



Jahresbericht 2025

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.–31.12.2025



Katholisches
Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiozesen 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](https://www.istockphoto.com) | [matejmo](https://www.matejmo.com)

10. Jahresbericht

**des Diözesandatenschutzbeauftragten für die Erzdiö-
zesen 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 01.01.2025–31.12.2025

Redaktionsschluss: 31.05.2026

Inhaltsverzeichnis

Vorwort	7
► 1 Entwicklungen im Datenschutzrecht	9
1.1 Entwicklungen auf Ebene der Europäischen Union	9
1.1.1 EuGH-Verfahren zur Löschung von Taufbucheinträgen.....	9
1.1.2 Der Digital-Omnibus zur Änderung der DSGVO.....	9
1.1.3 Verfahrensregeln für die Durchsetzung der Verordnung EU 2016/679	10
1.1.4 Geschlechtsangaben für Fahrkartenkauf nicht erforderlich	12
1.1.5 Entscheidung des EuGH zur datenschutzrechtlichen Verantwortlichkeit von Betreibern von nutzergenerierten Online-Marktplätzen.....	13
1.2 Datenschutzrechtliche Entwicklungen in der Bundesrepublik Deutschland.....	14
1.2.1 Verfügung des BfDI zu den Facebook-Fanpages – neuer Zwischenstand durch die Entscheidung des Verwaltungsgerichts Köln	14
1.2.2 Bundesgerichtshof entscheidet zum Anwendungsbereich des Medienprivilegs	15
1.2.3 Gastzugang im Onlinehandel.....	16
1.2.4 Verfassungsbeschwerde wegen Akteneinsicht in das Protokoll einer Kirchen- gemeinderatssitzung.....	17
1.2.5 NIS-2-Umsetzungsgesetz tritt in Kraft.....	18
1.2.6 Verantwortlichkeit des Auftraggebers für Löschung oder Rückgabe von Daten beim Auftragsverarbeiter bei Vertragsende	18
1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche	19
1.3.1 Abschluss der Evaluierung des Gesetzes über den Kirchlichen Datenschutz	19
1.3.2 Die Note „Antiqua et nova“ des Vatikans.....	20
1.3.3 Novellierung des KDG-Schulen	21
1.3.4 Erläuternde Note des Vatikans zum Löschen von Taufbucheinträgen	22
1.3.5 Verarbeitung personenbezogener Daten im Zusammenhang mit den Wahlen der Kirchenvorstände und der pastoralen Gremien im Erzbistum Paderborn	23
1.3.6 Bistum Aachen weist auf das Verbot von Löschungen im Taufbuch hin.....	24
1.4 Weitere datenschutzrechtliche Entwicklungen im kirchlichen Bereich, insbeson- dere der EKD	24
1.4.1 EKD-Datenschutzgesetz und Datenschutzaufsicht.....	24
1.4.2 Anerkennungsrichtlinie der EKD.....	25
1.5 Aus der Arbeit des Europäischen Datenschutzausschusses, des EDPS und der nationalen Datenschutzaufsichten	25
1.5.1 Entscheidung des EDPS über die Verwendung von MS365 durch die Europäi- sche Kommission	26



1.5.2	Empfehlungen 2/2025 des EDSA für die Verpflichtung zur Einrichtung von Benutzerkonten auf E-Commerce-Websites	28
1.5.3	Leitlinien für den Einsatz generativer KI	29
1.6	Aufarbeitung des Missbrauchs.....	30
1.6.1	Austausch mit den fünf Unabhängigen Aufarbeitungskommissionen in den nordrhein-westfälischen (Erz-)Diözesen.....	30
1.6.2	Diözesangesetze zur Regelung von Einsichts- und Auskunftsrechten.....	31
1.6.3	Verlängerte Aufbewahrungspflichten bestimmter Akten in der Kinder- und Jugendhilfe durch das UBSKM-Gesetz.....	32
1.6.4	Aufarbeitung und personenbezogene Daten in Archivakten.....	33
1.7	Schwerpunkt Cyberangriffe/IT-Sicherheit	34
1.7.1	Cyberangriff auf die IT-Systeme des Sekretariates der Deutschen Bischofskonferenz....	35
1.7.2	Was ist der „Stand der Technik“?.....	36
1.7.3	Überblick zu ausgewählten IT-Sicherheit-Standards.....	37
1.7.4	Passwörter und Passkeys	41
► 2	Aus der Tätigkeit des Datenschutzzentrums	45
2.1	Beratungen und Anfragen	45
2.1.1	Datenschutz in der Flüchtlingsarbeit	45
2.1.2	Einwilligung und leichte Sprache.....	46
2.1.3	Nachweis der Informationserteilung nach § 15 KDG	47
2.1.4	Datenschutzrechtliche Verantwortlichkeit in den Beratungsstellen.....	48
2.1.5	Aufbewahrungsdauer der Dokumentation zu Datenschutzverletzungen.....	50
2.1.6	Fotos demenziell erkrankter Personen im Krankenhausinformationssystem	50
2.1.7	Auskunftsanspruch getrenntlebender Eltern mit gemeinsamem Sorgerecht.....	51
2.2	Meldungen von Datenschutzverletzungen.....	52
2.2.1	Falscher Name in E-Mail einer medizinischen Studie.....	54
2.2.2	E-Mail für die Mitarbeitervertretung an den falschen Verteiler gesendet	54
2.2.3	Foto in sozialen Medien enthält Patientendaten auf dem Monitor im Hintergrund ..	55
2.2.4	Diebstahl von Gehaltsabrechnungen aus dem Briefkasten der Einrichtung	56
2.2.5	Ausdrucke mit personenbezogenen Daten als Malpapier in der Kita	56
2.2.6	Vertauschter Patientenaufkleber.....	57
2.2.7	Weitergabe von Patientendaten an Polizei	57
2.2.8	Ransomware-Angriff bei ehrenamtlicher Tätigkeit auf dienstlichem PC.....	58
2.2.9	Mitarbeiter verschafft sich unbefugt Zugriff auf E-Mail-Account	59

2.3	Beschwerden und Hinweise.....	60
2.3.1	Mängel bei der Datenbereitstellung über eine Online-Dateiablage	61
2.3.2	Offenlegung von personenbezogenen Daten in der Notaufnahme.....	62
2.3.3	Öffnung von Gehaltsabrechnungen durch Arbeitgeber.....	64
2.4	Prüfungen	65
2.4.1	Ist der betriebliche Datenschutzbeauftragte beim Katholischen Datenschutz- zentrum gemeldet?	65
2.4.2	Prüfung von Datenschutzhinweisen auf Internetseiten	65
2.4.3	Prüfung des Einsatzes von Videoüberwachung in kirchlichen Einrichtungen	66
2.5	Künstliche Intelligenz	67
2.5.1	Päpstliche Mahnungen und kirchliche Leitlinien	67
2.5.2	Handreichungen für die Bundesverwaltung zum Umgang mit Künstlicher Intelligenz	68
2.5.3	Interne Vorgaben zur Nutzung von KI.....	69
2.6	Austausch mit den betrieblichen Datenschutzbeauftragten der (Erz-)Diözesen und der Diözesan-Caritasverbände	70
2.7	ZenDiS und opencode.de.....	71
2.8	Nicht-Benachrichtigung nach § 34 KDG	72
2.9	Spam-Anrufe eines „Datenschutzzentrums Dortmund“.....	73
2.10	Alternativen zu den großen sozialen Netzwerken nutzen	74
2.11	Einsicht in Patientenakten durch Mitarbeitende	74
▶ 3	Die kirchliche Datenschutzaufsicht in den nordrhein-westfälischen (Erz-)Diözesen und beim Verband der Diözesen Deutschlands	77
3.1	Der gemeinsame Diözesandatenschutzbeauftragte.....	77
3.2	Das Katholische Datenschutzzentrum.....	78
3.3	Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums	79
3.4	Öffentlichkeitsarbeit.....	80
3.5	Verfahren vor dem Interdiözesanen Datenschutzgericht und dem Datenschutzge- richt der Deutschen Bischofskonferenz.....	81
3.6	Zusammenarbeit mit der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder.....	81
▶ 4	Dokumentation – Die Datenschutzaufsicht in der katholischen Kirche	83
	Abkürzungsverzeichnis	85

Vorwort

Unruhige Zeiten für den Datenschutz

In den aktuellen Diskussionen in der Politik und Wirtschaft muss der Datenschutz für viele Fehlentwicklungen der letzten Jahre als Ursache herhalten. Zu streng, zu bürokratisch oder zu wirtschaftshemmend sind nur einige wenige Vorwürfe gegen den Datenschutz.

Unbestritten gibt es Punkte, die man sich anschauen muss. Bei den Anforderungen an kleine Einrichtungen oder Vereine ohne die Verarbeitung sensibler Daten muss die in der DSGVO und damit auch im KDG angelegte Orientierung am Risiko für die personenbezogenen Daten durch die konkrete Verarbeitung der Daten noch stärker hervorgehoben werden. Hier sind stärkere Abstufungen der Pflichten möglich, denen diese Einrichtungen und Vereine unterliegen.

Keine Lösung ist die im Zusammenhang mit dem Schlagwort Entbürokratisierung immer wieder genannte Aufweichung oder Abschaffung der Bestellpflicht für betriebliche Datenschutzbeauftragte. Mit dem Entfall einer Bestellpflicht scheint oft assoziiert zu werden, dass auch die Verpflichtungen aus der DSGVO bzw. dem KDG für diese Verantwortlichen entfallen würden. Dies ist aber gerade nicht der Fall. Unternehmens- und Einrichtungsleitungen sind auch ohne Bestellpflicht eines betrieblichen Datenschutzbeauftragten vollständig verantwortlich – und damit bei grober Vernachlässigung ihrer Pflichten als Leitung evtl. auch haftbar – für die Einhaltung datenschutzrechtlicher Vorgaben und Pflichten. Es fehlt ihnen ohne betrieblichen Datenschutzbeauftragten dann eben nur die fachlich versierte Person im Haus, die sie berät.

