beim Empfänger ausreichende Maßnahmen zum Datenschutz getroffen sind, was durch eine Behörde des Bundeslandes festzustellen ist.

In der Gesetzesbegründung führt die Bundesregierung, die den Gesetzentwurf eingebracht hat, aus, dass es für diese Regelung keinen Bedarf mehr gebe. „Gemäß Artikel 91 der Datenschutz-Grundverordnung dürfen Kirchen und religiöse Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung angewendet haben, diese Regeln weiter anwenden, wenn sie mit der DSGVO in Einklang gebracht werden. In Deutschland sind die Voraussetzungen des Artikels 91 der DSGVO durch die römisch-katholische und die evangelische Kirche erfüllt. Beide Kirchen haben vor Inkrafttreten der DSGVO ihr bestehendes Datenschutzrecht an die Vorgaben der DSGVO angepasst, sodass die in § 42 Absatz 5 vorgesehene behördliche Feststellung insoweit nicht erforderlich ist."[16]

Die Bundesregierung beschreibt mit der Begründung im Gesetzentwurf die datenschutzrechtlichen Regelungen der katholischen Kirche als im Einklang mit der DSGVO und hält damit fest, dass die Anforderungen von Art. 91. Abs. 1 DSGVO erfüllt sind.

[13] Bundesrats-Drucksache 72/24 (B), Seite 2.
[14] Bundesrats-Drucksache 72/24 (B), Seite 2.
[15] Bundestags-Drucksache 20/12349 vom 24.07.2024.
[16] Bundestags-Drucksache 20/12349 vom 24.07.2024, Seite 20.

1.2.2 Namensnennung des betrieblichen Datenschutzbeauftragten in den Datenschutzhinweisen nicht notwendig

Der Bundesgerichtshof (BGH) hat mit seinem Urteil vom 14.05.2024 (Az. VI ZR 370/22) wichtige Fragen zum Auskunftsanspruch nach Art. 15 der DSGVO entschieden.

Die Klägerin hatte gegenüber einem Verantwortlichen einen umfassenden Auskunftsanspruch geltend gemacht. Sie begehrte nach Art. 15 DSGVO unter anderem Auskunft über alle gespeicherten personenbezogenen Daten, Speichermedien, Empfänger, technisch-organisatorische Maßnahmen, Profiling-Algorithmen und Löschungen.

Die Vorinstanzen hatten der Klage teilweise stattgegeben, jedoch nicht alle geforderten Informationen als erforderlich für eine Auskunft anerkannt.

In der Revision rügte die Klägerin insbesondere, dass der Datenschutzbeauftragte entgegen Art. 13 Abs. 1 lit. b) DSGVO nicht namentlich genannt worden sei, und beanstandete die Unvollständigkeit der Auskunft.

Der BGH vertritt die Ansicht, dass bei der Mitteilung der Kontaktdaten des Datenschutzbeauftragten nicht zwingend dessen Name genannt werden muss. Entscheidend sei, dass die Erreichbarkeit der zuständigen Stelle gewährleistet sei. Der BGH legt dabei den Wortlaut der Vorschrift, den Sinn und Zweck der Norm als auch die Systematik der DSGVO seiner Entscheidung zugrunde.

Hinweis für kirchliche Einrichtungen

Diese Entscheidung ist von hoher Relevanz für die kirchliche Praxis, da der Wortlaut des in diesem Verfahren streitgegenständlichen Art. 13 Abs. 1 lit. b) DSGVO sich wortidentisch im § 15 Abs. 1 lit. b) KDG wiederfindet. So bietet die hier besprochene Entscheidung all denjenigen Rechtssicherheit, die auch bisher schon auf die Nennung des Namens des betrieblichen Datenschutzbeauftragten (bDSB) verzichtet haben.

1.2.3 Zur Ermessensausübung durch die Datenschutzaufsicht, wie sie Eingaben bearbeitet und abschließt und zur Erteilung einer Negativauskunft

In einem Verfahren am VG Ansbach[17] war über die Frage zu entscheiden, welchen Spielraum die Datenschutzaufsicht hat, ob und wie sie einen an sie herangetragenen Sachverhalt bearbeitet beziehungsweise sanktioniert.

[17] VG Ansbach, Urteil vom 12.06.2024 – Az. AN 14 K 20.00941 (https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2024-N-20312).

Die Klägerin nahm 2020 an einem Seminar teil, dessen Veranstalter (Beigeladener) versehentlich eine Teilnehmerliste mit personenbezogenen Angaben versandte. Sie verlangte daraufhin vom Veranstalter Auskunft über die sie betreffenden personenbezogenen Daten gem. Art. 15 Abs. 1 DSGVO, erhielt jedoch keine vollständige Antwort. Nach einer Beschwerde bei der zuständigen Datenschutzaufsicht forderte diese den Verantwortlichen zwar zur Auskunft auf, sah aber nach dessen Mitteilung über eine angebliche Löschung der Daten von weiteren Maßnahmen ab und beendete das Verfahren durch eine Abschlussmitteilung. Die Klägerin klagte auf ein förmliches Einschreiten der Aufsichtsbehörde.

In der Entscheidung wird sowohl die materiell-rechtliche Frage einer Negativauskunft als auch die verfahrensrechtliche Frage der Ermessenausübung der Aufsicht und des Prüfungsmaßstabes der Gerichte angesprochen.

Verfahrensrechtliche Aspekte der Entscheidung
Das Gericht stellt in der Entscheidung fest, dass ein rechtsverbindlicher Beschluss einer Aufsichtsbehörde einer vollständigen inhaltlichen Überprüfung durch ein Gericht unterliegt. Das bedeutet, dass sowohl die Ermessensausübung, als auch der Ermessensspielraum der Behörde einer Prüfung unterfällt.

Je nach Schwere des geltend gemachten Verstoßes gegen datenschutzrechtliche Vorschriften, kann das Ermessen hinsichtlich des „Ob" des Einschreitens der Behörde (Entschließungsermessen) auf Null reduziert sein. Maßgeblich ist dabei, ob das Ergreifen einer Maßnahme durch die Behörde die einzig rechtmäßige Handlungsmöglichkeit darstellt. Dies kann der Fall sein, wenn der Verstoß gegen datenschutzrechtliche Vorschriften feststeht beziehungsweise sich aufdrängt und schwerwiegend in die Rechte des Betroffenen eingreift. Die entscheidenden Kriterien zur Bewertung eines Verstoßes orientieren sich dabei am Erwägungsgrund 148 DSGVO.

Stellt sich also heraus, dass ein Verstoß gegen ein zentrales Betroffenenrecht der DSGVO – im vorliegenden Fall das Auskunftsrecht nach § 15 DSGVO – vorliegt, ist eine Ermessensreduzierung auf Null hinsichtlich des Entschließungsermessens anzunehmen. Das bedeutet, dass die Datenschutzaufsichtsbehörde verpflichtet ist, mittels der Abhilfebefugnisse des § 58 Abs. 2 DSGVO tätig zu werden. Dieses Tätigwerden muss klar und eindeutig als formale Abhilfemaßnahme formuliert werden. Nur so kann sichergestellt werden, dass die Rechte der Betroffenen gewahrt und künftige Rechtsverstöße vom Verantwortlichen verhindert werden. Dementsprechend ist auch der Wortlaut der behördlichen Maßnahme so zu wählen, dass sich der Adressat der Verbindlichkeit der Anweisung bewusst wird. Die bloße Formulierung als Bitte, das Fehlen des Wortes „Anweisung" oder gar die fehlende Bescheidform inklusive Rechtsbehelfsbelehrung, machen die Umsetzung der Abhilfebefugnisse unverbindlich und werden der Ermessensreduzierung auf Null hinsichtlich des behördlichen Einschreitens nicht gerecht.

Dies könnte in der Praxis dazu führen, dass Aufsichtsbehörden künftig verstärkt mit formalen Verwarnungen oder Anweisungen agieren anstatt sich auf bloße Hinweise an den Verantwortlichen zu beschränken. Dabei wird von den Aufsichtsbehörden ein Balanceakt erwartet,

denn die jeweilige Aufsichtsbehörde hat bei der Anwendung ihrer Abhilfebefugnisse das Gebot einer doppelten Rücksichtnahme zu beachten: Einerseits ist sie verpflichtet, wirksam auf festgestellte Datenschutzverstöße zu reagieren, um die Effektivität der Betroffenenrechte zu gewährleisten; andererseits muss sie die Verhältnismäßigkeit ihres Einschreitens wahren und darf den Verantwortlichen nicht übermäßig belasten.

Materiell-rechtliche Aspekte der Entscheidung
Gemäß § 15 Abs. 1 DSGVO hat eine betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet. In Art. 15 Abs. 1 DSGVO werden unter den Buchstaben a) bis h) die Art der Informationen, über die Auskunft gegeben werden soll, näher aufgeführt. Die Auskunft ist dabei gegenüber der betroffenen Person zu erteilen und nicht lediglich gegenüber der Datenschutzaufsicht.

„Einem Auskunftsersuchen kann auch durch Negativauskunft nachgekommen werden. Selbst dann, wenn keine Datenverarbeitung stattfindet, hat der Betroffene einen Anspruch darauf, dass ihm dies gegenüber bestätigt wird."

Das Auskunftsverlangen soll dem Betroffenen ermöglichen, seine Rechte umfassend geltend zu machen, wozu neben der Löschung und Berichtigung auch das Recht auf Einlegung eines Rechtsbehelfs und Schadensersatz gehören.

Einem Auskunftsersuchen kann auch durch Negativauskunft nachgekommen werden. Selbst dann, wenn keine Datenverarbeitung stattfindet, hat der Betroffene einen Anspruch darauf, dass ihm dies gegenüber bestätigt wird. Zudem hat auch eine Negativauskunft substantiiert zu erfolgen. Das bedeutet beispielsweise, dass auch für den Fall einer Negativauskunft der Verantwortliche grundsätzlich konkrete vergangene und zukünftige Empfänger beauskunften und zu diesem Zweck Angaben über die Empfänger speichern muss. Ungeklärt ist jedoch die Aufbewahrungsfrist dieser Daten.

Hinweis für kirchliche Einrichtungen

Die Hinweise aus der Entscheidung zur Negativauskunft bei Auskunftsverlagen sind auch auf das KDG und damit die kirchlichen Einrichtungen übertragbar. Die kirchlichen Stellen sollten sich daher bei ihren Negativauskünften an die Vorgaben der Entscheidung halten.

Auch die Überlegungen zur Ermessensausübung der Aufsichten sind übertragbar und werden vom Diözesandatenschutzbeauftragten (DDSB) beziehungsweise Verbandsdatenschutzbeauftragen bei seiner Arbeit berücksichtigt.

1.2.4 Orientierungshilfe "Digitale Dienste" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Die Orientierungshilfe Digitale Dienste[18] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bietet einen

[18] https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

Leitfaden für die datenschutzrechtlichen Anforderungen, denen sich Anbieter digitaler Dienste stellen müssen. In der Version 1.2 des Dokuments von November 2024 wurde die Orientierungshilfe an die neue Terminologie durch das Digitale-Dienste-Gesetzes angepasst, wonach der Begriff „Telemedien" im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) nunmehr durch den Begriff „digitale Dienste" ersetzt wird. Das TTDSG wird nunmehr zum sogenannten Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Darüber hinaus beinhaltet die Orientierungshilfe Digitale Dienste Aktualisierungen, um die neusten Rechtsentwicklungen abzubilden. In diesem Zusammenhang werden die Anwendungsbereiche des TDDDG und der DSGVO miteinander verglichen und es wird ein zentraler Einblick in den § 25 TDDDG (Schutz der Privatsphäre bei Endeinrichtungen) gewährt. Daneben wird veranschaulicht, wie die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß DSGVO, die Gestaltung von Einwilligungsbannern und die Wahrnehmung von Betroffenenrechten praxisnah und lösungsorientiert umgesetzt werden können.

Allgemeines

Beim Betrieb von digitalen Diensten, wie insbesondere Internetseiten und Apps, kommen regelmäßig Technologien zum Einsatz, die es ermöglichen, personenbezogene Daten von Nutzenden zu verschiedenen Zwecken zu verarbeiten. Ein Beispiel solcher Technologien sind sog. Cookies. Mittels Cookies und ähnlicher Technologien können Informationen auf den Geräten der Nutzenden abgelegt, angereichert und verwaltet werden, die bei der Verwendung eindeutiger Kennungen (UID)[19] eine Identifikation oder Zuordnung zu einer natürlichen Person zulassen.

Das Setzen und Auslesen von Cookies berührt jedoch auch die Integrität der Endeinrichtungen, sodass die technischen Prozesse originär in den Regelungsbereich der Richtlinie 2002/58/EG[20] in der durch die Richtlinie 2009/136/EG geänderten Fassung (sog. ePrivacy-RL[21]) unterfallen. Nachdem es zur Umsetzung dieser Richtline mittels Telekommunikation-Telemedien-Datenschutz-Gesetz in deutsches Recht kam, hat man mit Art. 8 des Änderungsgesetzes zur Einführung des Digitale-Dienste-Gesetzes[22] den Begriff „Telemedien" im TTDSG nunmehr durch den Begriff „digitale Dienste" ersetzt, sodass das Gesetz nunmehr Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz heißt.

Anwendungsbereich und Abgrenzung

Adressaten des TDDDG sind neben den Anbietern von Telekommunikationsdiensten vor allem Anbieter von digitalen Diensten gemäß § 2 Abs. 2 Nr. 1 TDDDG. Hierunter fällt jede natürliche oder juristische Per-

[19] Ein Unique Identifier (UID) ist ein spezifischer Code oder eine Nummer, die Objekten, Personen oder Daten zugewiesen werden, um sie von anderen zu unterscheiden. Sie dienen der Identifizierung, Verfolgung und Verwaltung von Daten in verschiedenen Branchen und stellen sicher, dass jedes Objekt eine eindeutige Kennung erhält, die es von anderen unterscheidet.

[20] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.07.2002, S. 37–47).

[21] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (ABl. L 337 vom 18.12.2009, S. 11–36).

[22] Bundesgesetzblatt Jahrgang 2024 Teil I Nr. 149, ausgegeben zu Bonn am 13.05.2024.

son, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt.

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die ePrivacy-RL – und damit auch die nationale Umsetzung im TDDDG – zielt auf einen gleichwertigen Schutz des Rechts auf Privatsphäre und Vertraulichkeit ab und bezweckt eine Ergänzung der Bestimmungen der DSGVO in Bezug auf die Verarbeitung personenbezogener Daten. Werden durch den Einsatz von Technologien beispielsweise keine personenbezogenen Daten verarbeitet, sind nur die Vorgaben des TDDDG, nicht aber diejenigen der DSGVO zu beachten. Es kann jedoch auch zu Fallkonstellationen kommen, bei denen die Anwendungsbereiche sowohl des TDDDG als auch der DSGVO eröffnet sind. Für diesen Fall enthält Art. 95 DSGVO eine Kollisionsregel. Mithin gelten die spezifischen Bestimmungen des § 25 TDDDG vorrangig vor den Bestimmungen der DSGVO, soweit beim Speichern und Auslesen von Informationen in Endeinrichtungen personenbezogene Daten verarbeitet werden.

Schutz der Privatsphäre in Endeinrichtungen gemäß § 25 TDDDG

Bei dem § 25 TDDDG handelt es sich um eine zentrale Norm des TDDDG. Hier wird der Grundsatz der Einwilligungsbedürftigkeit normiert. Das bedeutet, dass die Speicherung von Informationen in der Endeinrichtung von Nutzenden oder der Zugriff auf solche Informationen, die bereits in der Endeinrichtung gespeichert sind, nur mit Einwilligung der Endnutzer zulässig sind. Dabei regelt § 25 TDDDG nicht eigenständig welche Anforderungen an die Einwilligung zu stellen sind, sondern verweist in diesem Fall auf die DSGVO. Beachtenswert sind die in § 25 Abs. 2 TDDDG normierten Ausnahmetatbestände betreffend die Einwilligungsbedürftigkeit.

Rechtmäßigkeit der Verarbeitung gemäß DSGVO

Die Speicherung von Informationen in der Endeinrichtung oder der Zugriff auf Informationen die bereits in der Endeinrichtung gespeichert sind, unterfällt dem Anwendungsbereich des TDDDG. Unberührt davon bleibt die Frage der Rechtmäßigkeit der nachfolgenden Verarbeitung von personenbezogenen Daten, die als Folge des Auslesens von Informationen aus den Endgeräten erlangt und anschließend verarbeitet werden. Diese unterliegt den Anforderungen des Datenschutzrechts, das heißt insbesondere der DSGVO. Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 DSGVO[23] erfüllt ist.

Gestaltung von Einwilligungsbannern

In der OH Digitale Dienste wird verdeutlicht, wie eine wirksame Einwilligung über ein Einwilligungsbanner entsprechend der Kriterien für § 25 Abs. 1 TDDDG und für Art. 6 Abs. 1 lit. a) DSGVO[24] eingeholt werden kann. Dabei werden allgemeine Anforderungen sowie Hinweise für die konkrete Gestaltung von Einwilligungsbannern vorgestellt. Beispielsweise müssen die beteiligten Akteure und deren Funktion ausreichend

[23] Entspricht § 6 Abs. 1 KDG.
[24] Entspricht § 6 Abs. 1 lit. b) KDG.

erklärt werden und über ein Auswahlmenü aktiviert werden können. Sofern auf der Internetseite Drittdienste eingesetzt werden, ist es nicht ausreichend, wenn allgemein darauf hingewiesen wird, dass Informationen an „Partner" weitergegeben werden. Eine Ablehnfunktion auf erster Ebene ist aus Sicht der Aufsichtsbehörden nicht generell erforderlich, sondern nur dann, wenn Nutzer mit dem Einwilligungsbanner interagieren müssen, um den Besuch der Internetseite fortzusetzen. Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zur Ausübung des Widerrufs implementiert werden. Der Widerruf muss gemäß Art. 7 Abs. 3 S. 4 DSGVO[25] so einfach möglich sein wie die Erteilung der Einwilligung.

Betroffenenrechte
Im Übrigen werden in der OH Digitale Dienste überblicksartig die Betroffenenrechte gemäß Art. 12 ff. DSGVO[26] vorgestellt. Dabei fokussiert sich die Orientierungshilfe auf die Informationspflichten gem. Art. 13 f. DSGVO[27], das Auskunftsrecht gem. Art. 15 DSGVO[28] und das Recht auf Löschung gem. Art. 17 DSGVO[29].

Hinweis für kirchliche Einrichtungen

Die Orientierungshilfe der DSK bietet auch für die kirchlichen Einrichtungen wichtige Hinweise für den Umgang mit personenbezogenen Daten und digitalen Diensten.

1.2.5 Auskunftsrecht zu Entscheidungen in Personalsachen von kirchengemeindlichen Gremien in nicht öffentlichen Sitzungen

In einem vom Bundesarbeitsgericht[30] zu entscheidenden Verfahren war die Klägerin als Kirchenmusikerin bei einer evangelischen Kirchengemeinde angestellt.

Im Rahmen einer nicht öffentlichen Sitzung des Kirchengemeinderates wurden arbeitsrechtliche Maßnahmen gegen die Klägerin besprochen. Die Klägerin begehrte vor Gericht – nach erfolgloser vorheriger Ablehnung durch die Kirchengemeinde – die Herausgabe einer Kopie dieses Protokolls, wobei sie sich auf das Recht auf eine kostenlose Kopie aus Art. 15 Abs. 3 DSGVO stützte, welches es zum damaligen Zeitpunkt noch nicht im DSG-EKD gab. Die Beklagte verweigerte dies mit Verweis auf die kirchenrechtliche Verschwiegenheitspflicht zu Inhalten nicht öffentlicher Sitzungen des Kirchengemeinderates.

Das Bundesarbeitsgericht sieht den Anspruch der Klägerin nicht vorrangig in Art. 15 DSGVO oder im kirchlichen Datenschutzgesetz, sondern begründet ihn vor allem aus arbeitsrechtlichen Vorschriften. Der

[25] Entspricht § 8 Abs. 6 S. 4 KDG.
[26] Entspricht den §§ 14 ff. KDG.
[27] Entspricht den §§ 15 f. KDG.
[28] Entspricht den § 17 KDG.
[29] Entspricht den § 19 KDG.
[30] BAG, Urteil vom 17.10.2024 – Az. 8 AZR 42/24.

Anspruch der Klägerin auf Auskunft und Überlassung einer Kopie beruht auf dem Arbeitsverhältnis und ist durch dieses bedingt.

Dabei verweist das Gericht auf die in der Landeskirche geltenden Regelungen der Kirchlichen Anstellungsordnung, welche ein Recht auf Einsicht in die „vollständige" Personalakte sowie auf Kopien dortiger Unterlagen gewährt. Dieses Recht besteht nach § 241 Abs. 2 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG auch nach Beendigung des Arbeitsverhältnisses. Das streitige Protokoll der Kirchengemeinderatssitzung ist somit Teil der materiellen Personalakte der Klägerin, weil es ausschließlich arbeitsrechtliche Maßnahmen betrifft und folglich inhaltlich in engem innerem Zusammenhang mit dem Arbeitsverhältnis steht. Die Tatsache, dass die Sitzung nicht öffentlich war und eine Verschwiegenheitspflicht der Mitglieder des Gremiums bestand, kann das Betroffenenrecht auf Auskunft, Herausgabe und Einsicht in dieses Protokoll nicht ausschließen.

Hinweis für kirchliche Einrichtungen

Die Entscheidung stärkt das Einsichts- und Kopierrecht von Beschäftigen in kirchlichen Arbeitsverhältnissen, selbst für Protokolle nicht öffentlicher Sitzungen, sofern in diesen Sitzungen Personalfragen behandelt werden. Dabei wird ein Anspruch nicht (nur) über die DSGVO oder das kirchliche Datenschutzrecht hergeleitet, sondern maßgeblich über arbeitsvertragliche Normen und die dahinterstehenden Grundrechte, wie z. B. das Recht auf informationelle Selbstbestimmung.