Da, wo es wirklich nicht rund läuft, muss nachgebessert werden. Aber bitte nach fachlicher Diskussion mit allen beteiligten Stellen, damit nachher wirklich ein besserer Datenschutz herauskommt – für die Unternehmen und die Einrichtungen, aber eben auch für die betroffenen Personen, die auf den Schutz durch ein Grundrecht hoffen.

Mit dem Ablauf meiner zweiten Amtszeit im Herbst 2026 werde ich die Aufgabe als Diözesandatenschutzbeauftragter für die fünf nordrhein-westfälischen (Erz-)Diözesen und als Verbandsdatenschutzbeauftragter als Datenschutzaufsicht über den Verband der Diözesen Deutschlands, den Rechtsträger der Deutschen Bischofskonferenz, nach 10 Jahren in andere Hände geben. Dabei gilt mein Dank den vielen Menschen, mit denen ich mich in diesen Jahren fachlich austauschen und vertrauensvoll zusammenarbeiten durfte.

Der Aufbau der Körperschaft „Katholisches Datenschutzzentrum“ als Datenschutzstelle für die Funktion des Diözesandatenschutzbeauftragten war eine einmalige Erfahrung. Zusammen mit den Kolleginnen und Kollegen haben wir etwas Gutes und Wirksames geschaffen – eine kirchliche Datenschutzaufsicht, die ihre Aufgabe wirksam im Sinne des Grundrechtsschutzes für die einzelnen Personen erfüllt, hierbei aber auch die Interessen der Kirche mit ihrer grundrechtlich garantierten Religionsfreiheit nicht außer Acht lässt. Diese Grundrechtsabwägung ist anspruchsvoll und mühsam und gelingt nicht immer zur Zufriedenheit der an den Verfahren beteiligten Personen oder kirchlichen Stellen. Eine



Abwägung, die mit dem EuGH auch das höchste europäische Gericht erreicht hat (Bisdom Gent, Rs. C-12/25 zur Löschung von Taufbucheinträgen). Wir hatten die Möglichkeit, als Zuhörer an der mündlichen Verhandlung des EuGH in Luxemburg Ende Juni 2026 teilzunehmen und dieses Ringen um die Abwägung dieser Grundrechte persönlich zu erleben. Die mit Spannung erwartete Entscheidung des EuGH wird auch die zukünftige Arbeit des Katholischen Datenschutzzentrums beeinflussen.

Abschließend gilt mein herzlicher Dank insbesondere den Kolleginnen und Kollegen des Katholischen Datenschutzzentrums, ohne die ich meine Aufgabe als Leitung der Datenschutzaufsicht nicht hätte erfüllen können.

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

1 Entwicklungen im Datenschutzrecht

Der Bereich des Datenschutzrechts ist kontinuierlich im Wandel. In diesem Abschnitt wird eine Auswahl einiger Entwicklungen im Datenschutzrecht auf europäischer, nationaler und kirchlicher Ebene im Jahr 2025 dargestellt.

1.1 Entwicklungen auf Ebene der Europäischen Union

Blickt man auf das Jahr 2025 zurück, zeigen sich auf europäischer Ebene erneut wichtige Entwicklungen im Bereich Datenschutzrecht. In diesem Abschnitt werden ein paar der Entscheidungen und Vorhaben aufgegriffen, die aus Sicht des Katholischen Datenschutzzentrums relevant sind.

1.1.1 EuGH-Verfahren zur Löschung von Taufbucheinträgen

In einem Anfang 2025 beim EuGH eingegangenen Verfahren¹, welches derzeit auch noch nicht entschieden ist, darf sich der EuGH mit der Frage der Löschung von Taufbucheinträgen beschäftigen. Im Jahresbericht 2024 hat das KDSZ bereits auf die Vorlagefragen des belgischen Gerichts an den EuGH hingewiesen.² Die Vorlagefragen des Gerichts gingen Anfang 2025 beim EuGH ein. Die mündliche Verhandlung fand Ende Juni 2026 statt und die Schlussanträge der Generalanwältin sollen am 01.10.2026 vorliegen. Das Urteil folgt dann wenige Monate nach den Schlussanträgen.

Der kirchliche Gesetzgeber in Deutschland hat auf die Diskussionen in Belgien und anderen europäischen Ländern reagiert und mit der am 01.03.2026 in Kraft getretenen novellierten Fassung des kirchlichen Datenschutzgesetzes eine Regelung hierzu in das KDG eingefügt. Mit der neuen Formulierung des § 19 Abs. 3 lit. f) KDG besteht ein Anspruch auf Löschung dann nicht, soweit die Verarbeitung erforderlich ist „zum Erhalt und zur Gewährleistung der Nachvollziehbarkeit von Amtshandlungen sowie von Urkunden und vergleichbaren Dokumenten; hierzu gehören insbesondere die durch kirchliche Rechtsvorschriften vorgesehenen Eintragungen in die Kirchenbücher (insbesondere Taufen, Trauungen, Todesfälle) sowie Dekrete, Beschlüsse von Gremien der Diözesen und Kirchengemeinden und sonstige Urkunden“.

1.1.2 Der Digital-Omnibus zur Änderung der DSGVO

Während die katholische Kirche in Deutschland im Berichtszeitraum die Novelle des kirchlichen Datenschutzrechts vorangetrieben hat³, hat die

¹ EuGH, Rs. C-12/25.

² Abschnitt 1.1.2 des Jahresberichts 2024.

³ Für Informationen zum novellierten KDG siehe in diesem Jahresbericht unter 1.3.1.

Europäische Kommission den Aufschlag für eine Erneuerung des staatlichen Datenschutzrechts gemacht.⁴

Anlass für die Reform des staatlichen Datenschutzrechts ist u. a. die immer größere Dichte an Rechtsakten, die sich mit digitalen Inhalten beschäftigen (z. B. KI und Datennutzung). Dabei hat der europäische Gesetzgeber stets betont, dass diese Rechtsakte nebeneinanderstehen und den Inhalt der jeweils anderen nicht beeinflussen sollen. Ein solches Bestreben erscheint aus Gesichtspunkten parlamentarischer Effizienz verständlich, da so bisher vermieden werden konnte, bei jedem neuen Digitalrechtsakt alte Gesetze zu überarbeiten. Diese Vorgehensweise ist aus Sicht des Rechtsanwenders jedoch nicht vorteilhaft. Die mittlerweile hohe Dichte an Digitalrechtsakten hat zu vielfältigen Compliancepflichten für Verantwortliche geführt, die zum Teil in einem (noch) unklaren Verhältnis zueinanderstehen. Das verursacht nicht nur einen hohen Verwaltungsaufwand, sondern auch hohe Kosten.

Um wirtschaftliches Wachstum und Innovationen zu fördern, möchte die EU-Kommission die Digitalgesetzgebung daher vereinfachen. Dabei sollen die Rechtsakte in einem höheren Maß zueinander harmonisiert werden. Auch die DSGVO soll im Rahmen dieses Gesetzespakets überarbeitet werden. Im Fokus des Änderungsentwurfs stehen dabei vor allem Entlastungen für kleine und mittlere Unternehmen (KMU). Hervorzuheben sind aus Sicht des Katholischen Datenschutzzentrums neue Rechtsgrundlagen für das Training von KI, Präzisierung von Versagungsgründen bei Betroffenenrechten, die deutliche Entschärfung der Meldepflichten für Datenschutzverletzungen (96 anstatt 72 Stunden und nur bei hohem Risiko), Harmonisierung von DSFA-Muss-Listen und die Festlegung von Pseudonymisierungskriterien durch die Kommission.

Das Katholische Datenschutzzentrum und die von ihm zu überwachen- den Einrichtungen sind zwar nicht unmittelbar von den Novellierungen der DSGVO betroffen. Änderungen in der DSGVO werden nachfolgend aber auch Änderungen im kirchlichen Datenschutzrecht nach sich ziehen. Kirchliche Verantwortliche sollten den europäischen Gesetzgebungsprozess daher beobachten. Das Katholische Datenschutzzentrum begrüßt jede Veränderung, die zum (sinnvollen) Abbau von Bürokratie beiträgt, ohne dabei die Rechte von Betroffenen zu schwächen. Wie EU-Kommission, Rat und EU-Parlament die Abwägung der Interessen zwischen Betroffenenrechten und Erleichterungen für KMU gestalten werden, bleibt abzuwarten.



„Das KDSZ begrüßt jede Veränderung, die zum (sinnvollen) Abbau von Bürokratie beiträgt, ohne dabei die Rechte von Betroffenen zu schwächen.“

1.1.3 Verfahrensregeln für die Durchsetzung der Verordnung EU 2016/679

Die Europäische Union hat mit der Verordnung EU 2025/2518⁵ vom 26.11.2025 die Verfahrensregelungen für die Durchsetzung der Verordnung EU 2016/679 konkretisiert. Sie trat 20 Tage nach Veröffentlichung in Kraft. Die verbindliche Anwendung beginnt ab dem 02.04.2027, um

⁴ Pressemitteilung der EU-Kommission u. a. abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_25_2718

⁵ Verordnung (EU) 2025/2518 vom 26. November 2025 zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679, ABl. L, 2025/2518, 12.12.2025.



den Aufsichtsbehörden und betroffenen Organisationen ausreichend Zeit zu geben, die neuen Abläufe einzurichten.