1.2.6 Arbeitsgericht Duisburg spricht immateriellen Schadenersatz wegen unerlaubter Weitergabe von Gesundheitsdaten zu

Das Arbeitsgericht Duisburg hat in einem datenschutzrechtlich interessanten Urteil[31] die Beklagte zur Zahlung von 10.000 Euro immateriellen Schadenersatz verurteilt. Hintergrund ist die unberechtigte und massenhafte Veröffentlichung sensibler Gesundheitsdaten eines Mitarbeiters.

Der Kläger war als technischer Leiter bei einem Luftsportverband e. V. mit mehreren tausend Mitgliedern angestellt. Die Beklagte war Präsidentin dieses Verbands. Im Jahr 2023 verschickte sie per E-Mail Informationen über den Gesundheitszustand des Klägers an rund 10.000 Verbandsmitglieder, ohne eine rechtswirksame Einwilligung des Klägers. In den E-Mails wurde unter anderem mitgeteilt, dass sich der technische Leiter seit November 2022 „im Krankenstand" befinde. Einen wirksamen Beschluss des Präsidiums zum Versand dieser E-Mail gab es nicht. Der Kläger machte geltend, dass seine Reputation stark beschädigt worden sei. Nicht nur im beruflichen Umfeld, sondern auch privat (z. B. auf dem Flugplatz) spreche ihn nun jeder auf seine angebliche Krankheit an.

[31] ArbG Duisburg, Urteil vom 26.09.2024 - Az. 3 Ca 77/24.

Das Gericht stellte einen Verstoß gegen die DSGVO fest, insbesondere gegen Art. 9 DSGVO, da Gesundheitsdaten besonders schützenswert sind. Es liege ein immaterieller Schaden vor, weil durch die Verbreitung das Ansehen und die Würde des Klägers erheblich beeinträchtigt wurden. Bei der Bemessung des Schadensersatzes orientierte sich das Gericht an der Zahl der Empfänger (fast 10.000 Vereinsmitglieder) und an der Schwere des Eingriffs. Das Gericht sah 10.000 Euro als angemessene Entschädigung an.

Ein Nachweis der Beklagten, dass sie nicht verantwortlich sei, gelang nicht. Sie konnte nicht darlegen, dass sie keine Schuld am Datenschutzverstoß trifft.

Hinweis für kirchliche Einrichtungen

Die tragenden Erwägungen der Entscheidung sollten auch in den kirchlichen Einrichtungen und Vereinigungen in Bezug auf die eigene Kommunikation und den Umgang mit besonderen Kategorien personenbezogener Daten analysiert werden. So sind Gesundheitsdaten auch im kirchlichen Datenschutzrecht nach §§ 4 Nr. 2, 11 KDG besonders geschützt. Fahrlässiger Umgang mit diesen besonders zu schützenden Daten birgt die Gefahr einer (immateriellen) Schadensersatzforderung gegen die Einrichtung.

Die Entscheidung zeigt auch, dass unter bestimmten besonderen Umständen auch eine persönliche Haftung der Leitung einer Einrichtung oder einer Vereinigung für Datenschutzverstöße möglich ist. Dies dürfte zwar die Ausnahme bleiben und nicht bei jeder fahrlässigen Verletzung datenschutzrechtlicher Vorgaben infrage kommen, kann aber – wie im vorliegenden Fall – nicht völlig ausgeschlossen werden.

„Die tragenden Erwägungen der Entscheidung sollten auch in den kirchlichen Einrichtungen … in Bezug auf die eigene Kommunikation und den Umgang mit besonderen Kategorien personenbezogener Daten analysiert werden."

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Der kirchliche Gesetzgeber hat im Berichtszeitraum ebenfalls Regelungen erlassen, die direkt oder indirekt datenschutzrechtliche Vorgaben enthalten.

1.3.1 Evaluierung des Gesetzes über den Kirchlichen Datenschutz

Das im Mai 2018 in Kraft getretene Gesetz über den Kirchlichen Datenschutz enthält in § 58 Abs. 2 KDG eine Vorgabe zur Evaluierung.[32] Eine Arbeitsgruppe auf der Ebene des Verbandes der Diözesen Deutschlands arbeitet dafür unter Einbeziehung verschiedener Beteiligter den Änderungsbedarf am kirchlichen Gesetz – immer vor dem Hintergrun ddes notwendigen Einklangs mit der DSGVO (Art. 91 Abs. 1 DSGVO) – heraus.

[32] Zur Evaluierung des KDG siehe auch das Vorwort im Jahresbericht 2023, Abschnitt 1.3.3 im Jahresbericht 2022 und Abschnitt 1.3.4 im Jahresbericht 2021.

Nach umfangreichen Vorarbeiten und Beratungen konnte die Arbeitsgruppe im Berichtszeitraum einen Entwurf der geplanten Änderungen am Gesetz über den Kirchlichen Datenschutz vorstellen. Dieser Entwurf wurde vom VDD im Oktober 2024 in einem Beteiligungsverfahren an die (Erz-)Diözesen und weitere kirchliche Gruppen und Einrichtungen verschickt, um eine möglichst breite Resonanz und Rückmeldung auf den Entwurf zu bekommen.[33] Eine Rückmeldung im Beteiligungsverfahren war bis Ende Januar 2025 möglich. Der Diözesan- beziehungsweise Verbandsdatenschutzbeauftragte hat sich in beiden Funktionen aktiv an dem Gesetzgebungsverfahren beteiligt und in dem mehrjährigen Prozess immer wieder Anregungen eingebracht. Außerdem hat die Konferenz der Diözesandatenschutzbeauftragten mehrere Stellungnahmen mit Vorschlägen abgegeben.

Nach Auswertung der Rückmeldungen aus dem Beteiligungsverfahren wird die Arbeitsgruppe einen überarbeiteten Gesetzentwurf vorlegen, der nach derzeitiger Planung im Herbst 2025 von den Verbandsgremien des VDD beschlossen werden soll und dann von den einzelnen Diözesanbischöfen in diözesanes Recht überführt werden muss.

1.3.2 Ordnung zum Betrieb einer Meldestelle nach Hinweisgeberschutzgesetz

Mit dem Inkrafttreten des Hinweisgeberschutzgesetzes waren auch die kirchlichen Stellen verpflichtet dieses Gesetz umzusetzen und interne Meldestellen einzurichten.[34] Diese Meldestellen sind für Meldungen im Anwendungsbereich des Hinweisgeberschutzgesetzes zuständig. Hierzu gehören auch Meldungen über Verstöße gegen die DSGVO (§ 2 Abs. 1 Nr. 3 lit. o) HinSchG).

Die Einrichtung der internen Meldestellen wurde in den (Erz-)Bistümern durch den Erlass von gesetzlichen Regelungen zur Einrichtung und Ausgestaltung der internen Meldestellen flankiert.[35]

Gemeinsam ist diesen Regelungen, dass Eingaben zu Verstößen gegen das Gesetz über den Kirchlichen Datenschutz nicht als Meldungen im Sinne der Ordnungen zu den internen Meldestellen nach HinSchG definiert werden.[36] Für Verstöße gegen Regelungen des KDG verbleibt es daher bei den bisherigen Meldewegen und Stellen. Personen können sich an den betrieblichen Datenschutzbeauftragten der kirchlichen Stelle wenden oder die Eingabe direkt beim Diözesandatenschutzbeauftragten als der zuständigen Datenschutzaufsicht einreichen.

[33] Der Entwurf des novellierten KDG aus September 2024, der im Beteiligungsverfahren verteilt wurde, ist auf der Internetseite der Deutschen Bischofskonferenz (https://www.dbk.de/ueber-uns/verband-der-dioezesen-deutschlands-vdd/dokumente im Abschnitt „Novellierung des Gesetzes über den Kirchlichen Datenschutz“) abrufbar (https://www.dbk.de/fileadmin/redaktion/diverse_downloads/Dossiers_alt/dossiers_2024/Novellierung_des_Gesetzes_%C3%BCber_den_Kirchlichen_Datenschutz.pdf).

[34] Siehe Abschnitt 1.2.1 des Jahresberichts 2023.

[35] Z. B. die „Ordnung zum Betrieb einer Meldestelle für den nordrhein-westfälischen Teil des Bistums Münster (Hinweisgebersystem)“ vom 19.12.2023 (KABl 2024 Seite 9).

[36] Siehe beispielsweise § 4 Abs. 3 lit. b) der Ordnung zum Betrieb einer Meldestelle für den nordrhein-westfälischen Teil des Bistums Münster (Hinweisgebersystem).

1.3.3 Einsicht in Missbrauchs-Akten in der Diözese Essen

Die Diözese Essen ermöglicht unter bestimmten Bedingungen die persönliche Akteneinsicht sowie die schriftliche Auskunft zu Inhalten aus Missbrauchsfällen zur persönlichen und wissenschaftlichen Aufarbeitung von sexueller Gewalt. Vor allem sollen Betroffene bei der persönlichen Verarbeitung von Missbrauchsfällen durch die neu eingeführte Möglichkeit der Akteneinsicht unterstützt werden.

Hierzu wurde die „Ordnung zur Regelung von Einsichts- und Auskunftsrechten von Betroffenen sexuellen Missbrauchs und Dritten" erlassen, die im Kirchlichen Amtsblatt Stück 2 des Bistums Essen vom 23.02.2024 unter Nr. 19 veröffentlicht wurde und mit der Veröffentlichung in Kraft trat.[37]

Bezug genommen wird auf Sachakten, die Informationen (z. B. zu Verdachtsfällen) enthalten, und auf Personalakten mit Auskünften über Einstellung und Entlassung sowie Versetzungen von Verdächtigen und Tätern.

Sachakten zu Missbrauchsfällen können insbesondere Betroffene von sexualisierter Gewalt einsehen. Außerdem haben auch die Aufarbeitungskommissionen der katholischen (Erz-)Diözesen sowie mit der Aufklärung von sexuellen Missbrauchsfällen beauftragte Hochschulen und Rechtsanwaltskanzleien Zugang zu diesen Akten. Die Akteneinsicht erfolgt auf Antrag.

Bei den Personalakten besteht die Möglichkeit der Aktenauskunft, da die Einsicht in Personalakten bisher nur unter engen Voraussetzungen möglich ist. Ab Beginn des Jahres 2024 wurden die Abschnitte der Personalakten, die sexuelle Gewalt betreffen, in die Sachakten integriert und sind somit grundsätzlich zugänglich.

1.3.4 Ordnung für die Aufbewahrung und Kassation von pfarramtlichen Unterlagen in der Erzdiözese Köln

Die Erzdiözese Köln hat am 21.05.2024 eine neue Ordnung für die Aufbewahrung und Kassation von pfarramtlichen Unterlagen erlassen.[38] Die Ordnung regelt die Aufbewahrungsfristen und legt die Anbietungs- und Übergabepflicht fest.

Besonders hilfreich für die Praxis ist die Anlage zur Ordnung, in der in Tabellenform ein detaillierter Fristen -und Bewertungskatalog für Unterlagen im pfarramtlichen Bereich abgebildet ist.

[37] https://netx.bistum-essen.de/portals/edr/#document/177523

[38] ABl. 2024 Nr. 104 (Seite 152); https://www.erzbistum-koeln.de/export/sites/ebkportal/erzbistum/generalvikariat/.content/documentcenter/amtsblatt/2024/2024-07-01-amtsblatt-erzbistum-koeln.pdf#page=18

1.3.5 Rahmenschulordnung für Schulen in der Trägerschaft des Bistums Essen

Die „Rahmenschulordnung für Schulen in der Trägerschaft des Bistums Essen" (RSO-BiE)[39] legt die Grundsätze und Richtlinien für alle Schulen fest, die dem Bistum Essen unterstehen. Die Ordnung ist am 01.08.2024 in Kraft getreten und ersetzt die vorherige Version aus dem Jahr 2000.

Die Ordnung wurde aktualisiert, um die rechtlichen Bedingungen der Schulen den tatsächlichen Realitäten im Schulalltag anzupassen, so stärkt sie z. B. die Entscheidungskompetenz der Schulleitungen vor Ort.

1.3.6 KI-Nutzungs-Ordnung der Erzdiözese Köln

Im Januar 2025 veröffentlichte die Erzdiözese Köln die „Ordnung über die Nutzung Künstlicher Intelligenz durch Einrichtungen und Institutionen im Erzbistum Köln (KI-Nutzungs-Ordnung)"[40] vom 10.12.2024.

Die Ordnung legt fest, unter welchen Voraussetzungen KI-Systeme im Erzbistum Köln eingesetzt werden dürfen. So soll ein sicherer und verantwortungsvoller Umgang mit und Einsatz von KI gewährleistet werden.

Hinweise für kirchliche Einrichtungen

Es sind mittlerweile so viele und so gute KI-Tools für berufliche Anwendungsfälle für die Mitarbeitenden verfügbar, dass die Mitarbeitenden diese Tools im beruflichen Alltag einsetzen wollen und auch einsetzen.

Die beim Einsatz der Tools oftmals entstehenden Gefahren für personenbezogene Daten oder Betriebs- und Geschäftsgeheimnisse der Einrichtung sind von der Einrichtung zu regeln. Mit diesen Regelungen sollte eine gesetzeskonforme Nutzung der KI-Tools durch die Mitarbeitenden erreicht werden.

1.3.7 Vatikaanstaat setzt Datenschutzgesetz in Kraft

Im Jahr 2024 hat der Vatikanstaat mit dem Dekret Nr. DCLVII[41] erstmals ein eigenes Datenschutzgesetz verabschiedet, das „Regolamento Generale sulla protezione dei Dati personali" (RGDP). Es trat zum 30.04.2024 in Kraft.

[39] KABl. 2024 Nr. 47 (Seite 83): https://netx.bistum-essen.de/portals/edr/#document/179741
[40] ABl. 2025 Nr. 2 (Seite 3): https://www.erzbistum-koeln.de/export/sites/ebkportal/erzbistum/generalvikariat/.content/documentcenter/amtsblatt/2025/2025-01-01-amtsblatt-erzbistum-koeln.pdf
[41] https://www.vaticanstate.va/phocadownload/leggi-decreti/normativa-generale/N.%20DCLVII.pdf

Das Regelwerk übernimmt in seiner Systematik zentrale Prinzipien der EU-Datenschutz-Grundverordnung, folgt aber nicht in allen Bereichen dem Vorbild der DSGVO.

Das RGDP ist zunächst für drei Jahre „ad experimentum" in Kraft gesetzt. Diese zeitlich befristete Einführung ermöglicht Anpassungen aufgrund praktischer Erfahrungen, schafft aber Unsicherheit in Bezug auf Rechtssicherheit und Langzeitbeständigkeit.

Das Gesetz gilt ausschließlich für die staatlichen Organe und Verwaltungen des Governatorats der Vatikanstadt – also für jene Stellen, die staatliche Verwaltungsaufgaben auf dem Territorium oder in exterritorialen Einrichtungen ausüben. Nicht erfasst vom Anwendungsbereich des Gesetzes sind: Der Heilige Stuhl, die Römische Kurie, sowie alle Dikasterien und Einrichtungen, die kirchliche Verwaltungsaufgaben mit weltweiter Zuständigkeit wahrnehmen.

Damit besteht eine klare institutionelle Abgrenzung zwischen „Staat Vatikanstadt" und „Heiliger Stuhl". Für datenschutzrechtliche Anfragen oder Beschwerden gegen kirchliche Behörden ist das RGDP daher nicht anwendbar.

Die im RGDP vorgesehenen Rechtsgrundlagen entsprechen weitgehend jenen der DSGVO. Neben der Einwilligung (in Art. 7 RGDP analog zur DSGVO geregelt) gibt es fünf weitere Rechtsgrundlagen:

- Verarbeitung im Rahmen der vatikanischen Diplomatie (Tätigkeiten, die in den Anwendungsbereich von Artikel 6 des Grundgesetzes des Staates Vatikanstadt vom 13.05.2023 fallen).
- Verarbeitung auf Grundlage internationaler Abkommen und zur Justiz-Zusammenarbeit.
- Zur Vertragserfüllung sowie zur Erfüllung von rechtlichen oder sittlichen Verpflichtungen (»obbligo legale« oder »impegno morale«), die nach dem Recht der Vatikanstadt rechtlich schutzwürdig sind.
- Lebenswichtiges Interesse, beschränkt auf Fälle, in denen die betroffene Person nicht einwilligungsfähig ist.
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt.

Ein berechtigtes Interesse gibt es nicht. Datenverarbeitungen brauchen damit also grundsätzlich eine Rechtsgrundlage. Eingeschränkt wird dieses Prinzip allerdings durch die sehr interpretationsoffene Rechtsgrundlage der »sittlichen Verpflichtung«.

Der Begriff der Kategorien besonderer Daten umfasst nach RGDP die rassische beziehungsweise ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, genetische und biometrische Daten, Gesundheitsdaten und Daten zum Privatleben. Explizit nicht genannt sind Daten zum Sexualleben oder zur sexuellen Orientierung; diese könnten jedoch unter die Kategorie „Privatleben" subsumiert werden.

„Das Regelwerk übernimmt in seiner Systematik zentrale Prinzipien der EU-Datenschutz-Grundverordnung, folgt aber nicht in allen Bereichen dem Vorbild der DSGVO."

Die gewährten Betroffenenrechte sind formal mit der DSGVO deckungsgleich. Das RGDP gewährt den Betroffenen ein Informationsrecht über Datenerhebung (spätestens innerhalb von 30 Werktagen), Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Die Frist für die Erfüllung von Betroffenenrechten ist 30 Werktage mit der Möglichkeit einer Verlängerung auf 90 Tage.

Das RGDP etabliert einen Datenschutzbeauftragten innerhalb des Governatorats. Dieser ist organisatorisch dem Präsidenten des Governatorats unterstellt und nicht unabhängig im Sinne von Art. 52 DSGVO.

Das Gesetz sieht auch ein Beschwerdeverfahren vor, bei dem eine Beschwerde bei dem Datenschutzbeauftragten einzureichen ist. Diese Beschwerde wird dort geprüft und anschließend zur Entscheidung durch ein Dekret des Präsidenten des Governatorats vorgelegt. Gegen das Dekret ist kein expliziter gerichtlicher Rechtsbehelf vorgesehen.

„Das RGDP stellt einen bedeutenden Fortschritt im vatikanischen Recht dar. Es kodifiziert den Datenschutz als staatliche Aufgabe und orientiert sich an internationalen Standards."

Das RGDP stellt einen bedeutenden Fortschritt im vatikanischen Recht dar. Es kodifiziert den Datenschutz als staatliche Aufgabe und orientiert sich an internationalen Standards. Dennoch wird die Praxis zeigen müssen, wie beispielsweise eine unabhängige Aufsicht und der Rechtsschutz sichergestellt werden können, um mit datenschutzrechtlichen Regelungen der Europäischen Union oder anderer Staaten vergleichbar zu sein.

1.4 Weitere datenschutzrechtliche Entwicklungen im kirchlichen Bereich, insbesondere der EKD

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

1.4.1 Einheitliche Datenschutzaufsicht im Bereich der EKD

Mit der damaligen Novellierung des Datenschutzgesetzes der EKD wurde 2013 die Grundlage für die Neustrukturierung der Datenschutzaufsicht der EKD geschaffen, mit dem kirchen- und diakoniepolitischen Ziel, diese Aufgabe einheitlicher als in der Vergangenheit und in größeren Strukturen wahrzunehmen.[42] Der unabhängigen Aufsichtsbehörde „Der Beauftragte für den Datenschutz der EKD (BfD EKD)" wurden seitdem im Laufe der Jahre die Datenschutzaufsicht über immer mehr Landeskirchen und Diakonien übertragen.

Im Berichtszeitraum gab es im Bereich der evangelischen Kirche neben dem Beauftragten für den Datenschutz der EKD noch eine weitere Aufsichtsbehörde für zwei ostdeutsche Landeskirchen und zwei diakonische Landesverbände mit ihren Mitgliedseinrichtungen. Mit dem Jahreswechsel 2024/2025 haben diese Gliedkirchen und diakonischen

[42] Siehe 1. Tätigkeitsbericht 2015/2016 des BfD EKD, S. 20.

Landesverbände die Datenschutzaufsicht auch auf den BfD EKD übertragen.

Der BfD EKD ist damit seit dem 01.01.2025 die Datenschutzaufsichtsbehörde im gesamten Bereich der Landeskirchen der EKD und der Diakonie.[43]

1.4.2 Überarbeitung des Datenschutzgesetzes der EKD

Das „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD)" enthielt in der ab Mai 2018 geltenden Fassung – ebenso wie das KDG – eine Vorgabe zur Überprüfung des Gesetzes. Für das DSG-EKD war die Frist zur Überprüfung des Gesetzes in § 54 Abs. 4 DSG-EKD auf fünf Jahre festgelegt.

Nach umfangreichen Vorarbeiten und einem Beteiligungsverfahren konnte der Synode der Evangelischen Kirche in Deutschland im November 2024 in Erfüllung des Überprüfungsauftrages aus dem Gesetz der Entwurf für die Anpassung des DSG-EKD vorgelegt werden. Die Synode beschloss die vorgeschlagenen Änderungen.[44]

Mit der Überarbeitung wurden zwei Ziele verfolgt. Einerseits soll der Einklang mit der DSGVO plausibilisiert werden und gleichzeitig sollen kirchliche Spezifika im Gesetz gestärkt werden. So seien z. B. mit der Überarbeitung der Betroffenenrechte, des Widerspruchsrechts und der Anpassung der Bußgeldvorschriften Annäherungen an die DSGVO vorgenommen worden. Gleichzeitig seien mit § 6 DSG-EKD (Rechtsmäßigkeit der Verarbeitung), §§ 8 und 9 DSG-EKD (Offenlegung) und § 50 DSG-EKD (Verarbeitung für Archiv- und Forschungszwecke, Statistik) Regelungen zu kirchlichen Besonderheiten überarbeitet und mit § 50b DSG-EKD eine Norm zur Mitgliederkommunikation eingefügt worden.[45]

Das novellierte Datenschutzgesetz der EKD ist am 01.05.2025 in Kraft getreten.

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses und der nationalen Datenschutzaufsichten

Der Europäische Datenschutzausschuss trägt als Gremium, in dem sich die Datenschutzaufsichtsbehörden der Mitgliedsländer der EU beraten und u. a. gemeinsame Positionen und Vorgehensweisen beschließen, zur einheitlichen Anwendung der DSGVO bei. Die Aufgaben des Ausschusses sind in Art. 70 DSGVO beschrieben.

Auf nationaler Ebene beraten sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in der Datenschutzkonfe-

[43] Die Struktur des BfD EKD kann hier abgerufen werden: https://datenschutz.ekd.de/ueber-uns/unsere-struktur/

[44] Die aktuelle Fassung des DSG-EKD kann unter https://www.kirchenrecht-ekd.de/document/58309 abgerufen werden.

[45] Siehe die Begründung zum Gesetzentwurf in der Drucksache XIII / 1 der 5. Tagung der 13. Synode der Evangelischen Kirche in Deutschland im November 2024.

renz. Mit ihren Beschlüssen verfolgt die DSK ebenfalls das Ziel, eine einheitliche Anwendung des europäischen wie auch des nationalen Datenschutzrechts in Deutschland zu erreichen.

Da das kirchliche Datenschutzrecht im Einklang mit der DSGVO steht und daher vergleichbare Regelungen enthält und den gleichen Grundsätzen folgt, sollten kirchliche Stellen die Auslegungen des EDSA und der DSK beachten. Unter Beachtung der kirchlichen Spezifika des KDG sind die Aussagen der Veröffentlichungen des EDSA beziehungsweise der DSK auf die Rechtslage nach dem KDG übertragbar. Die kirchlichen Datenschutzaufsichten berücksichtigen die Vorgaben des EDSA und der nationalen Datenschutzaufsichtsbehörden und stimmen sich teilweise mit diesen ab[46]. Auf den offiziellen Internetseiten können die Arbeit des EDSA[47] und der DSK[48] verfolgt werden.

Aus der Vielzahl der Leitlinien, Stellungnahmen und Beschlüssen des Europäischen Datenschutzausschusses und der nationalen Datenschutzaufsichtsbehörden können nachfolgend nur einige wenige Veröffentlichungen aufgegriffen werden.

1.5.1 Leitlinie 1/2024 des Europäischen Datenschutzausschusses mit Drei-Stufen-Modell zur Prüfung des berechtigten Interesses

„Der Europäische Datenschutzausschuss sieht in den Leitlinien ein Drei-Stufen-Modell vor, mit dem geprüft werden kann, ob ein berechtigtes Interesse im Sinne der Regelung des Art. 6 DSGVO vorliegt."

Mit den "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" vom 08.10.2024[49] hat sich der Europäische Datenschutzausschuss zum „berechtigten Interesse" im Sinne des Art. 6 Abs. 1 lit. f) DSGVO geäußert. Die Norm des § 6 Abs. 1 lit. g) KDG entspricht vom Regelungsgehalt dem Art. 6 Abs. 1 lit. f) DSGVO.

Der Europäische Datenschutzausschuss sieht in den Leitlinien ein Drei-Stufen-Modell vor, mit dem geprüft werden kann, ob ein berechtigtes Interesse im Sinne der Regelung des Art. 6 DSGVO vorliegt. Diese Prüfungsschritte sind auf die Vorgaben des § 6 KDG zum berechtigten Interesse übertragbar.

In einem vom Europäischen Datenschutzausschuss zusammen mit der Leitlinie herausgegebenen Informationsblatt[50] werden die drei Prüfungsschritte näher erläutert:

> ***"Step 1 - Is there a legitimate interest by the controller or a third party?***
> *Not all interests can be considered legitimate. As a general rule, the interest pursued by an organisation or a third party should be related to their actual activities and should not be contrary to EU or member*

[46] Siehe hierzu Abschnitt 3.6 dieses Jahresberichts.
[47] https://edpb.europa.eu/edpb_de
[48] https://www.datenschutzkonferenz-online.de
[49] Siehe https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_de
[50] EDPB "Legitimate interest when and how to apply it", Okt. 2024; siehe https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_de (Datei "Summary: legitimate interest, when and how to apply it").

state law. The legitimate interest should be clear and precisely articulated, and effective at the date of the data processing (not hypothetical).

Examples of legitimate interests may include fraud prevention, having access to information online, ensuring the continued functioning of publicly accessible websites, obtaining the personal information of a person who damaged someone's property in order to sue that person for damages, protecting the property, health and life of the co-owners of a building, commercial interest, product improvement and assessing the creditworthiness of individuals.

Step 2 - Is the processing really necessary for the legitimate interest?
When assessing if the processing is really necessary, the organisation should examine if the legitimate interest pursued can be achieved by other means less restrictive of the fundamental rights and freedoms of individuals.

Processing should be carried out only in so far as it is strictly necessary for the purposes of the legitimate interest identified. When carrying out this assessment, the organisation should examine if the data is relevant for the purpose pursued and limited to what is necessary to achieve this purpose (data minimisation principle).

Step 3 - Are the interests or fundamental rights and freedoms of individuals overridden by legitimate interest?
In order to apply legitimate interest, the third and last condition to be met is that the legitimate interest in question must not be overridden by the interests or fundamental rights and freedoms of individuals, taking into consideration the reasonable expectations of individuals based on their relationship with the organisation, and mitigating measures limiting the impact of the processing.

The interests of individuals that can override legitimate interest include, for example, financial interests, social interests or personal interests.

Fundamental rights and freedoms of individuals include the right to data protection and privacy, but also other fundamental rights and freedoms, such as the right to liberty and security, freedom of expression and information, freedom of thought, conscience and religion, freedom of assembly and association, prohibition of discrimination, the right of property, or the right to physical and mental integrity."

Diese drei Prüfungsschritte sind auf die konkrete Verarbeitung bezogen durchzuführen und zu dokumentieren, damit gerade der dritte Schritt der Interessenabwägung im Streitfall auch belegt und nachvollzogen werden kann.

Zum Inhalt der im Oktober 2024 veröffentlichten Version 1.0 der Guidelines konnte im Rahmen eines Konsultationsverfahrens Stellung genommen werden. Die Einarbeitung der Rückmeldungen aus dem Konsultationsverfahren ist derzeit noch nicht abgeschlossen. Nach Abschluss dieser Überarbeitungsphase wird der EDSA eine neue Version der Guidelines herausgeben.

„Diese drei Prüfungsschritte sind auf die konkrete Verarbeitung bezogen durchzuführen und zu dokumentieren, damit gerade der dritte Schritt der Interessenabwägung im Streitfall auch belegt und nachvollzogen werden kann."

Hinweise für kirchliche Einrichtungen

Wichtig ist, dass es für die kirchlichen Einrichtungen nicht ausreicht, auf der ersten Prüfungsstufe festzustellen, dass ein berechtigtes Interesse als solches vorhanden ist. Der wesentliche Schritt ist der dritte Prüfungsschritt, bei dem die eigentliche Interessenabwägung stattfindet. Dieser Schritt, der individuell auf den Einzelfall bezogen und nicht pauschal erfolgen muss, wird bei der Berufung auf das berechtigte Interesse oft vergessen oder eben nur pauschal vorgenommen.

1.5.2 Berechtigtes Interesse als Rechtsgrundlage für die Datenverarbeitung durch öffentlich-rechtlich organisierte kirchliche Stellen?

Mit den "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" vom 08.10.2024 hat der Europäische Datenschutzausschuss nicht nur ein dreistufiges Prüfungsschema zur Ermittlung des „berechtigten Interesses" im Sinne des Art. 6 Abs. 1 lit. f) DSGVO beschrieben.[51] Er hat sich auch noch zum zweiten Unterabsatz des Art. 6 Abs. 1 DSGVO geäußert.

Denn der Anwendungsbereich des Art. 6 Abs. 1 lit. f) DSGVO ist eingeschränkt. Behörden können sich bei einer „in Erfüllung ihrer Aufgaben vorgenommene[n] Verarbeitung" gemäß Art. 6 Abs. 1 Unterabsatz 2 DSGVO nicht auf diese Rechtsgrundlage berufen. Eine entsprechende Einschränkung wurde in das KDG übernommen, sodass diese Rechtsgrundlage „nicht für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung" gilt.

Zu dieser Einschränkung finden sich in dem Papier des Europäischen Datenschutzausschusses zwei Absätze:

2. Processing by public authorities

98. Article 6(1), second indent, of the GDPR states that the legal basis under Article 6(1)(f) shall not apply to processing carried out by public authorities in the performance of their tasks. Recital 47 of the GDPR clarifies the reason: "it is for the legislator to provide by law for the legal basis for public authorities to process personal data". Such provision indeed relates to the fact that, as a general rule, processing undertaken by public authorities falls under the scope of their tasks and missions provided for by EU or Member State law.

99. Nevertheless, these provisions do not prevent from relying, in exceptional and limited cases, on Article 6(1)(f) GDPR when the processing is not linked to or does not relate to the performance of their specific tasks or the exercise of their prerogatives as public authorities, but concerns, where permitted by the national legal

[51] Siehe hierzu Abschnitt 1.5.1 dieses Jahresberichts.

system, other activities that are lawfully carried out. Relying on Article 6(1)(f) GDPR in such exceptional cases should be documented internally. In no circumstances, public authorities may rely on Article 6(1)(f) for processing activities falling within the scope of the performance of their tasks.

Der EDSA betont in Rn. 99 am Ende nochmals die Wertung des Gesetzgebers, dass Behörden sich für Verarbeitungsvorgänge, die in den Bereich der Wahrnehmung ihrer Aufgaben fallen, unter keinen Umständen auf Art. 6 Abs. 1 lit. f) DSGVO berufen dürfen.

Der EDSA führt in Rn. 99 aber auch aus, dass es aus seiner Sicht möglich sein könne, sich in Ausnahmefällen und in begrenztem Umfang auf Art. 6 Abs. 1 lit. f) DSGVO zu stützen, wenn die Verarbeitung nicht mit der Wahrnehmung der spezifischen Aufgaben oder der Ausübung der Befugnisse als öffentliche Stellen in Verbindung stehe oder damit zusammenhänge, sondern, soweit dies nach dem nationalen Rechtssystem zulässig sei, andere rechtmäßig ausgeübte Tätigkeiten betreffe. Die Berufung auf Art. 6 Abs. 1 lit. f) DSGVO in solchen Ausnahmefällen sollte intern dokumentiert werden.

Da der EDSA an dieser Stelle keine Fallbeispiele anführt, welche Situationen aus seiner Sicht „exceptional and limited cases" darstellen sollen, bleibt diese vom EDSA angeführte Ausnahme schwer auszufüllen.

Zum Inhalt der im Oktober 2024 veröffentlichten Version 1.0 der Guidelines konnte im Rahmen eines Konsultationsverfahrens Stellung genommen werden. Die Einarbeitung der Rückmeldungen aus dem Konsultationsverfahren ist derzeit noch nicht abgeschlossen. Nach Abschluss dieser Überarbeitungsphase wird der EDSA eine neue Version der Guidelines herausgeben.

1.5.3 Europäischer Datenschutzausschuss veröffentlicht ersten Bericht zur Bewertung des EU-US Data Privacy Framework

Der Europäische Datenschutzausschuss hat im November 2024 seinen ersten Bericht zur Überprüfung des EU-US Data Privacy Framework (DPF)[52] veröffentlicht.

Der EDSA begrüßt, dass das US-Handelsministerium wesentliche Schritte zur Implementierung des Zertifizierungsverfahrens für DPF-zertifizierte Unternehmen unternommen hat – etwa durch den Aufbau einer neuen Internetseite, Verfahrensaktualisierungen, den Dialog mit Unternehmen und Sensibilisierungsmaßnahmen.

Der Ausschuss stellt fest, dass bislang nur wenige Beschwerden über den vorgesehenen Rechtsbehelfsmechanismus eingegangen sind. Dies unterstreicht nach Ansicht des EDSA die Notwendigkeit für verstärkte Überwachungs- und Kontrollmechanismen durch US-Behörden.

[52] Zum Data Privacy Framework siehe Abschnitt 1.1.3 des Jahresberichts 2023.

Der EDSA erwartet Leitlinien der US-Behörden zur Auslegung des Prinzips der Verantwortlichkeit bei der Weiterleitung von Daten, die aus der EU stammen – insbesondere bei DPF-zertifizierten Organisationen. Auch eine präzisere Definition von Personaldaten („HR-Daten“) wäre wünschenswert.

Der Ausschuss empfiehlt der Europäischen Kommission, die Entwicklungen bezüglich der Rechtsprechung und Gesetzgebung in den USA weiterhin eng zu begleiten.

2 Aus der Tätigkeit des Datenschutzzentrums

Die Meldungen von Datenschutzverletzungen nach § 33 KDG überstiegen im Berichtsjahr 2024 anzahlmäßig wieder bei weitem die Eingänge an Anfragen, Beschwerden und Hinweisen. In diesem Abschnitt werden einige neue oder stets relevante Aspekte und Sachverhalte präsentiert.

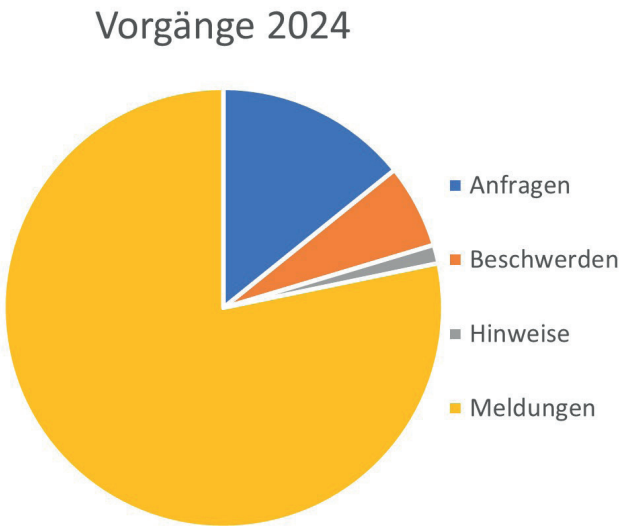


Abb. 1: Vorgänge beim Katholischen Datenschutzzentrum im Jahr 2024.

2.1 Beratungen und Anfragen

Auch im Jahr 2024 blieb die Beratungstätigkeit des Katholischen Datenschutzzentrums auf einem hohen Niveau. Viele Einrichtungen aus dem Zuständigkeitsbereich des Katholischen Datenschutzzentrums nutzten die Möglichkeit, sich an die Aufsicht zu wenden. Dabei wurde z. B. nach der Rechtsgrundlage für Ehrenamtliche gefragt oder schon vor der Verwendung eines Cloud-Speichers abgeklärt, ob dies datenschutzrechtlich möglich ist. Diese und weitere Beratungsschwerpunkte werden hier erläutert.

Hinweis für kirchliche Einrichtungen

Die Möglichkeit, mit der Datenschutzaufsicht schon im Vorfeld offene Fragen bei der Verarbeitung von personenbezogenen Daten zu klären, kann dazu beitragen, dass Datenschutzverletzungen bei der Umsetzung vermieden werden. Die Beratungsfunktion des Katholischen Datenschutzzentrums ergänzt dabei die Beratung durch die betrieblichen Datenschutzbeauftragten in den Einrichtungen.

2.1.1 Rechtsgrundlage für Ehrenamtliche

Wiederholt durfte sich das Katholische Datenschutzzentrum im Berichtszeitraum mit Anfragen von betrieblichen Datenschutzbeauftragten befassen, die nachgefragt haben, ob ehrenamtliche Mitarbeitende unter den Beschäftigtenbegriff des § 4 Nr. 24 KDG fallen und ihre personenbezogenen Daten dadurch auf Grundlage von § 53 KDG verarbeitet werden können. Insbesondere ging es ihnen um Ehrenamtliche, die ihre Tätigkeit ohne schriftlichen Vertrag und entgeltliche Vergütung ausüben.

„Ehrenamtliche sind keine Beschäftigten im Sinne der §§ 4 Nr. 24, 53 KDG."

Ehrenamtliche sind keine Beschäftigten i. S. d. §§ 4 Nr. 24, 53 KDG. Der Beschäftigtenbegriff wird in § 4 Nr. 24 KDG definiert. Ehrenamtliche fallen grundsätzlich nicht unter einen der in § 4 Nr. 24 KDG aufgezählten Fälle. Zwar ist die Aufzählung in der Norm nicht als abschließend zu verstehen – das folgt schon aus dem Wortlaut der Norm („insbesondere"). Sie sind aber auch nicht als sonstige Beschäftigte zu werten. Um als sonstiger Beschäftigter i. S. d. Norm zu gelten, wird grundsätzlich ein entgeltlicher Charakter vorausgesetzt. So zum Beispiel bei Werkstudenten oder Schülern.[53] Dieser entgeltliche Charakter liegt bei ehrenamtlichen Betreuern in der Regel nicht vor.

Nichts anderes ergibt sich, wenn man Meinungen aus der Literatur zu einer Parallelnorm aus dem staatlichen Bereich, z. B. § 26 BDSG, als Auslegungshilfe heranzieht. Vom Beschäftigtenbegriff sollen danach ehrenamtlich Tätige nicht umfasst werden.[54]

Dass ehrenamtliche Beschäftigte bisher nicht unter den Beschäftigtenbegriff des § 4 Nr. 24 KDG fallen ist auch am Evaluationsprozess des KDG erkennbar. Die kirchlichen Gesetzgeber haben, zumindest in einem ersten Entwurf des überarbeiteten KDG, Ehrenamtliche in die Aufzählung von § 4 Nr. 24 KDG aufgenommen. Eine solche Aufnahme wäre höchstwahrscheinlich nicht notwendig gewesen, wenn die Gesetzgeber davon ausgehen würden, dass Ehrenamtliche bereits unter den Begriff der sonstigen Beschäftigten fallen.

Die personenbezogenen Daten der Ehrenamtlichen müssen daher, bis zur Änderung des KDG in dieser Frage, auf Grundlage der allgemeinen Rechtsgrundlagen in § 6 KDG beziehungsweise § 11 KDG verarbeitet werden.

2.1.2 Übermittlung von personenbezogenen Daten zu Prüfzwecken an den Medizinischen Dienst

Krankenhäuser können seit 2021 eine OPS-Strukturprüfung bei den zuständigen Medizinischen Diensten (MDK) in den Ländern beantragen. Dabei wird geprüft, ob sie die Strukturmerkmale für bestimmte Leistungen erfüllen. Die zu prüfenden Strukturmerkmale sind in Kodes des Operationen- und Prozedurenschlüssels (OPS) nach § 301 Abs. 2 SGB V festgelegt, der jährlich vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) herausgegeben wird.

[53] Vgl. Fuhrmann in: Sydow, Kirchliches Datenschutzrecht, 1. Auflage 2021, § 53 Rn. 29.
[54] Vgl. z. B. Maschmann in: Kühling/Buchner DS-GVO BDSG 4. Auflage 2024, § 26 Rn. 7.

Die Medizinischen Dienste haben dabei die Aufgabe zu überprüfen, ob Krankenhäuser die vom Gemeinsamen Bundesausschuss festgelegten Qualitätsanforderungen einhalten. Grundlage der Begutachtung durch die Medizinischen Dienste ist eine vom Medizinischen Dienst Bund (MD-Bund) zu erlassene und jährlich zu aktualisierende Richtlinie „Regelmäßige Begutachtungen zur Einhaltung von Strukturmerkmalen von OPS-Kodes nach § 275d SGB V" (StrOPS-RL des MD-Bund). Die Verpflichtung der Krankenhäuser zur Übermittlung von personenbezogenen Daten folgt § 275a Abs. 1 S. 7 SGB V.

Auf Basis dieser Grundlage erhielt eine kirchliche Einrichtung im Zuständigkeitsbereich des Katholischen Datenschutzzentrums ein Schreiben eines Medizinischen Dienstes für eine Prüfung gem. des § 275a SGB V, in dem zum Teil die Vorlage von Arbeitsverträgen von Beschäftigten erwartet wurde, mit dem Hinweis, dass Angaben zum Gehalt unkenntlich gemacht werden können.

Die datenschutzrechtliche Grundlage für die Krankenhäuser zur Übermittlung von personenbezogenen Daten an den Medizinischen Dienst ergibt sich aus § 275a Abs. 1 S. 7 SGB V. Nach dessen Wortlaut haben Krankenhäuser allerdings nur die für die Begutachtung „erforderlichen" personen- und einrichtungsbezogenen Daten an den Medizinischen Dienst zu übermitteln. Fraglich ist, ob die Vorlage der gesamten Arbeitsverträge unter die Voraussetzung der Erforderlichkeit fällt und mit welcher Begründung. Die StrOPS-RL des MD-Bund enthält Vorgaben zu den konkret durch das zu prüfende Krankenhaus vorzulegende Unterlagen. Dort sind u. a. auch Arbeitsverträge genannt.

Die Erforderlichkeit dieser Daten für die Durchführung einer Qualitäts- oder Strukturprüfung durch den Medizinischen Dienst dürfte grundsätzlich nicht verneint werden können. Es erscheint zumindest nachvollziehbar, dass die in den Arbeitsverträgen enthaltenen Daten, wie z. B. die zu leistenden Arbeitsstunden oder die fachliche Ausrichtung und Qualifikation von Krankenhausangestellten, erforderlich für die Durchführung der oben genannten Prüfungen sind.