Ziel der Verordnung ist, die kohärente Anwendung und effiziente Bearbeitung von Beschwerden in grenzüberschreitenden Fällen zu gewährleisten und die Rechte der Betroffenen sowie die Pflichten der Aufsichtsbehörden klarer zu definieren.

Die neue Verordnung richtet sich primär an nationale Datenschutzbehörden, die im Rahmen der DSGVO tätig sind. Sie definiert Mindestanforderungen für die Zulässigkeit von Beschwerden, legt fest, wie Informationen zwischen Behörden ausgetauscht werden, regelt Verfahrensfristen und beschreibt den Ablauf von Ermittlungs- und Konsultationsverfahren. Damit soll die bisherige Praxis harmonisiert werden, da die Umsetzung der DSGVO in verschiedenen Mitgliedstaaten bislang unterschiedliche Verfahren, Zeitpläne und Anforderungen kannte.

Die Verordnung verlangt, dass eine Beschwerde ausreichende Mindestinformationen enthält, damit die Aufsichtsbehörde prüfen kann, ob sie die Angelegenheit bearbeitet. Dazu zählen insbesondere Angaben, die die Identität des Beschwerdeführers, die betroffenen Datenkategorien sowie eine Beschreibung des behaupteten Verstoßes betreffen.

Gleichzeitig stellt die Verordnung sicher, dass keine zusätzlichen oder unverhältnismäßigen Angaben verlangt werden dürfen. Betroffene müssen beispielsweise keine sensiblen Daten einreichen, die für die Prüfung der Beschwerde irrelevant sind. Auf dieser Grundlage können unzulässige Beschwerden von der Behörde innerhalb kurzer Fristen zurückgewiesen oder zur Nachbesserung zurückgegeben werden.

Für Fälle, die mehrere Mitgliedstaaten betreffen, legt die Verordnung die Zuständigkeit der federführenden Aufsichtsbehörde fest. Weitere beteiligte Behörden sind verpflichtet, Informationen innerhalb vorgegebener Fristen bereitzustellen und an Konsultationsverfahren teilzunehmen. Bei Meinungsverschiedenheiten zwischen den Behörden schreibt die Verordnung formal geregelte Abstimmungsprozesse vor, um eine kohärente Entscheidung zu gewährleisten.

Diese Mechanismen sollen sicherstellen, dass grenzüberschreitende Verfahren effizient bearbeitet werden und Rechtsunsicherheiten für Betroffene und Unternehmen minimiert werden.

Des Weiteren konkretisiert die Verordnung die Fristen für die Bearbeitung von Beschwerden und Ermittlungen. Sie sieht außerdem vereinfachte Verfahren für Fälle vor, in denen die Sachlage eindeutig ist oder das Unternehmen bereits Abhilfemaßnahmen ergriffen hat. Damit können einfache Verstöße schneller erledigt werden, ohne dass die beteiligten Behörden unnötig belastet werden.

Betroffene haben das Recht, über die Annahme ihrer Beschwerde informiert zu werden, sowie eine Gelegenheit zur Stellungnahme, bevor Entscheidungen getroffen werden. Unternehmen oder andere Verantwortliche, gegen die sich eine Beschwerde richtet, haben ebenfalls Anspruch auf Anhörung. Diese Regelungen gewährleisten, dass Verfahren transparent, fair und nachvollziehbar durchgeführt werden.



„Ziel der Verordnung ist, die kohärente Anwendung und effiziente Bearbeitung von Beschwerden in grenzüberschreitenden Fällen zu gewährleisten und die Rechte der Betroffenen sowie die Pflichten der Aufsichtsbehörden klarer zu definieren.“

1.1.4 Geschlechtsangaben für Fahrkartenkauf nicht erforderlich

In einem Verfahren⁶ befasste sich der EuGH mit den notwendigen Daten für einen Fahrkartenkauf. Mit seinem Urteil vom 09.01.2025 entschied der EuGH, dass Unternehmen beim Online-Verkauf von Fahrkarten nicht verpflichtend das Geschlecht ihrer Kunden abfragen dürfen, wenn diese Angabe für den Vertrag nicht erforderlich ist. Eine verpflichtende Auswahl zwischen den Anreden „Herr“ und „Frau“ verstößt demnach gegen die Datenschutz-Grundverordnung (DSGVO).

Auslöser des Verfahrens war eine Beschwerde gegen ein französisches Verkehrsunternehmen. Dieses verlangte beim Online-Ticketkauf zwingend die Auswahl einer geschlechtsspezifischen Anrede. Eine Datenschutzorganisation sah darin einen Verstoß gegen das Prinzip der Datenminimierung und rief die französische Datenschutzbehörde an. Nachdem diese die Beschwerde zurückgewiesen hatte, landete der Fall über den französischen Staatsrat beim EuGH.



„Der EuGH stellte klar, dass die Datenerhebung dem Zweck angemessen und auf das notwendige Maß beschränkt sein muss – ein zentraler Grundsatz der DSGVO.“

Der EuGH stellte klar, dass die Datenerhebung dem Zweck angemessen und auf das notwendige Maß beschränkt sein muss – ein zentraler Grundsatz der DSGVO. Die Angabe einer Anrede zur Personalisierung von E-Mails oder anderer Kommunikation sei für den Vertragsschluss oder die Leistungserbringung (also den Ticketkauf) nicht objektiv unerlässlich. Deshalb sei eine verpflichtende Abfrage des Geschlechts über diese Anrede datenschutzrechtlich nicht zulässig.

Nach Ansicht des Gerichts können Verkehrsdienstleister stattdessen neutralere Formen der Ansprache wählen oder die Abfrage einer Anrede als freiwillige Angabe kennzeichnen, wenn Kunden diese Option einer persönlicheren Ansprache nutzen möchten. Eine verpflichtende Auswahl zwischen „Herr“ und „Frau“ hingegen widerspreche dem Grundsatz der Datenminimierung und könne zudem Risiken der Diskriminierung bergen.

Hinweis für kirchliche Einrichtungen

Die Entscheidung ist auch auf die Datenerhebungen kirchlicher Stellen übertragbar. Kirchliche Stellen sollten in der Folge des Urteils daher prüfen, welche Angaben sie als verpflichtend im Rahmen ihrer Datenerhebungen z. B. zum Abschluss bzw. zur Erfüllung eines Vertrages abfragen. Der EuGH gibt hier die klare Linie vor, dass die Erhebung von Daten – soweit diese als verpflichtende Angabe ausgestaltet ist – dem Zweck angemessen und auf das notwendige Maß beschränkt sein muss. Sofern Daten, wie hier die Anrede, zur persönlicheren Kundenansprache erhoben und nicht als unbedingt notwendige Angabe benötigt werden, können diese Angaben zukünftig freiwillig erhoben werden.

⁶ EuGH, Urteil vom 09.01.2025, Rs. C 394/23.

1.1.5 Entscheidung des EuGH zur datenschutzrechtlichen Verantwortlichkeit von Betreibern von nutzergenerierten Online-Marktplätzen

Der EuGH hat mit Urteil vom 02.12.2025 in der Rechtssache C-492/23 („Russmedia Digital“) die datenschutzrechtliche Verantwortlichkeit von Betreibern nutzergenerierter Online-Marktplätze festgelegt. In seiner Entscheidung stellt der Gerichtshof klar, dass der Betreiber eines Online-Marktplatzes für die Verarbeitung personenbezogener Daten verantwortlich sein kann, wenn solche Daten in Nutzeranzeigen enthalten sind und über die Plattform im Internet veröffentlicht werden.⁷

Anlass war eine Anzeige auf dem rumänischen Portal „publi24.ro“, in der eine Frau ohne ihre Kenntnis und ohne Einwilligung mit sexuellen Dienstleistungen in Verbindung gebracht wurde. Die Anzeige enthielt zudem Fotos der Betroffenen und ihre Telefonnummer. Zwar entfernte der Betreiber den Inhalt nach einem Hinweis sehr schnell, dennoch war die Anzeige zu diesem Zeitpunkt bereits an anderer Stelle erschienen und blieb dort zugänglich. Vor den rumänischen Gerichten stellte sich daraufhin die Frage, ob der Plattformbetreiber für die Anzeige und deren Inhalt als Verantwortlicher mit eigenständigen Pflichten nach der DSGVO gelten kann.⁸

Der EuGH nahm im vorliegenden Fall an, dass der Betreiber eines Online-Marktplatzes verantwortlich für auf diesem Portal veröffentlichte Anzeigen beziehungsweise deren Inhalte sein könne. Dafür müsse der Plattformbetreiber u. a. eigene (kommerzielle) Zwecke verfolgen, weitgehende Nutzungsrechte an den eingestellten Inhalten haben (z. B. Nutzung, Verbreitung und Übermittlung) und bei der Festlegung der Mittel der Verarbeitung mitwirken (z. B. Zielpublikum, Darstellung, Dauer der Verbreitung). Indizien für eine Mitwirkung seien beispielsweise auch Nutzungsbedingungen der Plattform. Der Inhalt der allgemeinen Nutzungsbedingungen könne belegen, dass der Betreiber die Verarbeitung maßgeblich beeinflusse und damit die Mittel festlege. Bei Russmedia sprächen die dort vorbehaltenen Verwertungs- und Löschrechte dafür.⁹

Besonders praxisrelevant ist die vom Gerichtshof betonte Vorverlagerung von Schutz- und Rechenschaftspflichten bei Anzeigen, die sensible Daten enthalten. In dem Urteil heißt es unter Randnummer 97:

„... ist dieser Betreiber als Verantwortlicher daher verpflichtet, schon bei der Konzeption seines Dienstes geeignete technische und organisatorische Maßnahmen zu treffen, um solche Anzeigen vor ihrer Veröffentlichung zu identifizieren und so in der Lage zu sein, zu überprüfen, ob die in ihnen enthaltenen sensiblen Daten im Einklang mit den in Kapitel II dieser Verordnung festgelegten Grundsätzen veröffentlicht werden. Wie sich nämlich u. a. aus Art. 25 Abs. 1 DSGVO ergibt, obliegt ihm die Verpflichtung, solche Maßnahmen durchzuführen, nicht nur zum Zeitpunkt der Verarbeitung, sondern bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung und damit sogar schon, bevor auf seinem Online-Marktplatz unter Verstoß gegen diese Grundsätze sensible Daten veröffentlicht werden, da mit dieser Verpflichtung gerade solche Verstöße verhindert werden sollen.“

⁷ EuGH, Urteil vom 02.12.2025 (Rs. C-492/23).