Verantwortliche müssen aber in jedem Fall prüfen, ob die Übermittlung von Arbeitsverträgen immer wirklich erforderlich i. S. d. Norm sein kann. Gegebenenfalls sollte dies in einem Gespräch mit dem zuständigen Medizinischen Dienst geklärt werden. Ähnliche Problematiken stellen sich beispielsweise auch im Bereich der Pflege. Verantwortliche im Bereich der Pflege sind ebenfalls angehalten die Erforderlichkeit der Verarbeitungen zu überprüfen.[55]

2.1.3 Austausch über Patientendaten per Microsoft Teams

Ein externer Datenschutzbeauftragter wandte sich mit detaillierten Fragen zum Einsatz von Microsoft Teams im Rahmen eines Zertifizierungsverfahrens im Krankenhausbereich an das Katholische Datenschutzzentrum. Ein Wechsel des Videokonferenzanbieters sei nicht

[55] Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch den Medizinischen Dienst im Bereich der Pflege ergibt sich u. a. aus § 97 Abs. 1 S. 1 SGB XI. Auch nach dieser Norm dürfen personenbezogene Daten nur im erforderlichen Rahmen verarbeitet werden.

möglich, da die Zertifizierungsstelle ausschließlich Microsoft Teams als Plattform akzeptiere. Es wurden Überlegungen angestellt, wie man dennoch den Schutz der Patientendaten gemäß KDG gewährleisten könne. Ungeklärte Fachfragen trug man an das Katholische Datenschutzzentrum heran.

Generell müssen zuerst allgemeinere Problemstellungen mit Microsoft-Produkten beachtet werden. Hierzu hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 24.11.2022 eine Festlegung[56] speziell zu Microsoft 365 getroffen und den entsprechenden Bericht ihrer Arbeitsgruppe[57] veröffentlicht.

Der Festlegung und dem Bericht können weitere Problembereiche entnommen werden, die durch einen Verantwortlichen vor dem Einsatz von 365 (und verwandten) Produkten geklärt werden sollten und die nicht im Folgenden erklärt werden.

Ferner ist der Grundsatz der Datenminimierung einzuhalten. Bei der Anfrage war es für das Katholische Datenschutzzentrum anhand des beschriebenen Sachverhalts nicht plausibel, warum auf Echtdatensätze zugegriffen wird. Die Datensätze sollten auf die unbedingt notwendigen Bestandteile beschränkt und ansonsten anonymisiert/pseudonymisiert werden. Unabhängig von der Frage, welche Rechtsgrundlage möglicherweise für die Offenlegung der Daten einschlägig sein könnte, ist stets darauf zu achten, dass der gewählte Umfang der Verarbeitung überhaupt erforderlich ist.

„Unabhängig von der Frage, welche Rechtsgrundlage möglicherweise für die Offenlegung der Daten einschlägig sein könnte, ist stets darauf zu achten, dass der gewählte Umfang der Verarbeitung überhaupt erforderlich ist."

Zu folgenden Fragen bezog das Katholische Datenschutzzentrum Stellung:

Halten Sie es für problematisch, dass der Austausch von Patientendaten über Microsoft Teams stattfindet, insbesondere angesichts der fehlenden Ende-zu-Ende-Verschlüsselung?

Personenbezogene Daten der besonderen Kategorie gem. § 4 Nr. 2 KDG unterfallen der Datenschutzklasse III nach § 13 Abs. 1 KDG-DVO. Eine verschlüsselte Übertragung und Speicherung von Daten der Schutzklasse III ist nach § 13 Abs. 2 KDG-DVO vorgesehen. Eine fehlende Verschlüsselung der Patientendaten ist also grundsätzlich als problematisch einzustufen, sofern nicht gleichwertige technische oder organisatorische Maßnahmen zum Schutz der Daten getroffen werden können. Bezüglich weiterer möglicher Problemstellungen wird auf die allgemeinen Ausführungen verwiesen.

Wäre es ausreichend, eine Einwilligung der betroffenen Patienten einzuholen, um den datenschutzrechtlichen Anforderungen zu genügen?

Grundsätzlich ist eine Einwilligung als Rechtsgrundlage zwar denkbar.

[56] Siehe: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/104DSK-Festlegung-Microsoft-Onlinedienste.pdf?__blob=publicationFile&v=1

[57] Siehe: https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf

Einwilligungen in ein nicht ausreichendes Schutzniveau der Verarbeitung sind jedoch nur unter bestimmten Voraussetzungen zulässig.[58]

Welche rechtlichen Risiken könnten entstehen, wenn die Datenübermittlung über Microsoft Teams ohne Ende-zu-Ende-Verschlüsselung durchgeführt wird?

Eine fehlende Verschlüsselung erhöht grundsätzlich die Wahrscheinlichkeit einer unbefugten Einsichtnahme in die Daten. Dies ist mit allen üblichen rechtlichen Risiken verbunden.

Welche technischen und organisatorischen Maßnahmen könnten implementiert werden, um das Risiko einer unbefugten Datenverarbeitung zu minimieren?

Unabhängig von der grundsätzlichen datenschutzrechtlichen Frage der Zulässigkeit der gewählten Kommunikationslösung, sollten die bei Teams vorhandene Möglichkeit zur Ende-zu-Ende Verschlüsselung aktiviert und der Grundsatz der Datenminimierung beachtet werden.

Das Katholische Datenschutzzentrum weist daraufhin, dass es sich an dieser Stelle nicht um eine abschließende Beurteilung handelt, da der Themenbereich dazu zu komplex ist und immer der Einzelfall mit der konkreten Verwendung zu betrachten ist.

2.1.4 Feedback zur Cloud-Speicher-Nutzung

Im Berichtszeitraum erreichten das Katholische Datenschutzzentrum auch wieder Anfragen zur Nutzung von Cloud-Speichern, insbesondere im Rahmen von Microsoft 365. Beispielsweise wurde angefragt, ob OneDrive for Business datenschutzkonform genutzt werden kann beziehungsweise welche Vorkehrungen für eine KDG-konforme Nutzung getroffen werden müssten.

Verantwortliche müssen bei bestehender oder geplanter Nutzung von Microsoft 365 (OneDrive for Business als Teil von Microsoft 365) das Problem, dass Microsoft Anwenderdaten zu eigenen Zwecken nutzt, im Blick behalten und dazu in der Datenschutz-Folgenabschätzung Antworten finden. Eine datenschutzkonforme Nutzung des Produktes ist nicht möglich, so lange nicht für alle Aspekte eine datenschutzkonforme Lösung gefunden wird.

Ausführungen dazu hat das Katholische Datenschutzzentrum bereits in ähnlicher Form auf seiner Homepage veröffentlicht.[59]

„Eine datenschutzkonforme Nutzung des Produktes ist nicht möglich, so lange nicht für alle Aspekte eine datenschutzkonforme Lösung gefunden wird."

[58] Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 15.06.2022 zur Einwilligung in ein nicht angemessenes Schutzniveau: https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2022/08/KDB-Dispositionsrecht-Nichtanwendung-von-TOM-vom-15.06.2022.pdf

[59] https://www.katholisches-datenschutzzentrum.de/aktuelle-fragen-zu-microsoft-365/

2.1.5 Nutzung der Kontaktdaten von Angehörigen verstorbener Gemeindemitglieder

Eine Pfarrei richtete die Frage an das Katholische Datenschutzzentrum, ob die in der Verwaltungssoftware im Pfarrbüro gespeicherten Adressdaten der Angehörigen von verstorbenen Gemeindemitgliedern für eine Einladung zu einer Gedenkmesse genutzt werden dürfen. Die Adressdaten der Angehörigen, die Ansprechpartner für die Seelsorger beim Trauerfall sind, werden bei dem initialen Kontakt erhoben und in der Software gespeichert.

Für die Speicherung der Adressdaten und die Verwendung dieser Adressdaten über den Trauerfall hinaus wird eine Rechtsgrundlage benötigt. Als taugliche Rechtsgrundlage ist nur die Einwilligung gemäß § 6 Abs. 1 lit. b) KDG ersichtlich. Eine Verarbeitung der Adressdaten über den Trauerfall hinaus dürfte daher nur aufgrund einer Einwilligung zulässig sein. Eine Speicherung und Verwendung der Adressdaten zum Zweck der Einladung zur Gedenkmesse ist ohne Einwilligung daher unzulässig.

2.2 Meldungen von Datenschutzverletzungen

Nach § 33 Abs. 1 KDG hat die Meldung einer Verletzung des Schutzes personenbezogener Daten unverzüglich durch den Verantwortlichen an die Datenschutzaufsicht zu erfolgen, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. In § 33 Abs. 3 KDG werden die Mindestanforderungen an die Meldung einer Datenschutzverletzung formuliert. Das Katholische Datenschutzzentrum empfiehlt, für diese Meldungen das Online-Formular auf der Homepage[60] zu verwenden. So ist sichergestellt, dass alle relevanten Informationen gemeldet und Nachfragen vermieden werden.

Hinweis für kirchliche Einrichtungen

In der Meldung ist auf die Übermittlung von personenbezogenen Daten zu verzichten. Sollte es für die Meldung unerlässlich sein, personenbezogene Daten an das Katholische Datenschutzzentrum zu übermitteln, wird vom Katholischen Datenschutzzentrum eine gesicherte Übertragungsmöglichkeit für den entsprechenden Vorgang zur Verfügung gestellt.

Die Zahl der gemeldeten Datenschutzverletzungen ist im Berichtsjahr verglichen mit den Meldungen der Vorjahre weiterhin hoch und im direkten Vergleich zum Vorjahr nochmal leicht gestiegen.

Die Bandbreite der gemeldeten Datenschutzverletzungen reicht dabei von Hacker-Angriffen, über eine Offenlegung von User-Verzeichnissen bis hin zur nicht datenschutzkonformen Nutzung von Sprachassistenten. Eine grobe Einteilung der Themen zeigt die folgende Grafik, einzelne Themenfelder werden in diesem Abschnitt näher beschrieben.

[60] https://www.katholisches-datenschutzzentrum.de/meldung-dsv/

Das Katholische Datenschutzzentrum weist daraufhin, dass es auch immer wieder zu einem meldepflichtigen Tatbestand kommt, weil versehentlich Unterlagen/Dokumente mit personenbezogenen Daten an das Katholische Datenschutzzentrum gesendet werden, die eigentlich für eine Einrichtung in dessen Zuständigkeitsbereich bestimmt sind.

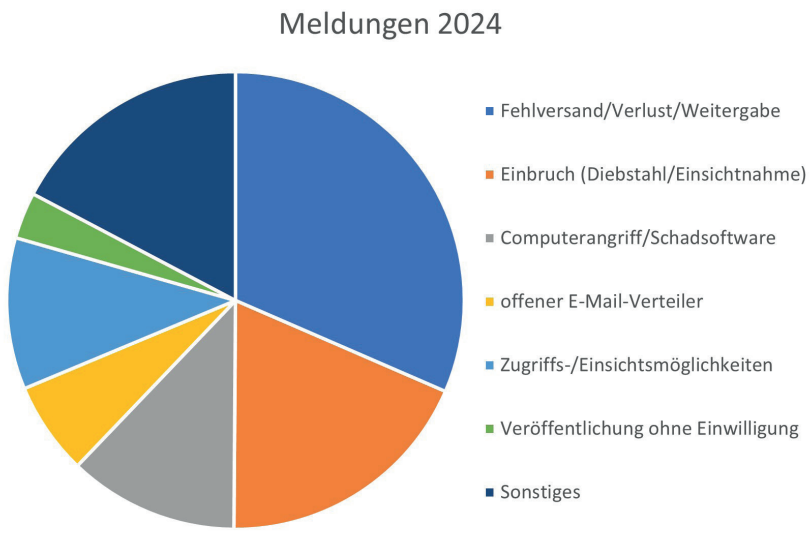


Abb. 2: Meldungen an das Katholische Datenschutzzentrum im Jahr 2024.

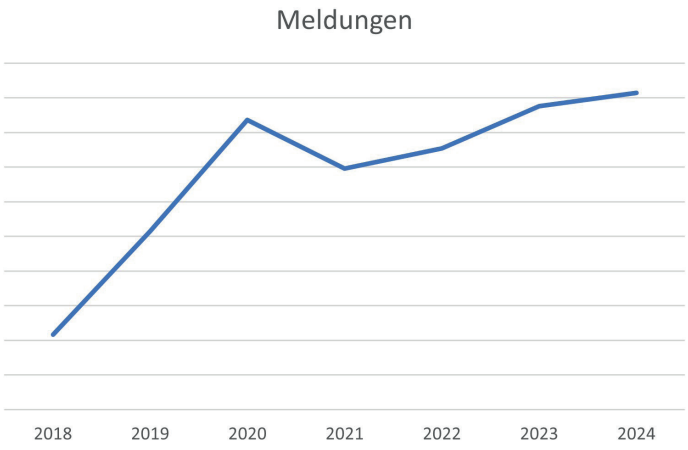


Abb. 3: Meldungen an das KDSZ im Verlauf der Jahre 2018 bis 2024.

2.2.1 Hacker-Angriff auf ein Krankenhaus

Ein Krankenhausverbund mit drei Standorten wurde Opfer eines Hacker-Angriffs. Durch eine Ransomware wurden zentrale Active-Directory-Dienste wie die Domänencontroller, aber auch E-Mail-Server und für den medizinischen Betrieb relevante Systeme verschlüsselt. Durch das IT-Personal wurden alle Systeme vom Internet getrennt und heruntergefahren, um den weiteren Zugriff der Angreifer zu unterbinden.

Das Krankenhaus musste aus der Notfallbereitschaft abgemeldet werden. Operationen wurden verschoben und einige Patienten in andere Krankenhäuser verlegt. Die Notfallversorgung der Patienten im Kran-

„Als Ausgangspunkt für den Hacker-Angriff wurde ein VPN-Zugang mit erhöhten Rechten identifiziert. Mit diesem kompromittierten Zugang konnten sich die Angreifer im Netzwerk bewegen."

kenhaus war während der Wiederherstellung der Systeme immer möglich.

Vom Krankenhaus wurden das Landeskriminalamt (LKA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Katholische Datenschutzzentrum informiert. Gemeinsam mit einem externen Dienstleister wurde der Vorfall untersucht und alle betroffenen Systeme wurden neu aufgebaut. Bei der Untersuchung der betroffenen Systeme wurde ein Datenabfluss aus dem Netzwerk festgestellt. Der Backup-Server des Krankenhauses war nicht von der Ransomware-Attacke betroffen. Als Ausgangspunkt für den Hacker-Angriff wurde ein VPN-Zugang mit erhöhten Rechten identifiziert. Mit diesem kompromittierten Zugang konnten sich die Angreifer im Netzwerk bewegen. Das Netzwerk wurde ausgespäht und über ausgehende RDP- und SSH-Verbindungen[61] wurde Schadsoftware ins Netzwerk eingeschleust sowie Daten exfiltriert.

Die Server wurden in Zusammenarbeit mit dem Dienstleister neu installiert. Die Daten wurden aus dem Backup zurückgeholt und in einer speziell dafür eingerichteten Zone untersucht und bereinigt, sodass keine Schadsoftware mehr im Datenbestand enthalten war. Die so aufbereiteten Daten wurden auf die neu installierten Server zurückkopiert.

Die Betroffenen wurden aufgrund der Anzahl und der Art der betroffenen Daten über die Homepage des Krankenhauses von dem Vorfall informiert. Die Betroffenen, deren personenbezogene Daten besonderer Kategorien betroffen waren, wurden individuell per Brief über den Vorfall informiert.

Hinweis für kirchliche Einrichtungen

Externe Zugänge wie z. B. VPN[62] sollten zusätzlich zum Benutzernamen und Passwort immer mit einem weiteren Faktor abgesichert sein. Verfahren wie One-Time-Passwords (OTP), die mittels App auf einem Smartphone oder einem speziell für diesen Fall konzipierten OTP-Generator erzeugt werden, bieten einen hohen Schutz. VPN-Zugänge sollten nur mit Standardbenutzerrechten ausgestattet sein. Administratoren können sich nach der VPN-Anmeldung im Netzwerk die benötigten Admin-Berechtigungen verschaffen. Höher privilegierte VPN-Benutzerkonten sollten möglichst vermieden werden.

2.2.2 Datenleck bei einem Dienstleister für Kitas und Schulen

Im März 2024 wurde ein Datenleck bei einem Unternehmen öffentlich, die Anbieter einer auf Software-as-a-Service[63] basierenden Anwendung zur Verwaltung von z. B. Kitas oder Schulen ist. Nach eigenen Angaben

[61] Remote Desktop Protocol (RDP) – ein Netzwerkprotokoll von Microsoft für den Fernzugriff auf Computer und Secure Shell (SSH) – ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke.
[62] Virtual Private Network (VPN): Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist.
[63] Bereitstellung von Anwendungsprogrammen in einer Cloud.

betreute das Unternehmen zum Zeitpunkt der Datenschutzverletzung mehr als 11.000 Einrichtungen mit mehr als 800.000 Nutzern.

Die Datenschutzverletzung wurde durch einen anonymen Hinweis an den Heise-Verlag gemeldet.[64] Der Heise-Verlag konnte die Datenschutzverletzung und die damit verbundene Sicherheitslücke verifizieren. Heise hat die bestätigte Sicherheitslücke an das Unternehmen gemeldet.

Die Sicherheitslücke bestand nach Analyse durch das Unternehmen aus zwei Komponenten. Durch einen falsch konfigurierten Webserver war der Zugriff ohne Transportverschlüsselung auf einen Teil des Servers möglich. Der Server generierte ein Directory Listing, durch das alle vorhandenen Dateien erkennbar waren und heruntergeladen werden konnten. Bei den Dateien handelt es sich um Avatarfotos aus dem Chatbereich der Anwendung, Anhänge, die mit einem Chat verschickt wurden, verschlüsselte Unterschriften der Eltern sowie ca. 1.500 Dateien mit Nutzerdaten wie z. B. Namen, Geburtsdaten, Anschriften. Bei diesen Dateien handelt es sich zugleich um die zweite fehlerhafte Komponente: Fehlgeschlagene Importversuche der Einrichtungen. Wurde ein Datenimport mit einem Fehler abgebrochen, wurde die Datei nicht gelöscht, sondern auf dem Server im zugänglichen Verzeichnis abgelegt.

Unter den 11.000 Einrichtungen waren auch katholische Einrichtungen als Kunden bei dem Unternehmen angelegt. Das Unternehmen arbeitet gemäß § 29 KDG als Auftragsverarbeiter und hat im Rahmen der Informationspflicht alle Auftraggeber über den Vorfall informiert. Bei dieser Information wurden nicht nur aktuelle Kunden, sondern auch Kunden aus der Vergangenheit informiert, da diese ebenso von der Datenschutzverletzung betroffen sein konnten. Durch die Verarbeitung der Daten im Auftrag nach § 29 KDG sind die Einrichtungen weiter verantwortlich für die Daten. Beim Katholischen Datenschutzzentrum sind Meldungen der einzelnen Einrichtungen sowie Sammelmeldungen ganzer Bistümer eingegangen.

Das Unternehmen hat kurzfristig nach Bekanntwerden der Datenschutzverletzung die Sicherheitslücke geschlossen und auf der Internetseite einen FAQ-Bereich eingerichtet, der regelmäßig aktualisiert wurde. Das Unternehmen hat in diesem Fall gut mit dem Katholischen Datenschutzzentrum zusammengearbeitet. Betroffene konnten kurzfristig durch die Einrichtungen informiert werden.

Hinweis für kirchliche Einrichtungen

Auftragsverarbeitung nach § 29 KDG belässt – wie in diesem Falle einer Software-as-a-Service Anwendung – die Verantwortlichkeit für die Daten bei der Einrichtung. Im Falle einer Datenschutzverletzung muss der Verantwortliche die Meldung der Datenschutzverletzung und ggf. die Information der Betroffenen durchführen.

[64] Über den Vorgang berichtete die c´t in dem Artikel „Fatale Fehlkonfiguration" von Holger Bleich und Sylvester Tremmel, c´t 2024, Heft 9, Seite 32 f.

2.2.3 Datenpanne bei E-Mail-Verteilern in einer (Erz-) Diözese

Bei einem externen Dienstleister, der von einer (Erz-)Diözese für den Versand von Newslettern genutzt wird, wurde ein Sub-Account[65] des Verantwortlichen kompromittiert. Da kein Brute-Force-Angriff[66] beim Dienstleister erkennbar war, kann davon ausgegangen werden, dass die Zugangsdaten bekannt waren. Diese könnten beispielsweise durch einen vorangegangenen Phishing-Angriff bereits erbeutet worden sein. Dies konnte im Rahmen der Sachverhaltsermittlung aber nicht mit Sicherheit geklärt werden.

Über den kompromittierten Account hatte der Angreifer Zugriff auf verschiedenste Mailinglisten und hat eine Phishing-E-Mail an einen großen Empfängerkreis verschickt. Direkt nach Bekanntwerden des Versandes der E-Mail wurde über den Haupt-Account des Dienstleisters der betroffene Sub-Account gesperrt und alle Empfänger der Phishing-E-Mail informiert.

Analysen beim Dienstleister haben ergeben, dass durch den Angreifer nur der Versand von einer Phishing-E-Mail durchgeführt wurde. Es wurden keine Daten aus dem Portal des Versanddienstleisters heruntergeladen.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt, auch bei externen Dienstleistern personalisierte Accounts/Logins zu verwenden. Als Passwortrichtlinie sollten bei externen Accounts mindestens die gleichen Anforderungen an ein Passwort gelten wie im internen Netzwerk. Weiterhin ist es empfehlenswert, eine Multi-Faktor-Authentifizierung bei externen Accounts zu aktivieren. Bietet der Dienstleister diese Optionen nicht als durchsetzbare Richtlinie an, ist eine Durchsetzung als organisatorische Maßnahme, z. B. als Arbeitsanweisung, in Erwägung zu ziehen.

2.2.4 Offenlegung der Userverzeichnisse im Netzwerk

Durch manuelle Änderung der Berechtigungsstruktur wurden bei einem Verantwortlichen die Benutzerprofile auf dem Server für alle 5.000 Mitarbeitenden untereinander zugänglich. Jeder Benutzer hätte die Benutzerprofile der anderen einsehen können.

In den Benutzerprofilen sind hauptsächlich Konfigurationsdateien für den Betrieb abgelegt. Da der Desktop Teil des Profils ist, konnten alle Dateien und Dokumente, die auf dem Desktop der Anwender abgelegt waren, eingesehen werden. Weitere Serverlaufwerke, wie z. B.