⁸ Pressemitteilungen des EuGH Nr. 14 und Nr. 150 aus 2025.

⁹ EuGH, Urteil vom 02.12.2025 (Rs. C-492/23), Rn. 47 bis 76.

Zusätzlich verlangt der EuGH unter Randnummer 122 der Entscheidung von Verantwortlichen Maßnahmen, um die Vervielfältigung und Kopie von unrechtmäßig veröffentlichten personenbezogenen Daten zu verhindern:

„Dabei muss der Verantwortliche u. a. alle nach dem Stand der Technik¹⁰ verfügbaren technischen Maßnahmen in Betracht ziehen, die die Kopie und Replikation des Online-Inhalts blockieren können.“

Hinweis für kirchliche Einrichtungen

Das Urteil ist für kirchliche Einrichtungen relevant, die Online-Angebote einsetzen, in denen die Möglichkeit gegeben wird, Inhalte zu veröffentlichen oder hochzuladen (etwa Marktplatz- oder Schwarzes-Brett-Funktionen, Kommentarräume, Portale für Gemeindekommunikation oder Bild-Uploads). Auch wenn solche Betreiberkonstellationen in kirchlichen Einrichtungen regelmäßig nicht zum Alltag gehören, sollten betroffene Verantwortliche die Rollenfrage (bloßer Dienstleister oder (Mit-)Verantwortlicher) konsequent prüfen. Das kann anhand der im Urteil festgelegten Kriterien gelingen (beispielsweise Plattformdesign, Moderations-/Durchsetzungsmöglichkeiten und Nutzungsbedingungen). Kommt es zu Beschwerden oder Meldungen bezüglich solcher Plattformen, Apps oder Angebote, wird diese Einordnung der Verantwortlichkeit durch das Katholische Datenschutzzentrum regelmäßig als Vorfrage überprüft werden.

1.2 Datenschutzrechtliche Entwicklungen in der Bundesrepublik Deutschland

Auch auf nationaler Ebene gab es im Berichtsjahr datenschutzrechtliche Entwicklungen. In diesem Abschnitt werden einige dieser Themen beleuchtet.

1.2.1 Verfügung des BfDI zu den Facebook-Fanpages – neuer Zwischenstand durch die Entscheidung des Verwaltungsgerichts Köln

Mit dem Bescheid im Jahr 2023 gegen den Betrieb einer Facebook-Fanpage durch das Bundespresseamt versucht der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die strittigen Fragen gerichtlich klären zu lassen. Die vom Bundespresseamt gegen den Bescheid erhobene Klage vor dem Verwaltungsgericht wurde im Berichtszeitraum vom VG Köln entschieden. Das Verfahren geht aber weiter. Die vor dem Verwaltungsgericht unterlegene BfDI hat beim Oberverwaltungsgericht Münster Berufung eingelegt.

In dem Bescheid des BfDI aus 2023 wurde dem Bundespresseamt der Betrieb der Facebook-Fanpage wegen Datenschutzmängeln untersagt.

¹⁰ Zum Stand der Technik siehe Abschnitt 1.7.2 des Jahresberichts.

Die damalige Untersagung stützte sich insbesondere auf die Tatsache, „dass beim Aufruf einer Fanpage von Meta auf den Endgeräten der Nutzerinnen und Nutzer unterschiedlich viele Cookies gespeichert und ausgelesen werden (...)“.¹¹

In seiner Entscheidung vom 17.07.2025 hat das Verwaltungsgericht Köln den Bescheid des BfDI aufgehoben¹². Das Verwaltungsgericht ist der Ansicht, dass sich nur Meta und nicht auch das Bundespresseamt eine Einwilligung der Nutzer für die Datenverarbeitung einholen müsse. Weiter betont das Gericht, dass das Bundespresseamt und Meta nicht als gemeinsame Verantwortliche im Sinne der DSGVO zu klassifizieren seien. Das VG stellt dabei insbesondere darauf ab, dass das Bundespresseamt selbst keine Parameter für die Platzierung der Cookies und die Auswertung der erhobenen Daten vorgeben könne.

Die BfDI hat in der Folge der Entscheidung des Verwaltungsgerichtes eine „Handreichung zur Nutzung sozialer Netzwerke durch öffentliche Stellen des Bundes“¹³ herausgegeben, mit der sie den ihrer Aufsicht unterliegenden Stellen eine Hilfestellung geben will, wie soziale Netzwerke in der Umsetzung des Urteils und bis zu einer endgültigen Klärung des Rechtsstreits rechtskonform genutzt werden können.

Hinweis für kirchliche Einrichtungen

Auch für kirchliche Einrichtungen ist die Handreichung interessant. Dabei ist zu beachten, dass sich die Handreichung nur auf die Datenverarbeitung in eigener Verantwortlichkeit bezieht. Die weitere Entwicklung des Verfahrens bleibt abzuwarten.

1.2.2 Bundesgerichtshof entscheidet zum Anwendungsbereich des Medienprivilegs

Der Bundesgerichtshof (BGH) hat in seiner Entscheidung vom 29.07.2025 (Az. VI ZR 426/24) klargestellt, dass der Schutz des sogenannten Medienprivilegs auch für Beiträge gilt, die über soziale Kommunikationsplattformen verbreitet werden und damit weit über klassische Presse- und Rundfunkformate hinausreicht.

Im Zentrum des Rechtsstreits stand ein Beitrag auf einem Telegram-Kanal, in dem der Name eines Abgeordneten im Zusammenhang mit einer politischen Aktion genannt wurde. Der Kläger machte geltend, seine Persönlichkeitsrechte seien dadurch verletzt worden und verlangte Unterlassung sowie Schadensersatz. Die Beklagte trat dem entgegen und berief sich auf das Medienprivileg gemäß Artikel 85 Absatz 2 der Datenschutz-Grundverordnung in Verbindung mit § 23 Absatz 1 Satz 4 des Medienstaatsvertrags (MStV).

¹¹ Der Bescheid der BfDI ist abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1.

¹² VG Köln, Az. 13 K 14 19/23.

¹³ Die Handreichung ist abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2025/Handreichung-Social-Media.pdf?__blob=publicationFile&v=4.



„Ziel dieser Regelung ist es, den Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.“

Der BGH bejahte die Anwendbarkeit des Medienprivilegs. Nach seiner Ansicht fällt die Veröffentlichung des streitigen Beitrags in den Anwendungsbereich des Medienprivilegs. Dieses Privileg erlaubt es, personenbezogene Daten zu verarbeiten, wenn dies zu journalistischen Zwecken geschieht, ohne dass die strengen Voraussetzungen der DSGVO erfüllt sein müssen. Ziel dieser Regelung ist es, den Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

Der nationale Gesetzgeber habe diesen Grundsatz im § 23 Absatz 1 Satz 4 MStV umgesetzt, indem er für Anbieter von Telemedien – zu denen auch Telegram-Kanäle gehören – Ausnahmen von den datenschutzrechtlichen Pflichten vorsehe, sofern sie journalistisch tätig seien. Dabei komme es nicht auf die bloße organisatorische Form des Anbieters an, sondern auf die Funktion der Tätigkeit.

Der BGH erläutert in seiner Entscheidung zudem den Begriff „journalistische Zwecke“. Dabei macht er deutlich, dass der Begriff nicht auf klassische Redaktionen beschränkt sei. Entscheidend sei, dass der jeweilige Beitrag an der öffentlichen Meinungsbildung mitwirke. Der hier streitige Telegram-Beitrag habe dazu gedient, über eine Demonstration zu informieren, an der politischen Willensbildung mitzuwirken und politische Kritik zu äußern. Damit verfolge er eindeutig journalistische Zwecke, so das Gericht. Entgegen früherer, restriktiverer Verwaltungs-Rechtsprechung müsse für das Medienprivileg nicht mehr eine organisatorisch eigenständige journalistische Redaktion vorliegen. Die Änderungen der gesetzlichen Regelungen im Rahmen der Anpassung des Medienstaatsvertrags an die DSGVO zeigten, dass bereits jede Datenverarbeitung „zu journalistischen Zwecken“ ausreiche.

Mit diesem Urteil bindet der Bundesgerichtshof die Reichweite des Medienprivilegs nicht mehr an die traditionelle Presseorganisation, sondern stellt auf die funktionale journalistische Tätigkeit ab. Das hat insbesondere für soziale Netzwerke, Blogs und andere Telemedien erhebliche Bedeutung, weil damit ein weites Schutzzfeld für öffentliche Kommunikation und Informationsverbreitung entsteht.

1.2.3 Gastzugang im Onlinehandel

Das Oberlandesgericht Hamburg hat in einer Entscheidung¹⁴ klargestellt, dass Betreiber von Online-Shops oder -Marktplätzen nicht grundsätzlich verpflichtet sind, einen Gastzugang für Bestellungen anzubieten. Das Gericht wies damit die Klage eines Verbraucherverbands ab, der dies von einem großen Online-Marktplatz unter Berufung auf Datenschutz- und Wettbewerbsrecht verlangt hatte.

Das OLG bestätigte mit seinem Urteil die klageabweisende Entscheidung der Vorinstanz¹⁵ und verneinte sowohl einen DSGVO-Verstoß als auch einen wettbewerbsrechtlichen Unterlassungsanspruch.

Das Gericht betonte, dass ein Gastzugang nicht zwingend vorgeschrieben sei. Entscheidend sei, dass die erhobenen Daten für die Bestellab-

¹⁴ OLG Hamburg, Urte. v. 27.02.2025, Az. 5 U 30/24.

¹⁵ LG Hamburg, Urte. v. 22.02.2024, Az. 327 O 250/22.

wicklung notwendig und verhältnismäßig sind. Die für die Registrierung erhobenen Daten – Name, Anschrift, E-Mail-Adresse – seien auch bei einem Gastkauf erforderlich, um Lieferung und Kommunikation zu gewährleisten. Ein Kundenkonto könne zudem organisatorische Vorteile bringen, etwa für die Abwicklung komplexer Marktplatzstrukturen, die Kommunikation mit mehreren Händlern und die Betrugsprävention.

Das OLG ließ einen wettbewerbsrechtlichen Unterlassungsanspruch schon daran scheitern, dass kein Verstoß gegen den Grundsatz der Datenminimierung feststellbar sei.

Hinweis für kirchliche Einrichtungen

Das OLG Hamburg bestätigt, dass ein verpflichtendes Kundenkonto im Onlinehandel rechtmäßig sein kann, auch wenn kein Gastzugang angeboten wird. Entscheidend ist eine Einzelfallprüfung, ob die erhobenen Daten notwendig, verhältnismäßig und zweckgerecht sind. Eine generelle Pflicht zur Bereitstellung eines Gastzugangs ergibt sich aus Sicht des OLG aus der DSGVO nicht.

1.2.4 Verfassungsbeschwerde wegen Akteneinsicht in das Protokoll einer Kirchengemeinderatssitzung

Im letzten Jahresbericht des Katholischen Datenschutzzentrums wurde bereits von einer Entscheidung des Bundesarbeitsgerichts¹⁶ berichtet, in der es um das Auskunftsrecht zu Entscheidungen in Personalsachen von kirchengemeindlichen Gremien in nicht öffentlichen Sitzungen einer evangelischen Kirchengemeinde ging. Darin begehrte die Klägerin nach Art. 15 Abs. 3 DSGVO die Herausgabe einer Kopie eines Protokolls einer nichtöffentlichen Sitzung des Kirchengemeinderates, in dem arbeitsrechtliche Maßnahmen gegen die Klägerin besprochen wurden. Die Beklagte hatte die Herausgabe unter Verweis auf die kirchenrechtliche Verschwiegenheitspflicht zu Inhalten nichtöffentlicher Sitzungen des Kirchengemeinderates verweigert. Das Bundesarbeitsgericht sah den Anspruch der Klägerin zwar nicht vorrangig in Art. 15 DSGVO oder im DSG-EKD, jedoch begründete es den Anspruch aus arbeitsrechtlichen Vorschriften. Der Anspruch der Klägerin auf Auskunft und Überlassung einer Kopie beruhe auf dem Arbeitsverhältnis und sei durch dieses bedingt.

Gegen die Entscheidung des Bundesarbeitsgerichts legte die Kirchengemeinde Verfassungsbeschwerde ein. Mit Beschluss vom 20.03.2026¹⁷ hat das Bundesverfassungsgericht die Verfassungsbeschwerde nicht zur Entscheidung angenommen, weil die Beschwerdeführerin nicht hinreichend substantiiert dargelegt hatte, dass und aus welchen Gründen das angegriffene Urteil des Bundesarbeitsgerichts sie in ihren Verfassungsrechten verletzte. Weder sei ersichtlich, dass das Bundesarbeitsgericht das kirchliche Recht willkürlich ausgelegt hätte, noch sei die Tragweite der geltend gemachten Grundrechte in Form des kirchlichen

¹⁶ BAG, Urt. v. 17.10.2024 – Az. 8 AZR 42/24; siehe Abschnitt 1.2.5 des Jahresberichts 2024.

¹⁷ BVerfG, Beschluss vom 20.03.2026 – 2 BvR 211/25, insbesondere Rn. 30, 35–45; vgl. für einen ausführlicheren Beitrag über die Entscheidung auch Neumann, BVerfG entscheidet im Streit um Kirchengemeindeprotokoll, Artikel 91 v. 07.04.2026.

Selbstbestimmungsrechts und der Religionsfreiheit verkannt worden. Darüber hinaus habe die Kirchengemeinde als Beschwerdeführerin nicht darlegen können, dass es in der Entscheidung des Bundesarbeitsgerichts zu einer willkürlichen Auslegung der Geheimhaltungsvorschriften der Kirchengemeindeordnung gekommen sei. Nach Auffassung des Gerichts steht der Herausgabe einer Protokollkopie der Schutz des internen Meinungsbildungsprozesses nicht entgegen. Denn der Inhalt der Beratungen muss nur insoweit protokolliert werden, wie dies zum Verständnis der gefassten Beschlüsse erforderlich ist.

1.2.5 NIS-2-Umsetzungsgesetz tritt in Kraft

Am 06.12.2025 trat das Gesetz zur Umsetzung der NIS-2-Richtlinie in Kraft.¹⁸ Die europäische NIS-2-Richtlinie soll die Sicherheit der Netz- und Informationssysteme verbessern. Mit dem nationalen Gesetz sind die Anforderungen der europäischen Vorgabe in nationales Recht überführt worden.

Im Vergleich zu den bisherigen Regelungen wird dadurch u. a. der Anwendungsbereich des BSI-Gesetzes deutlich erweitert. Nun unterfallen deutlich mehr Unternehmen den Vorgaben.

Fällt ein Unternehmen in den Anwendungsbereich der neuen Regelungen, so ist es gesetzlich verpflichtet, sich zu registrieren, erhebliche Sicherheitsvorfälle zu melden sowie Risikomanagementmaßnahmen zu implementieren und zu dokumentieren.

Von der neuen Regelung ist aber nicht nur die Privatwirtschaft betroffen, auch für Einrichtungen der Bundesverwaltung gelten die nun umgesetzten Regelungen. So wird von den Einrichtungen der Bundesverwaltung u. a. die Umsetzung von IT-Risikomanagementmaßnahmen auf IT-Grundschutz-Basis verlangt.

Ebenso können kirchliche Einrichtungen unter die Vorgaben fallen, sofern sie in den erfassten Sektoren tätig sind und die anderen Voraussetzungen erfüllen (z. B. Krankenhäuser).

1.2.6 Verantwortlichkeit des Auftraggebers für Löschung oder Rückgabe von Daten beim Auftragsverarbeiter bei Vertragsende

Der Bundesgerichtshof hat mit Urteil vom 11.11.2025 (Az. VI ZR 396/24) klargestellt, dass der Verantwortliche nach Beendigung eines Auftragsverarbeitungsverhältnisses dafür sorgen muss, dass personenbezogene Daten durch den Auftragsverarbeiter auch tatsächlich gelöscht oder zurückgegeben werden, sofern keine rechtliche Grundlage für eine weitere Speicherung besteht. Im zugrunde liegenden Fall eines Datenlecks beim Auftragsverarbeiter bejahte der BGH eine Verletzung datenschutzrechtlicher Pflichten und damit einen Schadensersatzanspruch nach Art. 82 DSGVO.



„Der BGH hat [...] klargestellt, dass der Verantwortliche nach Beendigung eines Auftragsverarbeitungsverhältnisses dafür sorgen muss, dass personenbezogene Daten durch den Auftragsverarbeiter auch tatsächlich gelöscht oder zurückgegeben werden.“

¹⁸ BGBl. 2025 I Nr. 301. Zum Regelungsrahmen NIS-2 und weiteren ausgewählten IT-Sicherheit-Standards siehe auch Abschnitt 1.7.3 dieses Jahresberichts.

Dabei betont der BGH, dass das Risiko eines unbefugten Zugriffs auf die gespeicherten Daten nicht erst bei einem Cyberangriff durch außenstehende Dritte bestehe, sondern schon dann, wenn die Daten nach Beendigung des Auftragsverhältnisses beim Auftragsverarbeiter gespeichert blieben, obwohl dessen Zugriffsrecht mit der Beendigung des Auftrags erloschen sei. Dies habe der Verantwortliche durch geeignete Maßnahmen „so weit wie möglich“ zu verhindern. Die Darlegungs- und Beweislast für die Angemessenheit dieser Maßnahmen trage der Verantwortliche selbst. Er könne sich nicht dadurch entlasten, dass der Auftragsverarbeiter die Daten vertragswidrig weiter speichert oder nutzt; für die Folgen eines eigenen Pflichtverstoßes bleibe er verantwortlich.

Hinweis für kirchliche Einrichtungen

Es gilt weiterhin: Bei der Auftragsverarbeitung wird die Datenverarbeitung delegiert, nicht aber die Verantwortung. Diese bleibt beim Auftraggeber. Es ist also wichtig, sich nicht nur auf den Auftragsverarbeiter zu verlassen. Sorgfältige Auswahl, rechtssichere Vereinbarungen und ernst gemeinte Kontrollen können dafür sorgen, dass der Auftragsverarbeiter personenbezogene Daten ausschließlich im Rahmen der dokumentierten Weisungen verarbeitet.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

Im kirchlichen Bereich war im Jahr 2025 vor allem der Abschluss der Evaluierung des Gesetzes über den Kirchlichen Datenschutz von großer Bedeutung. Diese und weitere Regelungen mit direktem oder indirektem Datenschutzbezug werden in diesem Abschnitt erläutert.