[65] Unter-Account mit eingeschränkten Berechtigungen zu einem Haupt-Account.
[66] Ein Brute-Force-Angriff ist eine Methode zur Datenentschlüsselung und Passwortsuche, bei der alle möglichen Kombinationen ausprobiert werden, bis die Richtige gefunden ist. Es ist gewissermaßen ein Raten durch systematisches Ausprobieren aller Möglichkeiten.

die Home-Laufwerke der Anwender, waren nicht von der geänderten Berechtigungsstruktur betroffen.

Nach Bekanntwerden der Datenschutzverletzung wurden die korrekten Berechtigungen wiederhergestellt. Da nicht festgestellt werden konnte, ob unberechtigte Zugriffe auf die Profile anderer Anwender stattgefunden haben, wurden alle Anwender über diesen Vorfall informiert. Mit dieser Information wurden alle Anwender aufgefordert, keine Dokumente mehr auf dem Desktop abzulegen, sondern lediglich Verknüpfungen zu den Dokumenten auf dem Desktop zu speichern.

Diese Maßnahmen des Verantwortlichen führen zu kleineren Userprofilen auf dem Server. Dies kann den An- und Abmeldevorgang erheblich beschleunigen und gleichzeitig die Sicherheit erhöhen. Dokumente liegen in einer anderen Berechtigungsstruktur, z. B. den Home-Laufwerken, die durch spezielle Berechtigungen geschützt sind.

Hinweis für kirchliche Einrichtungen

Für große Umgebungen mit komplexen Berechtigungsstrukturen können Tools von Drittanbietern helfen, die die Berechtigungsvergabe steuern und geplante Berechtigungsänderungen vor der Anwendung simulieren und ggf. Hinweise liefern können.

2.2.5 Unverschlüsselter Versand eines Screenshots mit Gesundheitsdaten an einen EDV-Anbieter

In einem Krankenhaus wurde zur Fehleranalyse ein Screenshot eines OP-Plans angefertigt und an den zuständigen Dienstleister per E-Mail verschickt. Es wurden nicht alle personenbezogenen Daten auf dem Screenshot unkenntlich gemacht und die E-Mail unverschlüsselt an den Dienstleister verschickt.

Direkt nach Bekanntwerden der Datenschutzverletzung wurde der Dienstleister aufgefordert, den Screenshot mit den personenbezogenen Daten zu löschen.

Die Löschung wurde bestätigt und da es sich bei den personenbezogenen Daten der betroffenen Personen um besondere Kategorien von personenbezogenen Daten gemäß § 4 Nr. 2 KDG handelt, wurden diese über den Vorfall informiert.

Die Mitarbeitenden des Verantwortlichen wurden nochmals sensibilisiert und das Thema wurde für alle Mitarbeitenden in den regelmäßigen Datenschutz-News noch einmal aufgegriffen.

Hinweis für kirchliche Einrichtungen

Die regelmäßige Information und Sensibilisierung der Mitarbeitenden hilft, dass der Datenschutz im täglichen Betrieb gelebt wird und dass die Mitarbeitenden über aktuelle Themen informiert sind.

2.2.6 Veröffentlichung von Beförderungslisten für Bustransporte im Intranet

Bei einem Verantwortlichen werden Beförderungslisten für Bustransporte erstellt. Diese Listen dienen als Hilfe und Anwesenheitskontrolle für die Busaufsicht. Die Listen enthalten Namen, Anschrift, Telefonnummern der zu befördernden Personen und teilweise Gesundheitsdaten.

Damit alle Busaufsichten diese Listen einsehen können, wurden die Listen im Intranet des Verantwortlichen zur Verfügung gestellt. Durch einen Fehler im Berechtigungskonzept des Intranets waren diese Listen für alle ca. 1.500 Mitarbeitenden des Verantwortlichen einsehbar. Eine Zugriffsprotokollierung innerhalb des Intranets findet nicht statt, daher konnten unberechtigte Zugriffe auf die Listen nicht ausgeschlossen werden.

Eine Information aller betroffenen Personen wurde umgehend durchgeführt. Die Listen wurden direkt nach Bekanntwerden der Datenschutzverletzung aus dem Intranet entfernt. Die zuständigen Mitarbeitenden, die die Listen erstellen und mit diesen arbeiten, wurden sensibilisiert und das Berechtigungskonzept im Intranet wurde durch die IT angepasst.

2.2.7 Veröffentlichung privater E-Mail-Adressen auf der Homepage einer Bildungseinrichtung

Auf der Homepage einer kirchlichen Bildungseinrichtung kam es zu einer ungewollten Veröffentlichung privater E-Mail-Adressen von Dozenten. Betroffen waren E-Mail-Adressen sowohl der Dozenten dieser Bildungseinrichtung, wie auch die privaten E-Mail-Adressen von Dozenten einer anderen Bildungseinrichtung.

Ursache für die ungewollte Veröffentlichung war ein Bearbeitungsfehler einer mitarbeitenden Person der Agentur, die mit der Pflege der Homepage des kirchlichen Auftraggebers beauftragt war. Nachdem der Fehler bemerkt und behoben wurde, erfolgte eine Klärung seitens der beteiligten Stellen, wie es zu der Veröffentlichung und Vermischung von Daten kommen konnte.

Ursache für die Vermischung von Daten waren Einträge in den Datenbanken, aus denen die jeweiligen Seiten ihre Informationen zur Anzeige generierten und die teilweise als Vorlage für Seiten anderer Auftraggeber verwendet worden waren. Die Vermischung wurde begünstigt durch die Unkenntnis der Mitarbeitenden über diesen Umstand. Als Folge eines Missverständnisses in einem Telefonat wurden die unpassenden Daten für die Veröffentlichung freigeben.

Bei der Klärung des Vorgangs legte das Katholische Datenschutzzentrum den Schwerpunkt auf die Verhinderung einer Wiederholung dieses Vorgangs. Es sollten Maßnahmen ergriffen werden, die den Eintritt einer derartigen Datenschutzverletzung für die Zukunft vermeiden. Daraufhin wurden die Freigabeprozesse zwischen der kirchlichen Einrichtung und der Agentur so geändert, dass einer Veröffentlichung von Seiten immer eine Freigabe seitens des Auftraggebers vorangeht.

Zudem wurden die technischen Zusammenhänge und der Rückgriff auf gespeicherte Vorlagen innerhalb der Agentur neu geregelt, um ungewollte Übernahmen von Daten zu verhindern.

2.2.8 Weitergabe von Informationen zur Arbeitsunfähigkeit von Kolleginnen und Kollegen an die Presse

Die Einrichtungsleitung einer Kindertagesstätte erfuhr aus der Zeitung, dass ihre Arbeitsunfähigkeit offensichtlich im Rahmen der Recherche einer Lokalredaktion zu aktuellen Auswirkungen des Kinderbildungsgesetzes NRW auf die Arbeit von Kindertageseinrichtungen, von einer mitarbeitenden Person der eigenen Einrichtung preisgegeben worden war. Diese hatte die Abwesenheit der Einrichtungsleitung im Zuge eines Telefonates erwähnt.

Die Pressevertreter hatten bereits mehrere Einrichtungen kontaktiert um ihre Fragen zu stellen. Der Träger der Einrichtungen hatte im Vorfeld angewiesen, der Presse keine Fragen zu beantworten, sondern an die Pressestelle des Trägers zu verweisen. Trotzdem kam es durch die unbedachte Auskunft zu einer Offenlegung von Daten der besonderen Kategorie, da durch die Kombination der öffentlich bekanntgemachten Informationen (Bezeichnung der Einrichtung und Funktion der betroffenen Person) auf die betroffene Person geschlossen werden konnte.

2.2.9 Offenlegung von Gesundheitsdaten im Netzwerk eines Krankenhauses

In einem Krankenhaus sollte ein Arztbrief elektronisch abgelegt werden. Durch einen individuellen Fehler wurde der Brief in einem Verzeichnis abgelegt, das als Systemlaufwerk diente und vorrangig technische Bedeutung für den Betrieb von verwendeten Anwendungen hatte. Auf dieses Verzeichnis konnte jedoch ein größerer Kreis von Mitarbeitenden zugreifen.

Nachdem dieses Problem erkannt worden war, erfolgte unverzüglich die Löschung der Datei und eine Überarbeitung der Berechtigungsstruktur durch die IT-Abteilung, um den Zugriff auf dieses Verzeichnis bedarfsgerecht einzurichten und sicherzustellen.

Ein fachlich abgestimmtes und aktuelles Berechtigungskonzept für die Verzeichnisse hätte hier die fehlerhafte Ablage des Arztbriefes mit den sensiblen Daten und die daraus resultierende unberechtigte Offenlegung von Daten mit der Verletzung der Vertraulichkeit der Daten verhindern können.

Auch die Daten in internen Netzlaufwerken dürfen nur von den Mitarbeitenden eingesehen werden können, die im Rahmen ihrer fachlichen Aufgaben Zugriff auf diese Daten benötigen.

„Auch die Daten in internen Netzlaufwerken dürfen nur von den Mitarbeitenden eingesehen werden können, die im Rahmen ihrer fachlichen Aufgaben Zugriff auf diese Daten benötigen."

2.2.10 Bildaufnahmen von Patienten mit dem Privathandy und Weitergabe der Aufnahmen über WhatsApp

Ein immer wieder auftretendes Problem vor allem in Krankenhäusern und Pflegeeinrichtungen ist, dass Mitarbeitende Fotos oder Videos zu privaten Zwecken während der Arbeit von den zu behandelnden oder zu pflegenden Personen machen. Diese Fotos und Videos werden dann anderen Personen im privaten Rahmen gezeigt oder per Messenger verschickt.

So hatte beispielsweise in einem konkreten Fall im Berichtszeitraum eine Mitarbeitende eines Pflegedienstes von verschiedenen Patienten Bilder (Fotos und Videos) aufgenommen und diese dann auch über einen Messengerdienst weitergeleitet. Eine Einwilligung der abgelichteten Personen lag nicht vor.

Dieses Verhalten ist datenschutzrechtlich unzulässig und verstößt wahrscheinlich auch gegen arbeitsrechtliche Vorgaben. Werden solche Fälle bekannt, kann dies arbeitsrechtliche Konsequenzen haben. Die Mitarbeitenden sind in solchen Fällen auch datenschutzrechtlich für ihr Handeln verantwortlich, da sie diese Aufnahmen nicht im Auftrag oder für Ihren Arbeitgeber aufgenommen haben, sondern für private Zwecke und unter Überschreitung ihrer Pflichten und Aufgaben als Angestellte. Dies bedeutet auch, dass sich eventuelle datenschutzrechtliche Bußgelder oder Schadensersatzansprüche gegen die Angestellten direkt richten können.

Auch wenn es sich hier um ein eigenmächtiges Handeln der Mitarbeitenden handelt, ist die kirchliche Einrichtung als Arbeitgeber nicht ganz aus dem Fokus der Datenschutzaufsicht. Die Aufsicht schaut in diesen Fällen, ob die Einrichtung als die für die Verarbeitung der personenbezogenen Daten der behandelten oder betreuten Personen verantwortliche Stelle, alle notwendigen technischen oder organisatorischen Schutzmaßnehmen ergriffen hat, um solche Vorfälle bestmöglich zu verhindern. Hier sollten organisatorische Maßnahmen ergriffen worden sein, wie beispielsweise ein in einer internen Anweisung niedergeschriebenes Verbot, die behandelten oder betreuten Personen aus nicht-dienstlichen Gründen zu fotografieren beziehungsweise zu filmen. Außerdem sollte eine regelmäßige Schulung zu den wichtigen Datenschutzthemen rund um den konkreten Arbeitsalltag der Mitarbeitenden erfolgen, um u. a. darüber ein datenschutzgerechtes Verhalten der Mitarbeitenden zu fördern.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt, die Datenschutz-Schulungskonzepte für (neue) Mitarbeitende – nicht nur in Bezug auf Privathandys und Messengerdienste – laufend zu überprüfen und zu aktualisieren und die Schulungen ausreichend häufig durchzuführen. Außerdem sollte in internen Vorgaben ausdrücklich vorgegeben sein, was im Umgang mit den personenbezogenen Daten der behandelten oder betreuten Personen erlaubt oder eben verboten ist.

2.3 Beschwerden und Hinweise

Jede Person, die der Ansicht ist, dass die Verarbeitung ihrer personenbezogenen Daten gegen Vorschriften über den Datenschutz verstößt, hat nach § 48 KDG das Recht, sich mit einer Beschwerde an die zuständige Datenschutzaufsichtsbehörde zu wenden. Das Recht auf Beschwerde besteht unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs. Eine Beschwerde wird als Hinweis gewertet, wenn die meldende Person nicht persönlich betroffen ist.

Wenn eine Beschwerde beim Katholischen Datenschutzzentrum eingeht, wird die Gegenseite zur Stellungnahme zum vorgetragenen Sachverhalt aufgefordert. Dies ist aber nur dann zeitnah möglich, wenn die Beschwerde alle wichtigen Informationen zum Beschwerdesachverhalt und zur betroffenen Person enthält. Damit es hier nicht zu Verzögerungen kommt, empfiehlt das KDSZ, die Beschwerde über das Beschwerdeformular auf der Homepage einzureichen. So ist nicht nur sichergestellt, dass die für die Bearbeitung der Beschwerde notwendigen Informationen mitgeteilt, sondern auch, dass die Informationen gesichert übermittelt werden. Personenbezogene Daten sollten grundsätzlich nur auf gesichertem Weg übermittelt werden.

Eine weitere mögliche Verzögerung in der Bearbeitung kann sich ergeben, wenn die Beschwerde bei einer örtlich oder sachlich unzuständigen Aufsichtsbehörde eingereicht wird. Wird eine Beschwerde in Deutschland bei einer unzuständigen Datenschutzaufsicht eingereicht, leitet die Aufsicht die Beschwerde – wenn gewünscht – an die zuständige Stelle weiter. Bei Fragen zur Zuständigkeitsabgrenzung der Datenschutzaufsichten der (Erz-)Diözesen, der päpstlichen Orden und der Landesdatenschutzbeauftragten für Einrichtungen im kirchlichen Bereich und deren Umfeld steht das Katholische Datenschutzzentrum gern zur Verfügung.

Die folgenden Grafiken stellen eine Übersicht der im Jahr 2024 an das Katholische Datenschutzzentrum herangetragenen Beschwerden und Hinweise dar. Einzelne Vorgänge werden in diesem Abschnitt aufgegriffen und erläutert.

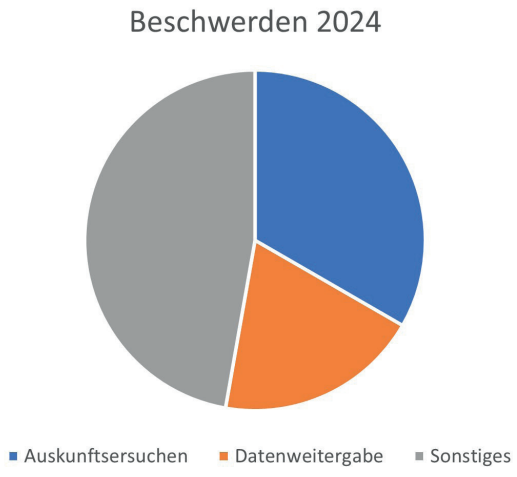


Abb. 4: Beschwerden an das KDSZ im Jahr 2024.

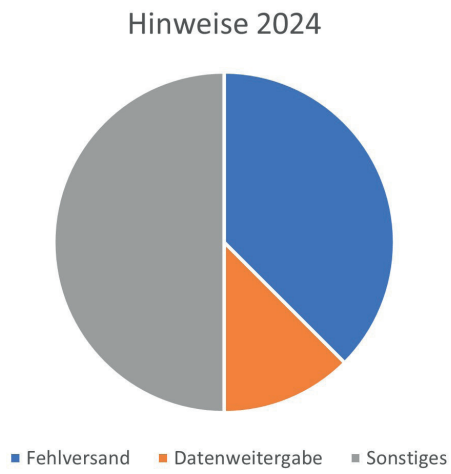


Abb. 5: Hinweise an das KDSZ im Jahr 2024.

2.3.1 Beschränkung des Auskunftsrechts

Im Berichtszeitraum war die Anzahl von Beschwerden bezüglich nicht, nicht rechtzeitig oder vermeidlich unvollständig beantworteter Auskunftsersuchen gemäß § 17 KDG unverändert hoch. Auch die Problembereiche waren in etwa dieselben wie in den Vorjahren.[67]

In diesem Berichtzeitraum kam es aber häufiger zu Beschwerden, die beim Katholischen Datenschutzzentrum eingelegt wurden, weil die Beschwerdeführer aufgrund von Schwärzungen in den ihnen erteilten Auskünften (beziehungsweise Kopien) von einer unvollständigen Auskunft ausgingen. Dabei wurde der Auskunft- und Kopieanspruch häufig als ein absolutes, nicht einschränkbares Recht verstanden.

Richtig ist, dass nach § 17 Abs. 1 und 3 KDG jede betroffene Person grundsätzlich ein Recht auf Auskunft und Kopie über alle ihre personenbezogenen Daten hat, die beim jeweiligen Verantwortlichen verarbeitet werden. Das Recht auf Auskunft und Kopie wird allerdings in bestimmten Fällen eingeschränkt. Das geschieht zum Beispiel zum Schutz der überwiegenden Rechte Dritter nach § 17 Abs. 6 lit. a) i. V. m. § 15 Abs. 5 lit. a) KDG. Dabei muss der Verantwortliche im Rahmen einer Interessenabwägung einschätzen, ob die Rechte des Dritten oder das Recht auf Auskunft und Kopie der betroffenen Person überwiegt. Diese Abwägung stellt immer eine Einzelfallentscheidung dar und kann nicht kategorisch erfolgen.

[67] Siehe Abschnitt 2.5.1 des Jahresberichts 2021, Abschnitt 2.3.1 des Jahresberichts 2022 und Abschnitt 2.3.2 des Jahresberichts 2023.

Hinweis für kirchliche Einrichtungen

Um Beschwerden in diesem Zusammenhang zu vermeiden, sollten Verantwortliche ihre Pflichten aus § 17 Abs. 7 KDG beachten und ihre Auskünfte beziehungsweise den Prozess dahinter für Betroffene transparent machen und Schwärzungen stets und einzelfallbezogen erläutern. Eine entsprechende Dokumentation für die (begründeten) Schwärzungen erleichtert außerdem die Kontrolle durch die Aufsichtsbehörde.

2.3.2 Veröffentlichung von Kinderfotos

Häufig sind (versehentlich) veröffentlichte Kinderfotos in Kindertageseinrichtungen Gegenstand von Beschwerdeverfahren im Berichtszeitraum gewesen. Dabei mangelte es selten am Bewusstsein der Einrichtungen, die Verarbeitung nur mit einer geeigneten Rechtsgrundlage durchzuführen.

Viel eher waren Beschwerden zu Veröffentlichungen von Kinderfotos (z. B. Gruppenbildern) durch Aushang oder woanders auf eine fehlende Kontrolle einer Einwilligung für die bestimmte Art des Fotos zurückzuführen. In einigen Fällen lag beispielsweise eine Einwilligung für Gruppenfotos für die Fotomappen der Kinder, aber nicht für Aushänge vor den Gruppenräumen vor.

Verantwortlichen ist daher zu raten, dass Mitarbeitende wiederholt im Umgang mit Fotos geschult werden, um ein akutes Bewusstsein für die Prüfung des Vorliegens einer Einwilligung zu verstärken und so Beschwerdeverfahren in diesem Bereich zu vermeiden.

Hinweis für kirchliche Einrichtungen

Für Fotos, auf denen Personen zu sehen sind, muss in der Regel eine zweckgebundene Einwilligungserklärung vorliegen. Dabei sollten Verantwortliche außerdem darauf achten, dass:

- Fotos nur von Kita Personal und nicht von Eltern, abholenden oder sonstigen Personen,
- nur mit Dienstgeräten zu dienstlichen Zwecken,
- nicht von sensiblen Situationen angefertigt werden.

Darüber hinaus sind Fotos zu löschen, sobald der Zweck entfällt.[68]

[68] Zu Einzelheiten mit den Voraussetzungen zum Umgang mit Bildern von Kindern und Jugendlichen siehe den Beschluss der Konferenz der Diözesandatenschutzbeauftragten vom 04.04.2019 (https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2019/05/KDB-Umgang-mit-Bildern-von-Kindern-und-Jugendlichen-vom-04.04.2019.pdf) oder Abschnitt 2.3 der Praxishilfe „Datenschutz im Kindergarten" der KDSA Ost (https://www.kdsa-ost.de/images/CONTENT/INFOTHEK/Mpraxishilfen/dok/PH-KITA_Datenschutz_im_Kindergarten_1.0.pdf).

2.3.3 Umgang mit Adressen beim Versand von Newslettern

Im Berichtszeitraum wurden an das Katholische Datenschutzzentrum einige Sachverhalte im Zusammenhang mit dem Versand von Newslettern herangetragen. Dabei waren öfter kirchliche Einrichtungen beteiligt, die sich noch manuell erzeugter beziehungsweise gepflegter E-Mail-Verteilerlisten bedienen, um darüber regelmäßig mithilfe lokal installierter E-Mail-Anwendungen (z. B. Outlook, Thunderbird) Nachrichten an feste Empfänger zu versenden. Hierbei zeigte sich, dass die Pflege der E-Mail-Adressen der Abonnenten aufwendig und fehleranfällig sein kann und immer wieder die Gefahr besteht, versehentlich den Verteiler offen zu verwenden (also das „AN"-Feld zu füllen), anstatt die E-Mail mithilfe des „BCC"-Feldes (blind carbon copy = nicht sichtbare Kopie, Blindkopie) zu versenden.