1.3.1 Abschluss der Evaluierung des Gesetzes über den Kirchlichen Datenschutz

In der Sitzung vom 24.11.2025 hat die Vollversammlung des Verbandes der Diözesen Deutschlands die Novellierung des Gesetzes über den Kirchlichen Datenschutz (KDG) und der dazugehörigen Durchführungsverordnung beschlossen. Mit dem Beschluss der Vollversammlung konnte ein mehrjähriger Überarbeitungsprozess des kirchlichen Datenschutzgesetzes erfolgreich abgeschlossen werden.¹⁹

Im Berichtszeitraum erfolgte noch die Auswertung der Äußerungen und Änderungsvorschläge aus dem Beteiligungsverfahren zum Entwurf des Gesetzes. Der überarbeitete Entwurf wurde dann im Herbst von den Gremien des VDD (Verband der Diözesen Deutschlands) als Mustertext beschlossen und den (Erz-)Diözesen als Vorschlag für das novellierte Gesetz zugesandt.

¹⁹ Zur Evaluierung des KDG siehe Abschnitt 1.3.1 im Jahresbericht 2024, das Vorwort im Jahresbericht 2023, Abschnitt 1.3.3 im Jahresbericht 2022 und Abschnitt 1.3.4 im Jahresbericht 2021.

Das Gesetz in seiner geänderten Fassung wurde von den Diözesanbischöfen für ihre jeweilige (Erz-)Diözese als Gesetz erlassen. Die Neufassung des Gesetzes ist zum 01.03.2026 in den (Erz-)Diözesen in Kraft getreten.²⁰

Zeitgleich mit dem KDG wurde auch der Text der Durchführungsverordnung novelliert.²¹

1.3.2 Die Note „Antiqua et nova“ des Vatikans

Der Vatikan hat ein neues Grundsatzdokument zur künstlichen Intelligenz (KI) veröffentlicht. In seiner Note „Antiqua et nova“²² beschäftigt er sich mit der Frage, wie diese schnell wachsende Technologie das menschliche Leben verändert – und welche ethischen Maßstäbe dabei gelten sollten. Deutlich wird: Technischer Fortschritt darf nicht auf Kosten der Menschenwürde gehen.

In dem Dokument beschreibt der Vatikan KI als eine der einflussreichsten Entwicklungen unserer Zeit. Programme können heute Texte verfassen, Bilder erzeugen oder Entscheidungen vorbereiten, die früher nur Menschen treffen konnten. Diese Entwicklung habe tiefgreifende Folgen für Arbeit, Bildung, Politik und zwischenmenschliche Beziehungen. Deshalb sei ein verantwortungsvoller Umgang dringend notwendig.

Ein zentraler Gedanke der Note „Antiqua et nova“ ist die klare Unterscheidung zwischen menschlicher und künstlicher Intelligenz. Während KI große Datenmengen auswerten und Muster erkennen kann, fehlt ihr nach Auffassung des Vatikans echtes Verständnis, moralisches Urteilsvermögen und persönliche Erfahrung. Menschen seien nicht nur leistungsfähige Problemlöser, sondern fühlende, verantwortliche und soziale Wesen.

Der Vatikan warnt davor, Menschen auf messbare Daten oder Leistungswerte zu reduzieren. Die Würde des Menschen dürfe nicht davon abhängen, wie effizient oder „optimierbar“ jemand sei.

Das Dokument versteht sich nicht als Ablehnung von KI. Vielmehr betont der Vatikan, dass neue Technologien durchaus positive Beiträge leisten können – etwa in der Medizin, im Umweltschutz oder bei der Katastrophenhilfe. Gleichzeitig fordert er klare ethische Leitlinien, damit KI dem Gemeinwohl dient und nicht zu Diskriminierung, Manipulation oder Machtmissbrauch führt.

Technische Möglichkeiten allein dürften nicht bestimmen, was eingesetzt wird. Entscheidend sei, ob der Einsatz von KI dem Menschen nützt oder ihm schadet.



„Das Dokument versteht sich nicht als Ablehnung von KI. Vielmehr betont der Vatikan, dass neue Technologien durchaus positive Beiträge leisten können...“

²⁰ Veröffentlichung: Erzdiözese Paderborn KAbI. 2026 Stück 1 Nr. 16; Erzdiözese Köln ABl. 2026 Stück 3 Nr. 71; Diözese Aachen ABl. 2026 Stück 3 Nr. 135; Diözese Essen KAbI. 2026 Stück 2 Nr. 15; Diözese Münster KAbI. 2026 Stück 3 Nr. 44.

²¹ <https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2026/07/kdg-und-kdg-dvo-2026-fassung-der-dbk-vollversammlung-2025-rev-10.pdf>

²² Siehe https://www.vatican.va/roman_curia/congregations/cfaith/documents/rc_dcf_doc_20250128_antiqua-et-nova_ge.html; vgl. zur datenschutzrechtlichen Einordnung ferner Neumann, Datenschutz im Vatikan-KI-Dokument, Artikel 91 v. 29.01.2025.

Dabei äußert sich der Vatikan auch kritisch zum Umgang mit personenbezogenen Daten in diesem Zusammenhang. Digitale Informationen spiegeln das Leben, die Beziehungen und Entscheidungen von Menschen wider und müssten entsprechend geschützt werden. KI-Systeme dürften nicht dazu genutzt werden, Menschen zu überwachen, zu kontrollieren oder aufgrund von Profilen zu benachteiligen.

Zudem weist das Dokument darauf hin, dass komplexe KI-Systeme oft schwer nachvollziehbar sind. Gerade deshalb müsse klar geregelt sein, wer Verantwortung für ihre Entscheidungen trägt – insbesondere dann, wenn diese Entscheidungen konkrete Auswirkungen auf das Leben von Menschen haben.

Ein weiteres Thema ist die zunehmende Verbreitung manipulierten Materials, etwa durch täuschend echte Bilder, Videos oder Texte. Solche Inhalte könnten das Vertrauen in Medien, Wissenschaft und demokratische Prozesse untergraben. Der Vatikan sieht darin eine ernsthafte Gefahr für den gesellschaftlichen Zusammenhalt.

Zum Abschluss ruft der Vatikan dazu auf, künstliche Intelligenz mit Umsicht und Verantwortungsbewusstsein einzusetzen. Fortschritt müsse immer daran gemessen werden, ob er Freiheit, Gerechtigkeit und menschliche Würde stärkt. KI solle ein Werkzeug bleiben – und nicht zum Maßstab dafür werden, wie Menschen bewertet oder behandelt werden.

1.3.3 Novellierung des KDG-Schulen

Im Berichtszeitraum haben alle nordrhein-westfälischen (Erz-)Diözesen neue datenschutzrechtliche Bereichsregelungen für Schulen erlassen. Das Gesetz über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen (KDG-Schulen) ersetzt die überarbeitungsbedürftigen Regelungen der Anordnung über den kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen (KDO-Schulen), die sich noch auf die Vorgängerregelung des KDG bezogen. Das KDG-Schulen wurde ganz überwiegend wortgleich in allen fünf nordrhein-westfälischen (Erz-)Diözesen erlassen.²³ Das KDG-Schulen ist im Verhältnis zum KDG als Spezialgesetz zu verstehen. Es geht den Regelungen des KDG vor, insofern es dessen Standards nicht unterläuft.²⁴

Hervorzuheben ist u. a., dass die kirchlichen Gesetzgeber die Klärung der Frage der Verantwortlichkeit nach § 2 Abs. 1 KDG-Schulen per separater diözesaner Bestimmung festlegen können. Von dieser Möglichkeit haben allerdings, zum Zeitpunkt der Erstellung des Berichts, nicht alle fünf (Erz-)Diözesen Gebrauch gemacht.²⁵ Zu beachten ist hierbei, dass eine solche separate Festlegung der Verantwortlichkeit mit den tat-

²³ Siehe Amtsblätter der (Erz-)Diözesen: KABI. Paderborn 2026 Stück 5 Nr. 51; ABl. Köln 2026 Stück 9 Nr. 220; ABl. Aachen 2026 Stück 6 Nr. 73; KABI. Essen 2026 Stück 4 Nr. 39; KABI. Münster 2026 Stück 6 Nr. 125.

²⁴ Für einen anderen Überblick vgl. Neumann, Gänsweins ToMs – Wochenrückblick KW 17/2025, Artikel 91 v. 25.4.2025, Abschnitt Schuldatenschutz in Paderborn und Neumann, DSG-EKD neu macht der Mai – Wochenrückblick KW 18/2025, Artikel 91 v. 2.5.2025, Abschnitt Zentrale Verantwortlichkeit bei Essener katholischen Schulen.

²⁵ So aber z. B. das Bistum Essen, siehe KABI. 2026 Stück 4 Nr. 40.

sächlichen Verhältnissen vor Ort übereinstimmen muss. Datenschutzrechtlich verantwortlich ist die Person oder Stelle, die die Zwecke und Mittel für eine Verarbeitung festlegt. Eine gesetzliche Festlegung kann also nicht die Grundsätze der Verantwortlichkeit umgehen. Soweit sich in der Praxis entsprechende Anhaltspunkte ergeben, wird das Katholische Datenschutzzentrum die Verantwortlichkeit im Einzelfall weiterhin überprüfen.

Das KDG-Schulen enthält recht breit gefasste Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten von Schülern, Lehrern und Eltern, wobei diese grundsätzlich nicht von den Anforderungen ähnlicher Rechtsgrundlagen im KDG abweichen und den Inhalten der entsprechenden staatlichen Regelungen folgen. Das KDG-Schulen und dessen Anlagen legen dabei detailliert fest, welche personenbezogenen Daten der Schüler, Lehrer und Eltern für die Erfüllung der Aufgaben der Schulen verarbeitet werden müssen. So wird aus Sicht des Katholischen Datenschutzzentrums ein klarer und übersichtlicher Rahmen für Betroffene von Verarbeitungen geschaffen.

Betroffenenrechte werden durch das KDG-Schulen nicht eingeschränkt. Es findet sich lediglich ein Verweis auf die Betroffenenrechte im KDG.

Hinweis für kirchliche Einrichtungen

In der Praxis werden die neuen Regelungen für Verantwortliche und das Katholische Datenschutzzentrum recht wenig verändern. Die mit der ausführlichen Darstellung geschaffene Transparenz für Verarbeitungen im schulischen Kontext ist aus Sicht des Katholischen Datenschutzzentrums sehr positiv.

1.3.4 Erläuternde Note des Vatikans zum Löschen von Taufbucheinträgen

Am 17.04.2025 veröffentlichte das Dikasterium für Gesetzestexte des Heiligen Stuhls eine „Nota esplicativa“²⁶ zur Handhabung von Einträgen in Taufregistern der Pfarreien. Die erklärende Note stellt klar, dass Eintragungen im Taufregister grundsätzlich nicht geändert oder gelöscht werden dürfen, außer zur Korrektur von Übertragungsfehlern. Nach Canon 535 des Codex Iuris Canonici (CIC) muss jede Pfarrei ein eigenes Taufregister führen und verwahren. Das Taufregister dient als objektive, sakramentale Dokumentation, die den Empfang der Taufe belegt und damit die Grundlage für den Empfang weiterer Sakramente bildet (z. B. Firmung, kirchliche Eheschließung, Weihe).

Das Taufregister dokumentiert damit historische Tatsachen über sakramentale Handlungen und ist keine Mitgliederliste der Kirche. Die Eintragung belegt einen tatsächlich vollzogenen Ritus, dient der theologischen Ordnung, der rechtlichen Sicherheit und dem Schutz von Rechten der betroffenen Personen und Dritter. Eine Löschung würde die theologische, rechtliche und verwaltungsinterne Funktion des Registers beeinträchtigen.

²⁶ Siehe <https://press.vatican.va/content/salastampa/it/bollettino/pubblico/2025/04/17/0259/00486.html>; für eine weitere Einordnung der Note, vgl. Neumann, Vatikan schaltet sich in Streit um Löschen von Taufbüchern ein, Art. 91 v. 22.04.2025.

Die „Nota esplicativa“ betont, dass das Taufregister keine Aussage über den religiösen Glauben oder die Mitgliedschaft einer Person in der Kirche treffe; es beschreibe allein die Tatsache des empfangenen Sakraments. Die persönliche Freiheit eines Gläubigen, die Kirche zu verlassen, wird nach Ansicht des Vatikans durch die Unveränderbarkeit des Registers nicht eingeschränkt. Personen, die aus der Kirche austreten möchten, können ihre Absicht im Register durch den Eintrag des „actus formalis defectionis ab Ecclesia Catholica“ dokumentieren lassen. Diese ergänzende Eintragung stellt die formelle Kirchenaustrittserklärung dar, ohne den ursprünglichen Taufbucheintrag zu löschen. Diese Willensbekundung zum Kirchenaustritt kann auf Anfrage und im Rahmen einer Anhörung ergänzt werden. Der Taufbucheintrag bleibt erhalten.

Der Vatikan trägt weiter vor, dass das Taufregister zudem die Ausstellung von Bescheinigungen über den Empfang der Taufe ermögliche, wenn eine Person weitere Sakramente empfangen möchte. Die Eintragung der Taufe und – gegebenenfalls – weiterer sakramentaler Ereignisse gewährleiste die rechtsverbindliche Dokumentation gegenüber kirchlichen Stellen und Dritten, etwa im Zusammenhang mit kirchlichen Eheschließungen oder anderen Sakramenten.

Schließlich stellt die „Nota esplicativa“ klar, dass das kanonische Recht kohärent mit diesen vertretenen Prinzipien ist. So erlaubt etwa Canon 869 CIC nur die bedingte (sub conditione) Spendung der Taufe in Fällen, in denen nicht sicher feststellbar ist, ob eine Taufe bereits empfangen wurde; eine gültige Taufe kann nicht wiederholt werden.²⁷

Die Nota des Dikasteriums erläutert die kirchenrechtliche Auffassung zur Handhabung von Taufregistern. Sie stellt dar, dass das Änderungsverbot nach Auffassung des Dikasteriums bereits aus dem geltenden Kirchenrecht folgt.

1.3.5 Verarbeitung personenbezogener Daten im Zusammenhang mit den Wahlen der Kirchenvorstände und der pastoralen Gremien im Erzbistum Paderborn

Mit Veröffentlichung im Amtsblatt vom 25.06.2025 trat die „Verwaltungsverordnung über die Auftragsverarbeitung personenbezogener Daten durch das Erzbistum Paderborn im Zusammenhang mit den Wahlen der Kirchenvorstände und der pastoralen Gremien im Erzbistum Paderborn (AV-VO)“ in Kraft.²⁸

Die Verordnung regelt die Verarbeitung von personenbezogenen Daten durch das Erzbistum Paderborn im Zusammenhang mit den Wahlen der Kirchenvorstände und pastoralen Gremien. Sie bestimmt die Verfahren, Verantwortlichkeiten und Richtlinien, um Datenschutz und Datensicherheit sicherzustellen, sowie die Rechte der betroffenen Personen hinsichtlich ihrer personenbezogenen Daten während des gesamten Prozesses zu wahren. Das umfasst u. a. den Umgang mit personenbezogenen Daten von Wählern und Kandidaten, Datenschutzmaßnahmen

²⁷ <https://www.vaticannews.va/de/vatikan/news/2025-04/vatikan-streichung-aus-taufregister-nicht-moeglich-sakrament.html>

²⁸ KABL Stück 7 Nr. 79: <https://www.kirchenrecht-ebpb.de/document/9098#s00000340>

beim Versenden und Empfangen von Daten, beim Speichern und bei der digitalen Übertragung sowie Festlegungen, wer Zugriff auf die Daten hat. Zudem wird der Umgang mit Datenpannen und Datenschutzverletzungen geregelt.

Außerdem gibt die Verordnung Rahmenbedingungen für Verträge mit Dritten vor, die an der Datenverarbeitung beteiligt sind.

Die ersten beiden Anlagen zur Verordnung listen die beauftragten Verarbeitungen und die Unterauftragsverarbeitungen auf. In der dritten werden technische und organisatorische Maßnahmen für den Bereich IT und Datensicherheit benannt, z. B. in Bezug auf Zutritts-, Zugriffs- und Zugangskontrolle.

Im Jahr 2025 konnten Gläubige im Erzbistum Paderborn erstmals hybrid mit Online- oder Briefwahl abstimmen. Die bis dahin übliche Urnenwahl vor Ort entfiel. Dadurch konnten die Gläubigen orts- und zeitunabhängig wählen.²⁹

1.3.6 Bistum Aachen weist auf das Verbot von Löschungen im Taufbuch hin

Das Bistum Aachen weist in seinem kirchlichen Amtsblatt vom 01.08.2025³⁰ darauf hin, dass das Dikasterium für die Gesetzestexte in seiner „Nota esplicativa“³¹ klarstellt, dass das Kirchenrecht keinerlei Änderungen oder Löschungen im Taufregister zulässt, außer bei Korrekturen von Übertragungsfehlern. Der entsprechende Kirchenaustritt sei stattdessen in der Anmerkungsspalte des Taufbuches zu vermerken.

1.4 Weitere datenschutzrechtliche Entwicklungen im kirchlichen Bereich, insbesondere der EKD

Im Berichtszeitraum gab es weitere erwähnenswerte Entwicklungen im kirchlichen Bereich. Einige wenige werden in diesem Abschnitt hervorgehoben.

1.4.1 EKD-Datenschutzgesetz und Datenschutzaufsicht

Seit dem 01.01.2025 ist der „Beauftragte für den Datenschutz der EKD (BfD EKD)“ die Datenschutzaufsichtsbehörde für alle Landeskirchen und Diakonien in der EKD.³² Damit wurde die Entwicklung hin zu einer zentralen Datenschutzaufsicht für den Bereich aller Landeskirchen und Diakonien in der EKD abgeschlossen. Der BfD EKD hat neben seiner Hauptstelle in Hannover noch vier Außenstellen.

²⁹ <https://www.erzbistum-paderborn.de/einrichtungen-gemeinden/pastorale-raeume-gemeinden/gremienwahlen-2025/>

³⁰ KABL Nr. 8, Nr. 101: <https://kirchenrecht-bac.de/document/9129#s00000237>

³¹ Siehe hierzu Abschnitt 1.3.4 des Jahresberichts.

³² Siehe Abschnitt 1.4.1 des Jahresberichts 2024.