Aber auch bei der Verwendung systemgestützter Newsletter-Systeme ist Sorgfalt im Umgang mit den Adressen geboten. Beispiel dafür war in 2024 ein beim Katholischen Datenschutzzentrum eingegangener Hinweis, bei dem sich ein verzweifelter, unfreiwilliger Abonnent eines Newsletters an das Katholische Datenschutzzentrum wandte. Er hatte mehrfach das Abo eines Pfarrbriefes einer Pfarrei automatisiert gekündigt, was ihm durch das verwendete Newsletter-System auch bestätigt wurde. Trotzdem erhielt er immer wieder den nicht mehr erwünschten Newsletter und vermutete eine mehrfache, unberechtigte Speicherung seiner Daten. Diese Situation wurde von dem Empfänger auch direkt gegenüber der Pfarrei kundgetan, was aber keine Abhilfe brachte. Nach Intervention des Katholischen Datenschutzzentrums wurde die Situation geprüft und so abgeschlossen, dass am Ende die Löschung der Daten aus dem Newsletter-System erfolgte und gegenüber dem Betroffenen eine Erklärung und Entschuldigung erfolgte. Die Erfahrung aus diesem Vorgang zeigt, dass auch bei der Verwendung von Newsletter-Systemen eine Kontrolle der Funktionen und zeitnahe Reaktion auf berechtigte Hinweise von Betroffenen notwendig sind, um das Vertrauen von Abonnenten in den Dienst nicht zu gefährden.

Hinweis für kirchliche Einrichtungen

Bei manuell versendeten Newslettern wird durch das Katholische Datenschutzzentrum empfohlen, von der nicht zufriedenstellenden manuellen Lösung auf eine systemgestützte Lösung zu wechseln. Dies ist sowohl mit auf eigenen Servern installierten Systemen als auch durch von einschlägigen Dienstleistern angebotenen Newsletter-Systemen möglich. Damit können manuelle Fehler bei der Versendung der Newsletter vermieden und die Verwaltung der Empfänger der Newsletter (An-/Abmeldung) vereinfacht werden.

2.3.4 Abruf von Protokollen über eine Online-Dateiablage

Im Berichtszeitraum richtete sich eine Beschwerde gegen die Verarbeitung personenbezogener Daten über eine Online-Dateiablage. Konkret ging es dabei um im Rahmen einer Pflegeelternschaft durch einen katholischen Verein erhobene und verarbeitete (sensible) Daten.

Der Beschwerdeführer wendete sich gegen eine unrechtmäßige Verarbeitung seiner personenbezogenen Daten, die Nichtbeachtung der Informationspflicht sowie unzureichende technische und organisatorische Maßnahmen durch den katholischen Verein (Beschwerdegegner).

Der Beschwerdeführer gab an, dass mit dem Verein und dem Jugendamt regelmäßig Gespräche durchgeführt werden. Dabei werde ein Protokoll mit der Adresse des Beschwerdeführers sowie der Lebenssituation angefertigt, welches der Beschwerdeführer im Nachgang über einen Downloadlink der Online-Dateiablage erhalte. Der Link werde per E-Mail zugeschickt, das Passwort zu dem Link mit einer zweiten E-Mail. Keine der E-Mails sei dabei verschlüsselt.

Dazu gab der Beschwerdeführer an, dass weder in der Datenschutzerklärung auf der Internetseite des Vereins, noch auf der Seite der Online-Dateiablage Angaben zur Verarbeitung der personenbezogenen Daten in der Online-Dateiablage gemacht würden. Eine Einwilligung für die Verarbeitung der personenbezogenen Daten in der Online-Dateiablage war nicht erteilt worden.

Dem Katholischen Datenschutzzentrum wurde mitgeteilt, dass im Jahr 2017 die bis dahin postalische Übermittlung des Protokolls der Gespräche auf einen elektronischen Abruf mithilfe einer Online-Dateiablage umgestellt worden ist. Hierüber wurde der Beschwerdeführer seinerzeit vom Beschwerdegegner mit einem Schreiben informiert. Eine Information mit einem Inhalt, wie ihn § 15 Abs. 1 und 2 KDG vorschreibt, ist nicht erfolgt.

Seit der Umstellung im Jahr 2017 wurde vom Beschwerdegegner zum Abruf des Dokuments ein Downloadlink per E-Mail mitgeteilt. Die Online-Dateiablage des Beschwerdegegners ist als unabhängige Cloud-Speicherplattform auf dem Server des Beschwerdegegners installiert, der sich in dessen Räumlichkeiten befindet. Zur Wartung und Administration besteht ein Vertrag über eine Verarbeitung personenbezogener Daten im Auftrag mit einer Software-Firma. Es gibt keine Unterauftragnehmer.

Datenschutzrechtlich problematisch war hier die Übermittlung des Links für den Download von Dokumenten mit (sensiblen) personenbezogenen Daten des Beschwerdeführers als auch des zugehörigen Passworts per E-Mail ohne ausreichende Schutzmaßnahmen (Verschlüsselung).

Personenbezogene Daten müssen nach § 7 Abs. 1 lit. f) KDG in einer Weise verarbeitet werden, die eine dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessene Sicherheit gewährleistet. Es sind gemäß §§ 26, 27 KDG geeignete technische und organisatorische Maßnahmen zu treffen und einzuhalten, um die personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen. Zu diesen Maßnahmen zählt nach § 26 Abs. 1 Satz 2 KDG insbesondere auch die Verschlüsselung personenbezogener Daten.

Der Verantwortliche hat gemäß § 5 Abs. 1 KDG-DVO sicherzustellen, dass bei der Verarbeitung durch innerbetriebliche Organisation und mittels technischer und organisatorischer Maßnahmen die Einhaltung des Datenschutzes gewährleistet wird. Hierzu sind unter Berücksichtigung

von § 26 KDG die in § 6 KDG-DVO aufgeführten Maßnahmen zu treffen. Nach § 6 Abs. 2 lit. b) und lit. d) KDG-DVO sind Maßnahmen zu erreifen, mit denen verhindert wird, dass Unbefugte IT-Systeme nutzen können und dass die Daten unter anderem auch während ihrer Übermittlung gegen unbefugtes Auslesen geschützt sind. Da das Gesprächsdokument in diesem Fall alle Kategorien personenbezogener Daten umfasst, gilt § 13 KDG-DVO, was auch die Vorgabe der Verschlüsselung nach § 12 Abs. 2 Satz 2 lit. e) KDG-DVO umfasst.

Da der Beschwerdegegner den Beschwerdeführer nicht über die Verarbeitung seiner Daten mit der Online-Dateiablage den gesetzlichen Vorgaben entsprechend informiert hatte, hat er außerdem gegen die Informationspflicht nach § 15 KDG verstoßen.

Die Beschwerde war aber unbegründet, soweit sich der Beschwerdeführer gegen eine unrechtmäßige Verarbeitung seiner personenbezogenen Daten wegen nicht erteilter Einwilligung gewandt hatte. Für die Verarbeitung der Daten des Beschwerdeführers auf der Online-Dateiablage in der vorliegenden Ausgestaltung ist keine Einwilligung erforderlich. Die Verarbeitung mithilfe der Online-Dateiablage, mit der die Daten auf dem Server in den Räumen des Beschwerdegegners gespeichert und zum Abruf durch den Beschwerdeführer bereitgehalten werden, konnte auf eine spezielle Rechtsgrundlage gestützt werden.

Als Ergebnis der Beschwerde hat der Beschwerdegegner mitgeteilt, die Übermittlung von Link und Passwort so neu zu gestalten, dass der Link per E-Mail und das Passwort (fern-)mündlich mitgeteilt werden. Außerdem hat der Beschwerdegegner angegeben, seiner Informationspflicht nach § 15 KDG nunmehr nachzukommen.

2.4 Prüfungen

„Das Katholische Datenschutzzentrum führt regelmäßig solche Prüfungen durch, um sicherzustellen, dass die … Datenschutzvorschriften eingehalten werden und damit die personenbezogenen Daten geschützt sind.“

Datenschutzüberprüfungen gehören nach § 44 KDG zu den Aufgaben der Datenschutzaufsicht. Der Diözesandatenschutzbeauftragte beziehungsweise das Katholische Datenschutzzentrum führt regelmäßig solche Prüfungen durch, um sicherzustellen, dass die Vorschriften des kirchlichen Datenschutzgesetzes und anderer Datenschutzvorschriften eingehalten werden und damit die personenbezogenen Daten geschützt sind.

Im Rahmen von anlassunabhängigen Prüfungen schaut sich das Katholische Datenschutzzentrum meist einen Querschnitt kirchlicher Einrichtungen an, die zu einem bestimmten Thema befragt und teilweise auch vor Ort geprüft werden. Mit diesen Querschnittsprüfungen will das Katholische Datenschutzzentrum sich einen Überblick über den Zustand beziehungsweise die Umsetzung des Datenschutzes zu einem bestimmten Thema verschaffen und gleichzeitig die Sensibilität der Einrichtungen für dieses Thema erhöhen. Je nach Thema kann auch die anlassunabhängige Prüfung der Verarbeitung bestimmter Daten bei nur einer Einrichtung Gegenstand der Prüfung sein. Über größere anlassunabhängige geplante, laufende und abgeschlossene Prüfungen

informiert das Katholische Datenschutzzentrum auf seiner Internetseite[69].

Im Berichtszeitraum wurden zwar anlassunabhängige Prüfungen durchgeführt. Diese Prüfungen konnten im Prüfungszeitraum aber noch nicht abgeschlossen werden.

Neben den anlassunabhängigen Prüfungen führt das Katholische Datenschutzzentrum auch anlassbezogene Prüfungen einzelner Einrichtungen durch. Diesen Prüfungen liegen Meldungen, Beschwerden oder andere Erkenntnisse zur Verarbeitung von personenbezogenen Daten durch diese Einrichtungen zugrunde, die einer Überprüfung der Verarbeitung der Daten im Rahmen einer Prüfung angeraten erscheinen lassen.

2.5 Aufsichtsbehördliche Maßnahmen: Bußgelder

Im Rahmen einer Prüfung hat das Katholische Datenschutzzentrum im Berichtszeitraum zwei Bußgelder in dreistelliger Höhe verhängt. Die beiden Einrichtungen hatten sich auf mehrfache Schreiben des Datenschutzzentrums nicht gemeldet. Aufgrund der fehlenden Rückmeldung sah die Aufsicht es als notwendig an, die gesetzlich vorgesehene Mitwirkungspflicht mit einem Bußgeld einzufordern.

2.6 Austausch mit den betrieblichen Datenschutzbeauftragten der (Erz-)Bistümer und der Diözesan-Caritasverbände

Das Katholische Datenschutzzentrum war auch in diesem Berichtszeitraum regelmäßiger Gast bei den Treffen der betrieblichen Datenschutzbeauftragten der Generalvikariate und der Diözesan-Caritasverbände und stand so auch durch direkten Kontakt in stetem Austausch mit diesen betrieblichen Datenschutzbeauftragten.

Im Berichtsjahr fanden wieder mehrere Treffen statt, bei denen aktuelle und grundsätzliche Fragen und Sachverhalte diskutiert wurden. So wurden im Berichtszeitraum zusammen mit dem Katholischen Datenschutzzentrum beispielsweise Fragen rund um die in den Einrichtungen genutzten Anwendungen besprochen. Weitere Beratungspunkte waren u. a. die Vereinheitlichung von Formularen/Datenschutzhinweisen, die KDG-Novellierung[70] und die Auswirkungen beziehungsweise die Umsetzung der KI-Verordnung[71] in den kirchlichen Einrichtungen.

[69] https://www.katholisches-datenschutzzentrum.de/themen/pruefungen/
[70] Siehe Abschnitt 1.3.1 dieses Jahresberichts
[71] Siehe Abschnitt 1.1.4 dieses Jahresberichts.

2.7 Benennen eines betrieblichen Datenschutzbeauftragten

> **„Das Bekleiden einer Führungsposition mit Verantwortung für die Datenverarbeitung und die [gleichzeitige] Ausübung der Funktion des Datenschutzbeauftragten dürften … gegen das Benennungsverbot aus § 36 Abs. 7 S. 1 KDG verstoßen."**

Im Berichtzeitraum kam es vereinzelt dazu, dass Einrichtungen dem KDSZ Datenschutzbeauftragte gemeldet haben, die gleichzeitig Führungspositionen in den Einrichtungen ausüben, wie beispielsweise die Geschäftsführung oder die Verwaltungsleitung. Das Bekleiden einer Führungsposition mit Verantwortung für die Datenverarbeitung und die Ausübung der Funktion des Datenschutzbeauftragten dürften allerdings grundsätzlich gegen das Benennungsverbot aus § 36 Abs. 7 S. 1 KDG verstoßen.

Einrichtungen die nach § 36 Abs. 1 oder 2 KDG einen Datenschutzbeauftragten benennen müssen, können für diese Aufgabe nach § 36 Abs. 5 S. 1 Alt. 1 KDG einen betriebsinternen Mitarbeitenden auswählen, wenn diese Person die erforderliche Fachkunde und Zuverlässigkeit gemäß § 36 Abs. 6 KDG besitzt. Die Möglichkeit einen Datenschutzbeauftragten betriebsintern zu benennen wird allerdings durch § 36 Abs. 7 KDG eingeschränkt. So darf der betriebliche Datenschutzbeauftragte nicht gleichzeitig eine Funktion ausüben, bei der er für einen Teil oder die gesamte Verarbeitung personenbezogener Daten der Einrichtung verantwortlich ist (z. B. als Geschäftsführung oder Leitung der Personalabteilung oder der IT-Abteilung). Der kirchliche Gesetzgeber versucht durch diese Einschränkung Interessenkonflikten vorzubeugen. Das bloße Innehaben einer Führungs- oder Leitungsposition führt allerdings nicht automatisch zu einem Interessenkonflikt. Entscheidend sind die Nähe der Person zu den Verantwortlichen im Sinne des KDG sowie eine umfassende Betrachtung der aktuellen und zukünftigen Aufgaben und Pflichten der zu benennenden Person.[72]

2.8 Datenschutzpflichten der Leitung von kirchlichen Einrichtungen ohne bDSB

Mit dem 2. Datenschutz-Anpassungs- und Umsetzungsgesetz EU wurde 2019 im Bundesdatenschutzgesetz unter anderem § 38 Abs. 1 Satz 1 BDSG geändert. Damit ist die Benennung eines betrieblichen Datenschutzbeauftragten im Geltungsbereich des BDSG erst dann erforderlich, wenn eine verantwortliche Stelle im Sinne dieser Regelung in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Mit der Erhöhung der Grenze von 10 auf 20 Personen wollte der deutsche Gesetzgeber kleinere und mittlere Unternehmen sowie ehrenamtlich tätige Vereine entlasten.

Diese Gesetzesänderung wird voraussichtlich bei der Novellierung des kirchlichen Datenschutzgesetzes in das kirchliche Gesetz übernommen werden.

Auch wenn mit dieser Gesetzesänderung die Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten für einige kirchliche Einrichtungen entfallen wird, bleiben die datenschutzrechtlichen Verpflichtungen gleich, die die Einrichtungen zu erfüllen haben. Die Leitungen

[72] Vgl. Schulten in: Sydow, Kirchliches Datenschutzrecht, § 36 Rn. 22 f.

der Einrichtungen sind für die Einhaltung der datenschutzrechtlichen Verpflichtungen verantwortlich – unabhängig davon, ob ein betrieblicher Datenschutzbeauftragter zu benennen ist oder nicht. Die Leitungen der Einrichtungen ohne einen bDSB müssen daher auf andere Weise das notwendige Fachwissen für sich nutzbar machen, damit sie als Leitung der Einrichtung neben den anderen gesetzlichen Pflichten auch die datenschutzrechtlichen Vorgaben erfüllen können.

„Die Leitungen der Einrichtungen sind für die Einhaltung der datenschutzrechtlichen Verpflichtungen verantwortlich – unabhängig davon, ob ein betrieblicher Datenschutzbeauftragter zu benennen ist oder nicht.“

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

Die katholische Kirche in Deutschland hat die Möglichkeiten des Art. 91 DSGVO für sich in Anspruch genommen und ihr bis dahin schon vorhandenes eigenes Datenschutzrecht an die DSGVO angepasst. Zur Überwachung der Einhaltung dieses kirchlichen Datenschutzrechts kann die Kirche nach Art. 91 Abs. 2 DSGVO auch eine eigene kirchlichen Datenschutzaufsicht vorsehen.

Die fünf nordrhein-westfälischen (Erz-)Diözesen haben diese Möglichkeit mit der Benennung eines gemeinsamen Diözesandatenschutzbeauftragten und der Einrichtung des Katholischen Datenschutzzentrums wahrgenommen.

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). Die Gebiete dieser fünf (Erz-)Diözesen umfassen in etwa das Gebiet des Landes Nordrhein-Westfalen.[73] Im Zuständigkeitsgebiet leben 6 Millionen Menschen römisch-katholischen Glaubens (Stand 2023).

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands[74] (den Rechtsträger der Deutschen Bischofskonferenz) zuständig. 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 beschrieben.[75]

Der Diözesandatenschutzbeauftragte, sein Stellvertreter und die Mit-

[73] Einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zur Erzdiözese Köln gehören, und von Niedersachsen und Hessen, die Teil der Erzdiözese Paderborn sind, gehören ebenfalls zum Zuständigkeitsgebiet des Katholischen Datenschutzzentrums.

[74] Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter".

[75] Für eine ausführliche Darstellung der Aufgaben der Datenschutzaufsicht siehe Abschnitt 3.5 des Jahresberichts 2021.

arbeiterinnen und Mitarbeiter bringen ihre Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von kirchlichen Gremien, Arbeitsgruppen und der kirchlichen Einrichtungen ein. Die Beratung der Gremien, Arbeitsgruppen und kirchlichen Einrichtungen 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 seinem Zuständigkeitsbereich.

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.[76] 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 soll sichergestellt werden, dass die Datenschutzaufsicht die gesetzlich vorgesehene Kontrollfunktion auch unbeeinflusst wahrnehmen kann.[77]

Abb. 6: Das Katholische Datenschutzzentrum hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn. (Bild: Sozialinstitut Kommende Dortmund)

[76] 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.

[77] 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.

Dem Diözesandatenschutzbeauftragten sind ein Vertreter, Referenten und Sachbearbeiter zur Seite gestellt. Es sind im Berichtszeitraum elf Stellen vorgesehen, die zum Jahresende nicht alle besetzt sind.

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 2024 sieht der Haushaltsplan für das Katholische Datenschutzzentrum ein Volumen in Höhe von 1.264.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben vor. Für das Folgejahr 2025 sinkt das genehmigte Budget leicht auf 1.239.000 Euro.

3.3 Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums

Mit der Gründung wurde dem Katholischen Datenschutzzentrum auch ein Schutzpatron von den (Erz-)Diözesen mitgegeben – der hl. Ivo.

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. Sein Gedenktag ist der 19. Mai.[78]

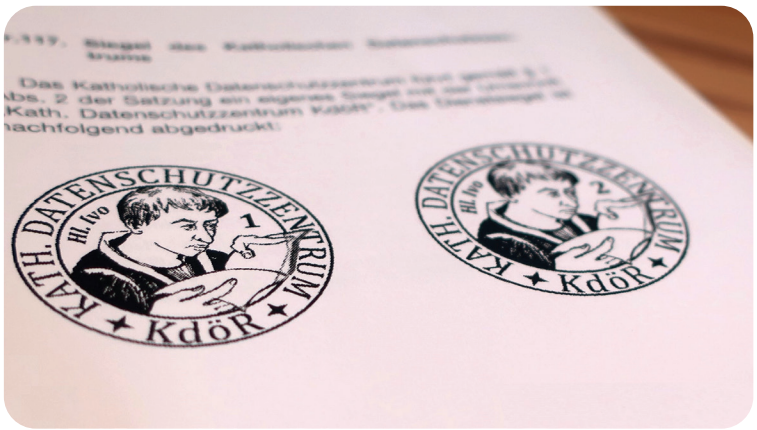


Abb. 7: Darstellung des Siegels des KDSZ im Amtsblatt der Erzdiözese Paderborn (Bild: Katholisches Datenschutzzentrum)

[78] 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.

3.4 Öffentlichkeitsarbeit

Das Katholische Datenschutzzentrum macht 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 dazu. Dies geschieht z. B. durch Veröffentlichungen auf der Homepage des KDSZ oder die Teilnahme an themenbezogenen Veranstaltungen und Fortbildungen im Datenschutz und in der Informationstechnik.

Im Jahr 2024 war das KDSZ u. a. als Referent auf der Veranstaltung „faith + funds“ in Hannover anzutreffen. Bei dem Fachtag für Fundraising für Kirche, Caritas, Diakonie und Orden war die Beachtung des Datenschutzes beim Fundraising kirchlicher Einrichtungen mit einem Vortrag aus dem Haus des Beauftragten für den Datenschutz der EKD und dem Vortrag des KDSZ ein inhaltlicher Block der Veranstaltung.

Bei der Amtseinführung der (neuen) Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Frau Prof. Dr. Louisa Specht-Riemenschneider, zu der auch der Diözesandatenschutzbeauftragte eingeladen worden war, wurde in verschiedenen Gesprächen der Austausch mit den staatlichen Datenschutzaufsichten weiter intensiviert.

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. Von einschlägigen Gesetzestexten für die jeweilige (Erz-)Diözese bis hin zu Mustern und Vorlagen – eine Bandbreite an Hilfestellungen ist hier zu finden. Auch werden laufend Beiträge zu aktuellen Themen im Datenschutzbereich veröffentlicht und auch der jährliche erscheinende Tätigkeitsbericht des KDSZ ist eine wichtige Informationsquelle.

Das Katholische Datenschutzzentrum ist mit einem eigenen „besonderen elektronischen Behördenpostfach (beBPo)“ an den elektronischen Rechtsverkehr angebunden. Das Besondere Behördenpostfach ist ein elektronisches Kommunikationsmittel für Behörden und Verwaltungen in Deutschland und ermöglicht einen sicheren, vertraulichen und nachweisbaren digitalen Austausch von Dokumenten und Nachrichten.

3.5 Antragsverfahren vor dem Interdiözesanen Datenschutzgericht

Im Berichtszeitraum sind zwei erstinstanzliche Verfahren aus 2024 beim Interdiözesanen Datenschutzgericht (IDSG) und ein zweitinstanzliches Verfahren vor dem Datenschutzgericht der Deutschen Bischofskonferenz (DSG-DBK), bei denen das Katholische Datenschutzzentrum als Antragsgegner oder Beteiligter geführt wird, anhängig. In einem Verfahren der 1. Instanz wurde der Antrag für erledigt erklärt und konnte im Berichtsjahr abgeschlossen werden. Die anderen Verfahren laufen noch. In den teilweise noch anhängigen Verfahren aus den Jahren 2022 und 2023 stehen die Entscheidungen des IDSG noch aus.

Die Verfahren im Berichtsjahr betreffen inhaltlich fast ausschließlich Beschwerdeverfahren, die durch das Katholische Datenschutzzentrum gem. § 48 KDG bearbeitet wurden. Vorausgegangen waren hier datenschutzrechtliche Eingaben durch Betroffene und die Einlegung eines gerichtlichen Rechtsbehelfs gegen den Bescheid.

Hinweis für kirchliche Einrichtungen

Die Entscheidungen der 1. und 2. Instanz werden regelmäßig auf der Internetseite der Deutschen Bischofskonferenz veröffentlicht.[79] Die Verfahren vor den kirchlichen Gerichten in Datenschutzangelegenheiten richten sich nach der Kirchlichen Datenschutzgerichtsordnung (KDSGO)[80].

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

Das Katholische Datenschutzzentrum tauscht sich mit den anderen Datenschutzaufsichtsbehörden der Kirchen, des Rundfunks und des Bundes und der Länder aus, um datenschutzrechtliche Fragen möglichst einheitlich auszulegen und gemeinsame Standpunkte zu entwickeln.

Allgemein
Die Intensivierung der Zusammenarbeit der katholischen und evangelischen Datenschutzaufsichten mit der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder wurde auch in diesem Berichtszeitraum fortgesetzt.

Zum grundsätzlichen Austausch findet zweimal im Jahr der „Austausch zwischen Mitgliedern der DSK und spezifischen Datenschutzaufsichtsbehörden“ in Präsenz oder als Videokonferenz statt.[81] Hier nimmt als Vertreter der Konferenz der Diözesandatenschutzbeauftragten der Diözesandatenschutzbeauftragte der bayerischen (Erz-)Diözesen an den Treffen teil.

Auch unabhängig von diesen regelmäßigen Terminen findet ein reger Austausch untereinander statt. Der Diözesandatenschutzbeauftragte hält die regelmäßigen Kontakte zu den andern Datenschutzaufsichten auf allen Ebenen für sehr wichtig und will dies weiter intensivieren.

[79] https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen und https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/entscheidungen
[80] Siehe hierzu Abschnitt 1.3.2 im Jahresbericht 2018 und Abschnitt 2.5.1 im Jahresbericht 2019.
[81] Protokolle stehen auf der Internetseite der DSK zur Verfügung: https://www.datenschutzkonferenz-online.de/protokolle.html

Arbeitskreise der DSK

Die unabhängigen Datenschutzbehörden des Bundes und der Länder beraten sich in der Datenschutzkonferenz[82]. Eine ihrer Aufgaben ist es, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts, z. B. durch Entschließungen und Beschlüsse, zu erreichen. Unterstützung erhält die Datenschutzkonferenz dabei durch fachbezogene Arbeitskreise[83], die deren Entscheidungen maßgeblich vorbereiten.

Die fünf katholischen Datenschutzaufsichten arbeiten in verschiedenen dieser Arbeitskreise mit und haben sich die Teilnahme an den Arbeitskreisen aufgeteilt. So vertritt das Katholische Datenschutzzentrum die katholischen Datenschutzaufsichten im AK Grundsatz der DSK.

Austausch der IT-Labore der Datenschutzaufsichtsbehörden

Im Frühjahr 2024 hat der damalige Bundesbeauftragte für Datenschutz und Informationsfreiheit in Zusammenarbeit mit dem Landesbeauftragten für Datenschutz (LfD) aus Niedersachsen, der Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI) Nordrhein-Westfalen und dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) zu einem Informationsaustausch der IT-Labore aller Datenschutzaufsichten in Deutschland eingeladen. Neben den staatlichen Datenschutzaufsichten waren auch alle spezifischen Aufsichtsbehörden zu diesem Treffen eingeladen. Das Treffen fand in den Räumen des BfDI in Bonn statt. Schwerpunkt des Austausches war die App-Prüfung an konkreten Beispielen mit verschiedenen Herangehensweisen. Neben der Prüfung von z. B. Datenschutzhinweisen wurden auch die Prüfungen von Cookies, App-Berechtigungen und des Netzwerkverkehrs thematisiert. Ein weiterer Informationsaustausch fand im Herbst 2024 in den Räumen der BfDI in Berlin statt. Vorgehen bei technischen Prüfungen sowie verwendete Tools und Abläufe standen beim zweiten Treffen im Vordergrund. Das Katholische Datenschutzzentrum hat mit seinem IT-Labor[84] an beiden Treffen teilgenommen. Inhalte zur Durchführung von Prüfungen wurden zum Informationsaustausch beigesteuert und neue Impulse für laufende und zukünftige Prüfungen konnten mitgenommen werden.

Der Informationsaustausch der IT-Labore wird im Jahr 2025 fortgesetzt.

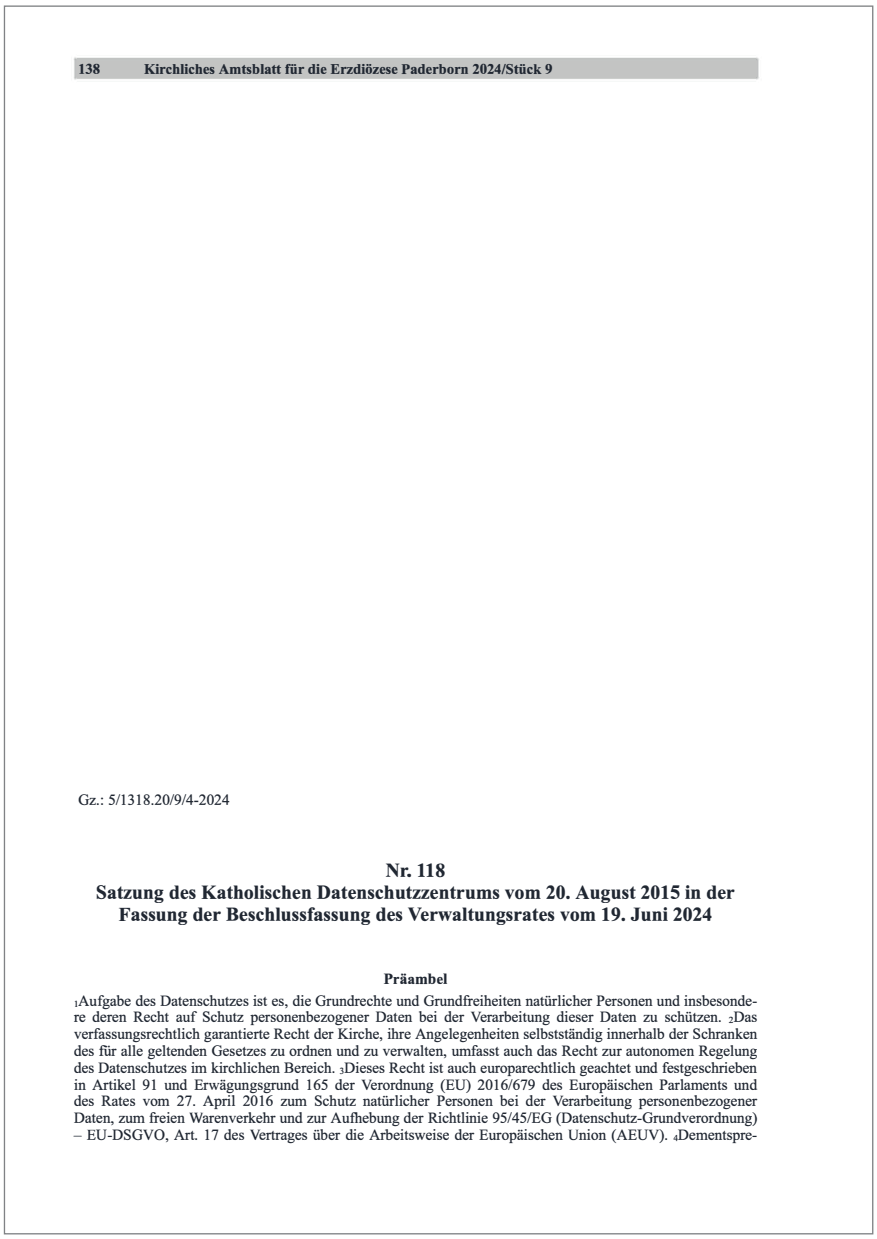
3.7 Überarbeitung der Satzung des Katholischen Datenschutzzentrums

Das Katholische Datenschutzzentrum wurde als Rechtsträger der gemeinsamen Datenschutzstelle zur Gewährleistung eines dem staatlichen Bereich vergleichbaren Datenschutzstandards mit Urkunde vom 20.08.2015 von den nordrhein-westfälischen Erzdiözesen und Diözesen als Körperschaft des öffentlichen Rechts errichtet. Auch die Satzung des KDSZ ist Gegenstand dieser Urkunde und bildet seit diesem Zeitpunkt die Grundlage für die eigenständige und unabhängige Arbeit der Datenschutzstelle als Körperschaft des öffentlichen Rechts.

[82] https://www.datenschutzkonferenz-online.de/dsk.html
[83] https://www.datenschutzkonferenz-online.de/ak.html
[84] In den IT-Laboren der Datenschutzaufsichten werden technische Sachverhalte nachgestellt und überprüft.

Nach nun fast zehnjährigem Bestehen der Satzung des Katholischen Datenschutzzentrums wurde diese vom Verwaltungsrat mit Beschluss vom 19.06.2024 behutsam angepasst. Änderungsbedarf ergab sich vor allem dadurch, dass in der bisherigen Satzung noch auf die Vorgängerregelung des aktuell geltenden Gesetzes über den Kirchlichen Datenschutz verwiesen wurde. Außerdem wurde bei den Änderungen auf gendergerechtere Formulierungen geachtet und es wurden kleinere Anpassungen an die praktischen Erfahrungen der letzten Jahre vorgenommen.

Inzwischen haben alle Mitgliedsdiözesen die Satzung in der Fassung der Beschlussfassung des Verwaltungsrates vom 19.06.2024 in ihren Amtsblättern veröffentlicht.[85]



138 Kirchliches Amtsblatt für die Erzdiözese Paderborn 2024/Stück 9

Gz.: 5/1318.20/9/4-2024

Nr. 118
Satzung des Katholischen Datenschutzzentrums vom 20. August 2015 in der Fassung der Beschlussfassung des Verwaltungsrates vom 19. Juni 2024

Präambel

[1]Aufgabe des Datenschutzes ist es, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten bei der Verarbeitung dieser Daten zu schützen. [2]Das verfassungsrechtlich garantierte Recht der Kirche, ihre Angelegenheiten selbstständig innerhalb der Schranken des für alle geltenden Gesetzes zu ordnen und zu verwalten, umfasst auch das Recht zur autonomen Regelung des Datenschutzes im kirchlichen Bereich. [3]Dieses Recht ist auch europarechtlich geachtet und festgeschrieben in Artikel 91 und Erwägungsgrund 165 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Warenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenschutz-Grundverordnung) – EU-DSGVO, Art. 17 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV). [4]Dementspre-

[85] Der Text der Satzung in der Fassung vom 19.06.2024 ist am Beispiel des Erzbistums Paderborn (KABl. Stück 9 Nr. 118) im Jahresbericht abgedruckt. Weitere Veröffentlichungen: Bistum Aachen ABl. Stück 10 Nr. 101; Bistum Essen KABl. Stück 9 Nr. 63; Erzbistum Köln ABl. Stück 10 Nr. 132 und Bistum Münster KABl. Stück 10 Nr. 137. Siehe hierzu auch den Beitrag auf der Homepage des KDSZ mit Verlinkungen zu den Amtsblättern (https://www.katholisches-datenschutzzentrum.de/ueberarbeitung-der-satzung-des-katholischen-datenschutzzentrums/).

chend haben die Diözesanbischöfe von Aachen, Essen, Köln, Münster und Paderborn für ihren Zuständigkeitsbereich in Einklang mit den Bestimmungen der EU-DSGVO umfassende datenschutzrechtliche Regelungen getroffen und sich darauf verständigt, die Datenschutzaufsicht in einer überdiözesanen Datenschutzstelle (Katholisches Datenschutzzentrum) zu organisieren.

§ 1
Rechtsform, Name, Sitz, Grundordnung, Datenschutzrecht

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

(2) Es führt den Namen „Katholisches Datenschutzzentrum“ (KDSZ) und ein eigenes Siegel mit der Umschrift „Kath. Datenschutzzentrum KdöR“.

(3) Sitz des Katholischen Datenschutzzentrums ist Dortmund.

(4) [1]Für das katholische Datenschutzzentrum gilt das kirchliche Recht, insbesondere

a) die Grundordnung des kirchlichen Dienstes;

b) das Gesetz über den kirchlichen Datenschutz (KDG) und die zu seiner Durchführung ergangenen Regelungen;

c) die diözesanen Bestimmungen zur Prävention von sexualisierter Gewalt;

d) die diözesane Ordnung über den Umgang mit sexuellem Missbrauch Minderjähriger und schutz- oder hilfebedürftiger Erwachsener durch Kleriker und sonstige Beschäftigte im kirchlichen Dienst,

in ihren jeweils gültigen, vom Diözesanbischof der für den Sitz des Datenschutzzentrums zuständigen (Erz-)Diözese in Kraft gesetzten Fassungen. [2]Satz 1 bezieht sich auch auf etwaige Nachfolgeregelungen.

§ 2
Mitgliedschaft

(1) Mitglieder der Körperschaft sind im Zeitpunkt ihrer Errichtung

- die Diözese Aachen (KdöR),
- die Diözese Essen (KdöR),
- die Erzdiözese Köln (KdöR),
- die Diözese Münster (KdöR) und
- die Erzdiözese Paderborn (KdöR).

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

(3) Mitglieder können unter den in dieser Satzung festgelegten Voraussetzungen aus der Körperschaft ausscheiden.

§ 3
Zweckbestimmung

(1) [1]Der Zweck des Katholischen Datenschutzzentrums ist die Wahrnehmung der kirchlichen Datenschutzaufsicht auf der Grundlage der für die Mitgliedsdiözesen geltenden kirchlichen Datenschutzregelungen, insbesondere des Gesetzes über den kirchlichen Datenschutz (KDG), in der für die Mitgliedsdiözesen jeweils geltenden Fassung. [2]Mit der Wahrnehmung der kirchlichen Datenschutzaufsicht wird insbesondere sichergestellt, dass bei den Verantwortlichen im Sinne des KDG ausreichende Maßnahmen zum Datenschutz getroffen sind.

(2) [1]Die Datenschutzaufsicht erstreckt sich auf die Bereiche der Mitgliedsdiözesen, im Bereich der Diözese Münster beschränkt auf deren nordrhein-westfälischen Teil. [2]Sie kann beim Beitritt weiterer Mitgliedsdiözesen gemäß § 2 Abs. 2 oder einer Entscheidung gemäß § 7 Abs. 1 Buchstabe h) entsprechend erweitert werden.

(3) Das Katholische Datenschutzzentrum ist

a. Rechtsträger der überdiözesanen Datenschutzstelle der Mitgliedsdiözesen sowie

b. Anstellungsträger sowohl des oder der von den Diözesanbischöfen der Mitgliedsdiözesen nach den Vorgaben des KDG bestellten Diözesandatenschutzbeauftragten als auch der von diesem oder dieser ausgewählten Mitarbeitenden der überdiözesanen Datenschutzstelle.

§ 4
Organe

Organe des Katholischen Datenschutzzentrums sind

- der Diözesandatenschutzbeauftragte und
- der Verwaltungsrat.

§ 5
Diözesandatenschutzbeauftragter oder Diözesandatenschutzbeauftragte, Rechtsstellung, Aufgaben, Geschäftsstelle

(1) [1]Gesetzlicher Vertreter des Katholischen Datenschutzzentrums ist der oder die von den Diözesanbischöfen der Mitgliedsdiözesen gemäß den Vorgaben des KDG bestellte Diözesandatenschutzbeauftragte. [2]Er oder sie ist für die angeschlossenen Mitgliedsdiözesen und ggf. weiteren kirchlichen Rechtsträger, die dem Datenschutzzentrum nicht als Mitglied angehören, der oder die Diözesandatenschutzbeauftragte gemäß den jeweils geltenden Bestimmungen des KDG. [3]Der oder die Diözesandatenschutzbeauftragte vertritt das Katholische Datenschutzzentrum gerichtlich und außergerichtlich und führt dessen Geschäfte. [4]Vertreter oder Vertreterin ist der jeweilige Stellvertreter oder die jeweilige Stellvertreterin des oder der Diözesandatenschutzbeauftragten. [5]Diözesandatenschutzbeauftragter oder Diözesandatenschutzbeauftragte und Stellvertreter oder Stellvertreterin sind jeweils einzeln zur Vertretung berechtigt. [6]Entsprechende Erklärungen sind unter Beidrückung des Siegels des Katholischen Datenschutzzentrums abzugeben.

(2) Die Rechtsstellung, der Rahmen für die Dauer der Bestellung und die Aufgaben des oder der Diözesandatenschutzbeauftragten ergeben sich aus dem Gesetz über den kirchlichen Datenschutz (KDG) in der für den Sitz des Katholischen Datenschutzzentrums jeweils geltenden Fassung.

(3) [1]Zur Erledigung seiner oder ihrer Aufgaben steht dem oder der Diözesandatenschutzbeauftragten eine Geschäftsstelle (Datenschutzstelle) mit der erforderlichen Personal- und Sachausstattung zur Seite. [2]Der Umfang der Ausstattung ist nach Maßgabe des KDG festzulegen und im Haushalts- oder Wirtschaftsplan der Datenschutzstelle zu veröffentlichen.

§ 6
Zusammensetzung des Verwaltungsrates, Vertretung

(1) [1]Die Diözesanbischöfe von Aachen, Essen, Köln, Münster und Paderborn bilden den Verwaltungsrat des Katholischen Datenschutzzentrums. [2]Im Falle der Behinderung oder Sedisvakanz (cc. 412 ff., 416 ff. CIC) werden die den Diözesanbischöfen nach dieser Satzung zukommenden Aufgaben von derjenigen Person wahrgenommen, der gemäß den kirchenrechtlichen Bestimmungen die Leitung der jeweiligen (Erz-)Diözese obliegt.

(2) Die Mitglieder des Verwaltungsrates können für den Einzelfall oder dauerhaft eine von ihnen bevollmächtigte Person als Vertretung in den Verwaltungsrat entsenden.

(3) Wird das Katholische Datenschutzzentrum um weitere Mitgliedsdiözesen erweitert oder scheiden Mitgliedsdiözesen aus, ändert sich die Zusammensetzung des Verwaltungsrates entsprechend.

(4) [1]Der Verwaltungsrat wählt für eine Amtszeit von jeweils fünf Jahren aus seiner Mitte einen Vorsitzenden und einen stellvertretenden Vorsitzenden, im dauerhaften Vertretungsfall nach Abs. 2 einen oder ggf. eine Vorsitzende und einen oder ggf. eine stellvertretende Vorsitzende. [2]Wiederwahl ist zulässig.

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

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

§ 7
Aufgaben des Verwaltungsrates

(1) [1]Unter Wahrung der den Diözesanbischöfen kirchenrechtlich vorbehaltenen Zuständigkeiten und unter Wahrung der im KDG festgelegten organisatorischen und sachlichen Unabhängigkeit des oder der Diözesandatenschutzbeauftragten kommen dem Verwaltungsrat insbesondere die nachfolgend genannten Aufgaben zu:

a) Entscheidung über die dem oder der Diözesandatenschutzbeauftragten zukommende Personal- und Sachausstattung nach Maßgabe der durch die Mitgliedsdiözesen zur Verfügung gestellten Mittel; die Festsetzung erfolgt durch Umlagebeschluss;

b) Entgegennahme des gemäß den Vorgaben des KDG regelmäßig zu erstattenden Tätigkeitsberichtes des oder der Diözesandatenschutzbeauftragten;

c) Erlass einer Geschäftsordnung für den Verwaltungsrat;

d) Entscheidungsvorschlag an den jeweiligen Diözesanbischof zur Bestellung des oder der Diözesandatenschutzbeauftragten;

e) Entscheidungsvorschlag an den jeweiligen Diözesanbischof zum Widerruf der Bestellung zum oder zur Diözesandatenschutzbeauftragten;

f) Entgegennahme der Information über die Einstellung neuer Mitarbeitenden der Datenschutzstelle;

g) Entscheidung über den Beitritt weiterer Mitgliedsdiözesen;

h) Entscheidung über die Übernahme der Datenschutzaufsicht über sonstige, nicht über die Mitgliedschaft der (Erz-)Diözesen erfasste kirchliche Rechtsträger;

i) Entscheidung über Satzungsänderungen des Katholischen Datenschutzzentrums;

j) Entscheidung über die Auflösung des Katholischen Datenschutzzentrums.

[2]Beschlüsse zu Buchstaben d) und e) sowie g) bis j) müssen mit den Stimmen aller Verwaltungsratsmitglieder einstimmig erfolgen.

(2) [1]Der oder ggf. die Vorsitzende des Verwaltungsrates ist Dienstvorgesetzter des oder der Diözesandatenschutzbeauftragten. [2]Die Dienstaufsicht ist gemäß den Vorgaben des KDG so zu regeln, dass dadurch die Unabhängigkeit des oder der Diözesandatenschutzbeauftragten nicht beeinträchtigt wird. [3]Entsprechendes gilt für den Stellvertreter oder die Stellvertreterin in Ausübung der Vertretung.

§ 8
Arbeitsweise des Verwaltungsrates

(1) [1]Die Sitzungen des Verwaltungsrates können in Präsenz oder virtuell durchgeführt werden; über das Format befindet der Vorsitzende. [2]Der Verwaltungsrat ist beschlussfähig, wenn wenigstens die Hälfte seiner Mitglieder, darunter der oder ggf. die Vorsitzende oder der oder ggf. die stellvertretende Vorsitzende, teilnehmen.

(2) [1]Sitzungen des Verwaltungsrates finden mindestens einmal jährlich, darüber hinaus nach Bedarf, statt. [2]Zu diesen Sitzungen ist textlich (Brief, Telefax, E-Mail) mit einer Frist von mindestens vier Wochen unter Angabe der Beratungspunkte einzuladen. [3]Der Verwaltungsrat ist von dem oder ggf. der Vorsitzenden einzuberufen, wenn es mindestens zwei Mitglieder unter Angabe der Beratungspunkte schriftlich verlangen.

(3) [1]Soweit in dieser Satzung nicht ausdrücklich etwas anderes bestimmt ist, entscheidet der Verwaltungsrat mit der Mehrheit der Stimmen der teilnehmenden Mitglieder. [2]Der Verwaltungsrat kann Beschlüsse im Einzelfall auch textlich im Umlauf- oder Sternverfahren fassen, wenn alle Verwaltungsratsmitglieder bzw. Vertreter dieser Form der Beschlussfassung zustimmen.

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

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

§ 9
Beitritt weiterer Mitgliedsdiözesen

[1]Weitere (Erz-)Diözesen (Körperschaften des öffentlichen Rechts) können der Körperschaft als Mitglieder beitreten, wenn der Verwaltungsrat dem Beitrittsgesuch mit den Stimmen aller seiner Mitglieder zustimmt. [2]Die näheren Einzelheiten sind in einer Beitrittsvereinbarung zu regeln.

§ 10
Austritt von Mitgliedsdiözesen

[1]Mitgliedsdiözesen können mit einer Frist von einem Jahr zum Jahresende ihren Austritt aus der Körperschaft erklären. [2]Die näheren Einzelheiten sind in einer Austrittsvereinbarung mit den verbleibenden Mitgliedsdiözesen zu regeln.

§ 11
Auflösung der Körperschaft

[1]Über eine Auflösung der Körperschaft entscheidet der Verwaltungsrat nach Anhörung des oder der Diözesandatenschutzbeauftragten. [2]Die Auflösung kann nur mit den Stimmen aller Mitglieder des Verwaltungsrates beschlossen werden.

§ 12
Vermögensanfall

Bei Auflösung der Körperschaft fällt das vorhandene Vermögen zu gleichen Teilen an die Mitglieder der Körperschaft, die es ausschließlich zu steuerbegünstigten Zwecken im Sinne des Abschnitts „Steuerbegünstigte Zwecke" der AO in ihrer jeweils geltenden Fassung zu verwenden haben.

§ 13
Inkrafttreten

Diese Satzung tritt mit Unterzeichnung der Errichtungsurkunde durch die Diözesanbischöfe von Aachen, Essen, Köln, Münster und Paderborn in Kraft.

Köln, den 17. Juli 2024

L.S.

+ Rainer Maria Kardinal Woelki
Erzbischof von Köln

Paderborn, den 27. Juni 2024

L.S.

+ Dr. Udo Markus Bentz
Erzbischof von Paderborn

Aachen, den 10. August 2024

L.S.

+ Dr. Helmut Dieser
Bischof von Aachen

Essen, den 08. Juli 2024

L.S.

+ Dr. Franz-Josef Overbeck
Bischof von Essen

Münster, den 03. Juli 2024

L.S.

+ Dr. Felix Genn
Bischof von Münster

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. 8: 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[86].

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.[87]

Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der Diözesandatenschutzbeauftragten aus. Zu den Konferenzen werden auch die Ordensdatenschutzbeauftragten der DOK ein-

[86] Siehe Abschnitt 3.1 des Jahresberichts.
[87] Siehe https://datenschutz.orden.de/.

geladen.[88] Zur leichteren Erreichbarkeit und besseren Koordination ihrer Zusammenarbeit hat die Konferenz eine „Geschäftsstelle“ eingerichtet, die sich beim Katholischen Datenschutzzentrum in Dortmund befindet.

4.2 Veröffentlichungen der Konferenz der Diözesandatenschutzbeauftragten

Im Berichtsjahr veröffentlichte die Konferenz eine Gemeinsame Stellungnahme[89] zu den Unabhängigen Aufarbeitungskommissionen hinsichtlich der Anwendbarkeit des kirchlichen Datenschutzrechts, der datenschutzrechtlichen Verantwortlichkeit und der Gewährleistung der Datensicherheit.

Gemäß der „Gemeinsamen Erklärung“ der Deutschen Bischofskonferenz und der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) soll in allen (Erz-)Diözesen eine unabhängige Aufarbeitung des sexuellen Missbrauchs erfolgen. Hierfür wurden in den (Erz-)Diözesen Unabhängige Aufarbeitungskommissionen (UAK) eingerichtet, die nun im Rahmen ihrer Aufgaben eine Vielzahl von personenbezogenen Daten verarbeiten.[90] Die Stellungnahme der Konferenz adressiert einige der datenschutzrechtlichen Fragestellungen, die zur Arbeit der UAK an die Aufsichten herangetragen wurden.

[88] Ausführlich zur Konferenz der Diözesandatenschutzbeauftragten siehe Abschnitt 4.1.3 im Jahresbericht 2021.
[89] https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2024/11/Stellungnahme-UAK.pdf
[90] Siehe auch Abschnitt 1.3.2 des Jahresberichts 2023.

Gemeinsame Stellungnahme der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

zu den Unabhängigen Aufarbeitungskommissionen:

Anwendbarkeit des Kirchlichen Datenschutzrechts, datenschutzrechtliche Verantwortlichkeit und Gewährleistung der Datensicherheit

vom 12.11.2024

Bei den Diözesandatenschutzbeauftragten sind in den vergangenen Monaten immer wieder Fragen zur datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung personenbezogener Daten durch die in den (Erz-)Diözesen eingerichteten Unabhängigen Aufarbeitungskommissionen (UAK) angekommen. Die Konferenz der Diözesandatenschutzbeauftragten nimmt zur Klarstellung ihres Standpunktes in diesen Fragen gemeinsam wie folgt Stellung:

I. Anwendbarkeit des Kirchlichen Datenschutzrechts

Die Aufarbeitung des sexuellen Missbrauchs ist gemäß der „Gemeinsamen Erklärung über verbindliche Kriterien und Standards für eine unabhängige Aufarbeitung von sexuellem Missbrauch in der katholischen Kirche in Deutschland“[1] genuine Aufgabe des jeweiligen Ortsordinarius. Es handelt sich um eine primär kirchliche Aufgabe, die den errichteten Aufarbeitungskommissionen zugewiesen ist.

Für die Tätigkeit der Unabhängigen Aufarbeitungskommissionen findet daher kirchliches Datenschutzrecht Anwendung.

II. Datenschutzrechtliche Verantwortlichkeit

Die Unabhängigen Aufarbeitungskommissionen sind datenschutzrechtlich Verantwortliche. Nach § 4 Nr. 9 KDG ist „Verantwortlicher“ die natürliche oder juristische Person, Behörde,

[1] https://www.dbk.de/fileadmin/redaktion/diverse_downloads/presse_2020/2020-074a-Gemeinsame-Erklaerung-UBSKM-Dt.-Bischofskonferenz.pdf

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

Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Bestimmung der datenschutzrechtlichen Verantwortlichkeit hat in der Regel anhand einer funktionalen Analyse der tatsächlichen Gegebenheiten zu erfolgen. Die „Entscheidung" beschreibt eine bewusst oder unbewusst ausgewählte Entscheidungsgewalt.[2] Nach den „Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO"[3] ist der Verantwortliche anhand folgender Kriterien zu bestimmen.

> *„Bei einer bestimmten Verarbeitung ist der Verantwortliche der Akteur, der entschieden hat, warum die Verarbeitung erfolgt (also „mit welchem Ziel" oder „wozu"), und auf welche Weise dieses Ziel erreicht werden soll (also welche Mittel eingesetzt werden, um das Ziel zu erreichen).*"[4]

a) Mittel der Verarbeitung

Hinsichtlich der Mittel der Verarbeitung (im Rahmen einer Verarbeitungstätigkeit) ist zu berücksichtigen, dass es hierbei im Kern nicht um die Bereitstellung finanzieller Mittel oder Sachmittel geht. Vielmehr geht es bei den Mitteln der Verarbeitung darum zu fragen, wie die Datenverarbeitung erfolgt, um das angestrebte Ziel zu erreichen. Gemeint sind beispielsweise Entscheidungsbefugnisse darüber, welche Daten verarbeitet werden, über die konkrete Art und Weise der Verarbeitung sowie die Auswahl der technischen und organisatorischen Maßnahmen.[5]

Nach Ziffer 2.1. der „Gemeinsamen Erklärung über verbindliche Kriterien und Standards für eine unabhängige Aufarbeitung von sexuellem Missbrauch in der katholischen Kirche in Deutschland"[1] richtet jede (Erz-)Diözese eine Kommission (UAK) ein und stellt ihr zur Erfüllung der Aufgaben die erforderlichen Mittel zur Verfügung. Die (Erz-)Diözesen haben hierdurch die Verpflichtung übernommen, die Kommissionen mit den erforderlichen (Sach- und Finanz-) Mitteln auszustatten, um die unabhängige Aufarbeitung durch die jeweiligen Kommissionen zu ermöglichen. Vorgaben in Bezug auf die Mittel der Verarbeitung i. S. d. § 4 Nr. 9 KDG, also in Bezug auf das „Wie" der Verarbeitung, enthält die Gemeinsame Erklärung nicht, sodass die

[2] Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 7 Rn. 13.
[3] https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf
[4] Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, Seite 16.
[5] Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 181, beck-online.

ausschließliche Entscheidungsbefugnis über das „Wie“ der Verarbeitung bei den jeweiligen Kommissionen liegt.

b) Zweck der Verarbeitung

Wesentlich für die Festlegung der datenschutzrechtlichen Verantwortlichkeit ist der Umfang der Entscheidungsbefugnis über den Zweck, d. h. über das Ob, Wofür und Wieweit einer Datenverarbeitung.[6] Nach den Leitlinien 07/2020 (Rn. 24) wird in der Regel eine Rechtsvorschrift „jemandem die Aufgabe zuweisen oder die Verpflichtung auferlegen, bestimmte Daten zu erheben und zu verarbeiten. In diesen Fällen ist der Zweck der Verarbeitung häufig im Gesetz bestimmt. Verantwortlicher ist normalerweise derjenige, der nach dem Gesetz diesen Zweck zu erreichen, diese öffentliche Aufgabe wahrzunehmen hat.“

Bei der Alternative, bei der sich die Verantwortlichkeit aus einer Rechtsvorschrift ergeben kann, bezieht sich der EDSA auf die Regelung des Art. 4 Nr. 7 Halbsatz 2 DSGVO („…; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;“).

Dies ist eine Regelung, die der kirchliche Gesetzgeber nicht in das KDG übernommen hat. Zumindest in Bezug auf Vorgaben von Zwecken und Mitteln bzw. der Benennung von Kriterien für die Bestimmung von Verantwortlichen in den kirchlichen Gesetzen sind keine Gründe ersichtlich, die einer Übertragung und Anwendung des Regelungsgedankens dieser Regelung der DSGVO auch im kirchlichen Bereich entgegenstehen würden. Daher ziehen wir den Regelungsgedanken bei unserer Auslegung der Definition des Verantwortlichen mit heran.

Nach Ziffer 1.1 der Gemeinsamen Erklärung ist die Aufarbeitung des sexuellen Missbrauchs genuine Aufgabe des jeweiligen Ortsordinarius. Diese Aufgabe ist nach Ziffer 2.1 der Gemeinsamen Erklärung den einzurichtenden Kommissionen zur Erfüllung zugewiesen.

Die Regelungen aus der Gemeinsamen Erklärung sind durch die jeweiligen Bistümer in Form von Ordnungen und Statuten erlassen und in Kraft gesetzt worden. Durch die Berufung einer externen Kommission ist die unabhängige Aufarbeitung gewährleistet. Auch die Musterord-

[6] Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 7 Rn. 13, beck-online.

nung[7], welche in einer Vielzahl von Bistümern erlassen worden ist, enthält keine Einschränkungen in Bezug auf das „Ob“ und „Wofür“ der Verarbeitung von personenbezogenen Daten. Die Entscheidungsbefugnis in Bezug auf die Erfüllung der Aufgabe liegt damit ausschließlich bei den jeweiligen Unabhängigen Aufarbeitungskommissionen, sodass diese als datenschutzrechtlich Verantwortliche i. S. d. § 4 Nr. 9 KDG anzuerkennen sind.

Bei der Bestimmung der datenschutzrechtlichen Verantwortlichkeit kommt es nicht auf eine eigene Rechtspersönlichkeit des Verantwortlichen an. Neben Organisationen können auch Einzelpersonen oder Gruppen von Einzelpersonen Verantwortliche sein, sofern diese über Schlüsselelemente der Verarbeitung entscheiden.[8] Die Aufgaben, Befugnisse und Rollen, die den von den jeweiligen (Erz-)Bistümern einzurichtenden UAK nach der gemeinsamen Erklärung und den hierzu erlassenen Ordnungen und Statuten zugewiesen werden, gelten in tatsächlicher Hinsicht für die UAK, ohne dass es darauf ankommt, ob diese mit oder ohne eigener Rechtspersönlichkeit tätig sind.

c) Fazit zur datenschutzrechtlichen Verantwortlichkeit

Als datenschutzrechtlich Verantwortliche im Sinne des § 4 Nr. 9 KDG müssen die Unabhängigen Aufarbeitungskommissionen die datenschutzrechtlichen Pflichten des KDG einhalten. Hervorzuheben sind an dieser Stelle:

- Bestellung eines betrieblichen Datenschutzbeauftragten
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten
- Erstellung eines Datenschutzkonzepts
- Festlegung und Einhaltung von angemessenen technischen und organisatorischen Maßnahmen (vgl. zur Datensicherheit auch Ausführungen unter Ziff. III)
- Verpflichtung auf das Datengeheimnis

Die für die Umsetzung einer datenschutzkonformen Aufarbeitung erforderlichen (Finanz- und Sach-)Mittel sind den UAK bereitzustellen.

[7] Musterordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- oder hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung

[8] Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 7 Rn. 9.

III. Datensicherheit

Die Unabhängigen Aufarbeitungskommissionen müssen sicherstellen, dass die im Rahmen der Aufarbeitung verarbeiteten personenbezogenen Daten vor Verlust, Manipulation, unberechtigtem Zugriff und sonstigen Bedrohungen geschützt sind. Dafür haben sie gemäß § 26 KDG i. V. m. §§ 5, 6 Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen.

Im Rahmen der Aufarbeitung werden personenbezogene Daten der Datenschutzklasse III gemäß § 13 Abs. 1 KDG-DVO verarbeitet. Im Falle der Nutzung von IT-Systemen[9] sind bei der Wahl der technischen und organisatorischen Maßnahmen daher die konkreten Vorgaben nach § 13 Abs. 2 i. V. m. § 12 Abs. 2 KDG-DVO einzuhalten. Hervorgehoben werden sollen an dieser Stelle die folgenden beiden Vorgaben:

a) Zentrale Speicherung

Eine Speicherung der personenbezogenen Daten hat auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu erfolgen, sofern keine begründeten Ausnahmefälle vorliegen.

Mit Blick darauf, dass die Mitglieder der Unabhängigen Aufarbeitungskommissionen i. d. R. von unterschiedlichen Standorten aus arbeiten, ist diese Anforderung besonders relevant. Ein dezentrales Speichern von personenbezogenen Daten sollte ausgeschlossen werden, um zu verhindern, dass die personenbezogenen Daten der Datenschutzklasse III zur Realisierung der Aufarbeitung unübersichtlich vervielfacht werden und somit mehrfach vorhanden sind – wodurch insbesondere die Sicherstellung der Vertraulichkeit erschwert wird.

Es gibt verschiedene Möglichkeiten, hierfür eine passende Infrastruktur zu schaffen. Beispielsweise bietet sich hier eine eigene private Cloudlösung an, die im Hinblick auf Zugangs- und Zugriffs-, aber auch Datenexport-Möglichkeiten restriktiv konfiguriert ist.

[9] Auch im Falle papierbasierter Verarbeitung sind angemessene Schutzmaßnahmen zu treffen, auf die in dieser Stellungnahme nicht gezielt eingegangen wird.

b) Sichere Datenübermittlung

Die elektronische Übermittlung der personenbezogenen Daten außerhalb eines geschlossenen und gesicherten Netzwerks muss grundsätzlich verschlüsselt erfolgen.

Auf die Nutzung eines Faxgerätes sollte verzichtet werden. Im Falle des E-Mail-Versands sollte eine Ende-zu-Ende-Verschlüsselung sichergestellt sein. Hierfür kommen zum einen E-Mail-Verschlüsselungsverfahren wie S/MIME oder PGP in Betracht und zum anderen auch der Versand der personenbezogenen Daten ausschließlich in ausreichend passwortgeschützten Dokumenten.

c) Fazit Datensicherheit

Der Aufbau einer IT-Infrastruktur, die einen angemessenen Schutz der personenbezogenen Daten gewährleisten kann, hat in der Verantwortung der Unabhängigen Aufarbeitungskommission im Vorfeld der Aufarbeitung nachweisbar zu erfolgen, bzw. ist im Falle bereits begonnener Aufarbeitung dringend nachzuholen.

Da dies unerlässlich ist, damit die Aufarbeitung durch die Aufarbeitungskommissionen datenschutzkonform möglich ist, sind die dafür erforderlichen (Finanz- und Sach-)Mittel entsprechend der gemeinsamen Erklärung durch die (Erz-)Bistümer bereitzustellen.

12.11.2024

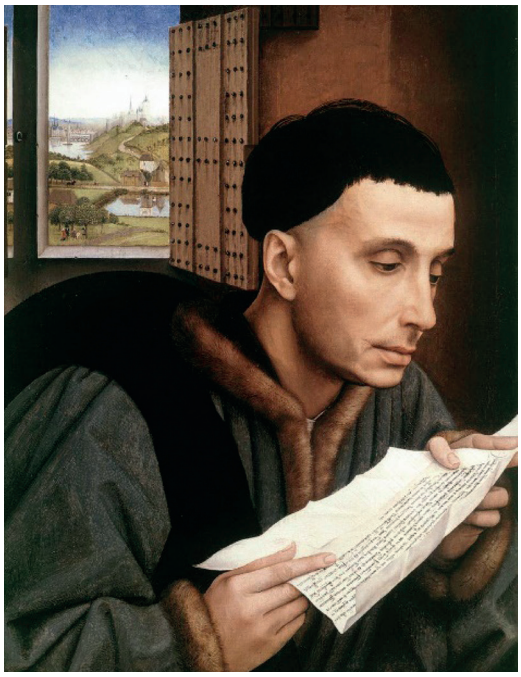
Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands
c/o Katholisches Datenschutzzentrum (KdöR), Brackeler Hellweg 144, 44309 Dortmund
Email: mail@konferenz-ddsb.de, Tel. 0231 / 138 985–0; Fax 0231 / 138 985–22

[6]

Abkürzungsverzeichnis

ArbG	Arbeitsgericht
Az	Aktenzeichen
beBPo	besonderes elektronisches Behördenpostfach
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfD EKD	Der Beauftragte für den Datenschutz der EKD
BfDI	Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
CNIL	Die Commission Nationale de l'Informatique et des Libertés (deutsch: Nationale Kommission für Informatik und Freiheiten) ist die nationale Datenschutzbehörde Frankreichs mit Sitz in Paris.
DBK	Deutsche Bischofskonferenz
DDSB	Diözesandatenschutzbeauftragte/r
DOK	Deutsche Ordensobernkonferenz
DPF	Data Privacy Framework (Datenschutzrahmen EU-USA)
DSG-DBK	Datenschutzgericht der Deutschen Bischofskonferenz – 2. Instanz
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz)
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss (englisch EDPB – European Data Protection Board)
EKD	Evangelische Kirche in Deutschland
EU	Europäische Union
EuGH	Europäischer Gerichtshof
HBDI	Der Hessische Beauftragte für Datenschutz und Informationsfreiheit
HinSchG	Hinweisgeberschutzgesetz
IDSG	Interdiözesanes Datenschutzgericht – 1. Instanz
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDG-VDD	KDG für den Verband der Diözesen Deutschlands
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum

KI	künstliche Intelligenz
KI-VO	Verordnung über künstliche Intelligenu (KI-Verordnung)
LDI	Landesbeauftragte für den Datenschutz und die Informationsfreiheit
LfD	Landesbeauftragte/r für Datenschutz
LKA	Landeskriminalamt
MD	Medizinischer Dienst
MDK	Medizinischer Dienst der Krankenversicherung
OH	Orientierungshilfe
OPS	Operationen- und Prozedurenschlüssel
OTP	One-Time-Password
RDP	Remote Desktop Protocol – ein Netzwerkprotokoll von Microsoft für den Fernzugriff auf Computer
RGDP	Regolamento Generale sulla protezione dei Dati personali (Datenschutzgesetz Vatikanstaat)
RL	Richtlinie
RSO-BiE	Rahmenschulordnung für Schulen in der Trägerschaft des Bistums Essen
SSH	Secure Shell – ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke
StrOPS-RL	„Regelmäßige Begutachtungen zur Einhaltung von Strukturmerkmalen von OPS-Kodes nach § 275d SGB V" (Richtlinie für die Begutachtung von Strukturmerkmalen von abrechnungsrelevanten Operationen- und Prozedurenschlüsseln)
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TOM	Technische und organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UAK	Unabhängige Aufarbeitungskommissionen
UBSKM	Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs
UID	Unique Identifier
US	United States (Vereinigte Staaten)
VDD	Verband der Diözesen Deutschlands (1.3.1)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VO	Verordnung
VPN	Virtual Private Network (Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist)



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