Gemäß dem Beschluss der Synode der EKD im November 2024 ist das überarbeitete „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD)“³³ am 01.05.2025 in Kraft getreten.³⁴

1.4.2 Anerkennungsrictlinie der EKD

Die „Richtlinie der Evangelischen Kirche in Deutschland zur Anerkennung sexualisierter Gewalt“ vom 21.03.2025³⁵ definiert einen einheitlichen Standard für Anerkennungsverfahren in evangelischer Kirche und Diakonie. Dabei werden unabhängige Kommissionen zur Umsetzung eingesetzt. Die Richtlinie ist am 01.04.2025 in Kraft getreten.³⁶

1.5 Aus der Arbeit des Europäischen Datenschutzausschusses, des EDPS und der nationalen Datenschutzaufsichten

Das kirchliche Datenschutzrecht steht im Einklang mit der DSGVO und folgt den gleichen Grundsätzen. Deshalb sind die Themen, mit denen sich der Europäische Datenschutzausschuss (EDSA), der Europäische Datenschutzbeauftragte (EDPS) und die nationalen Datenschutzaufsichten befassen, auch für kirchliche Stellen interessant und wichtig. Ihre Auslegungen sind, unter Beachtung der kirchlichen Spezifika, auf die Rechtslage nach dem KDG übertragbar und die kirchlichen Datenschutzaufsichten berücksichtigen diese Vorgaben.

Der EDSA trägt zur einheitlichen Anwendung der DSGVO bei, denn in diesem Gremium beraten sich die Datenschutzaufsichtsbehörden der Mitgliedsländer der EU und beschließen z. B. gemeinsame Vorgehensweisen und Positionen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder tauschen sich auf nationaler Ebene in der Datenschutzkonferenz (DSK) aus. Dies erfolgt ebenfalls mit dem Ziel, die einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu gewährleisten.

Auf den offiziellen Internetseiten kann die Arbeit des EDSA³⁷ und der DSK³⁸ verfolgt werden. Die kirchlichen Datenschutzaufsichten stimmen sich teilweise mit diesen ab³⁹. Aus der Vielzahl der Leitlinien, Stellungnahmen und Beschlüsse des Europäischen Datenschutzausschusses und der nationalen Datenschutzaufsichtsbehörden im Berichtsjahr werden nachfolgend einige wenige Veröffentlichungen aufgegriffen.

³³ Aktuelle Fassung des DSG-EKD: <https://www.kirchenrecht-ekd.de/document/58309>

³⁴ Zur Überarbeitung des DSG-EKD siehe Abschnitt 1.4.2 des Jahresberichts 2024.

³⁵ <https://kirchenrecht-ekd.de/document/58272>

³⁶ Zum Stand der Umsetzung und für weitere Informationen: <https://www.ekd.de/anerkennungsrictlinie-der-ekd-89097.htm>

³⁷ https://edpb.europa.eu/edpb_de

³⁸ <https://www.datenschutzkonferenz-online.de>

³⁹ Siehe hierzu Abschnitt 3.6 dieses Jahresberichts.

1.5.1 Entscheidung des EDPS über die Verwendung von MS365 durch die Europäische Kommission

Im Mai 2021 eröffnete der Europäische Datenschutzbeauftragte eine umfassende Untersuchung zur Nutzung von Microsoft 365 durch die Europäische Kommission im Rahmen des Interinstitutionellen Lizenzvertrags von 2021. Ziel war es zu prüfen, ob die Verarbeitung personenbezogener Daten durch Microsoft-Dienste mit den Vorgaben der Datenschutzverordnung für EU-Institutionen – Verordnung (EU) 2018/1725⁴⁰ vereinbar ist.

Die Verordnung (EU) 2018/1725 regelt die Verarbeitung personenbezogener Daten durch Institutionen, Organe, Ämter und Einrichtungen der EU und entspricht in vielen Grundprinzipien der DSGVO.

Am 08.03.2024 veröffentlichte der EDPS seine Entscheidung („Decision 2024-05“, Case 2021-0518), wonach die EU-Kommission mehrere datenschutzrechtliche Vorschriften verletzt habe.⁴¹

Der EDPS stellte im Kern fest:

1. Verletzung von Zweckbindungs- und Informationspflichten:
Die Kommission habe in ihren Verträgen mit Microsoft nicht hinreichend spezifiziert, welche personenbezogenen Daten von Microsoft verarbeitet werden und zu welchen Zwecken.
2. Unzureichende Schutzmaßnahmen bei Drittlandtransfers:
Die Übermittlung personenbezogener Daten an Microsoft sowie dessen Unterauftragsverarbeiter in Drittländer außerhalb der EU / des EWR ohne angemessene Schutzmaßnahmen sei nicht mit der Verordnung (EU) 2018/1725 vereinbar.
3. Mängel bei der Kontrolle des Datenverarbeitungsumfelds:
Die Kommission habe nicht ausreichend dokumentiert, welche Datenverarbeitungsprozesse sie selbst steuert und welche durch Dritte in ihrem Auftrag erfolgen.

Infolge dieser Feststellungen ordnete der EDPS verbindlich an, dass die Kommission bis zum 09.12.2024 alle Datenflüsse, die aus der Nutzung von Microsoft 365 zu Microsoft selbst, zu verbundenen Unternehmen und zu Unterauftragnehmern in Drittländern führen – sofern kein Angemessenheitsbeschluss vorliegt – aussetzen (Suspension Order) und die Verarbeitungsvorgänge so anpassen muss, dass sie mit der Verordnung (EU) 2018/1725 vollständig konform sind (Compliance Order).

Der EDPS betonte, dass diese Maßnahmen angemessen, notwendig und verhältnismäßig seien angesichts der Schwere und Dauer der Verstöße.

Unmittelbar nach der Entscheidung reichten sowohl die Europäische Kommission als auch Microsoft Ireland Operations Ltd. Klagen vor dem Gericht der Europäischen Union ein.

⁴⁰ <https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng>

⁴¹ Siehe https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en; für eine ähnliche Darstellung vgl. SVB Mülöt, M365, EDSB und Europäische Kommission: Eine Kontroverse mit weiten Folgen v. 31.07.2024.

Die Kommission beantragte mit ihrer Klage⁴² die Aufhebung der EDPS-Entscheidung und rügte dabei u. a. die angeblich fehlerhafte Auslegung und Anwendung zentraler Artikel der Verordnung (EU) 2018/1725.⁴³ Mit der parallel dazu von Microsoft Ireland eingereichten Klage⁴⁴ fordert Microsoft ebenfalls die Aufhebung der EDPS-Entscheidung bzw. einzelner Teile und rügt u. a. Rechts- und Sachfehler bei der Feststellung von Verstößen gegen die Verordnung (EU) 2018/1725, bei internationalen Datenübermittlungen und der Zweckbindung von Datenverarbeitung sowie unangemessene Korrekturmaßnahmen.⁴⁵

Nach Veröffentlichung im Amtsblatt der Europäischen Union wurden beide Klagen im Sommer 2024 formal registriert. Bis Mitte 2025 lagen jedoch keine veröffentlichten Urteile oder rechtskräftigen Beschlüsse des Gerichts vor; die Verfahren liefen weiter, parallel zur Überprüfung der Umsetzung durch die Kommission. Dort war unklar, ob das Gericht substantielle rechtliche Klärungen zu den strittigen Auslegungsfragen treffen würde.

Nach der im EDPS-Beschluss gesetzten Frist reichte die Kommission im Dezember 2024 einen umfassenden Bericht über ihre Maßnahmen zur Umsetzung der EDPS-Anordnungen ein.⁴⁶

In der Folge prüfte der EDPS den Compliance-Nachweis, führte mehrere technische und rechtliche Abstimmungen mit der Kommission durch und kam im Juli 2025 zu dem Ergebnis, dass die früher festgestellten Verstöße behoben worden seien. In einer entsprechenden Mitteilung bestätigte der EDPS, dass Zweckbindung, Datenübermittlung und Dokumentationsanforderungen nun mit den Vorgaben der Verordnung (EU) 2018/1725 in Einklang stehen und die Korrekturmaßnahmen der Kommission sowie abgestimmte technische und organisatorische Maßnahmen Microsoft-bezogener Datenverarbeitungsprozesse als wirksam angesehen werden.⁴⁷

Auf dieser Grundlage schloss der EDPS das Durchsetzungsverfahren offiziell ab.

Hinweise für kirchliche Einrichtungen

Kirchliche Einrichtungen sollten beachten, dass die letztendlich positive Bewertung des EDPS aufgrund spezieller vertraglicher und technisch-organisatorischer Vereinbarungen zwischen der EU-Kommission und Microsoft möglich war. Eine Berufung auf diese Entscheidung durch kirchliche Stellen setzt also vergleichbare Vereinbarungen mit Microsoft voraus.

⁴² EuG, Rs. T-262/24.

⁴³ <https://eur-lex.europa.eu/eli/C/2024/3925/oj/eng>

⁴⁴ EuG, Rs. T-265/24.

⁴⁵ <https://eur-lex.europa.eu/eli/C/2024/3926/oj/eng>

⁴⁶ https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-follows-compliance-european-commissions-use-microsoft-365_en

⁴⁷ https://www.edps.europa.eu/press-publications/press-news/press-releases/2025/european-commission-brings-use-microsoft-365-compliance-data-protection-rules-eu-institutions-and-bodies_de und https://www.edps.europa.eu/system/files/2025-07/2025-07-28_Press-Release_EDPS_Microsoft_EC_in_compliance_EN.pdf

1.5.2 Empfehlungen 2/2025 des EDSA für die Verpflichtung zur Einrichtung von Benutzerkonten auf E-Commerce-Websites

Die Empfehlungen 2/2025 zur Rechtsgrundlage für die verpflichtende Einrichtung von Benutzerkonten auf E-Commerce-Websites⁴⁸ des Europäischen Datenschutzausschusses befassen sich mit der Rechtsgrundlage und den damit verbundenen datenschutzrechtlichen Anforderungen für die Pflicht, dass Nutzer vor dem Zugriff auf Angebote oder dem Kauf von Waren auf E-Commerce-Websites ein Online-Nutzerkonto anlegen müssen. Dieses Dokument wurde am 03.12.2025 vom EDSA zur öffentlichen Konsultation angenommen.

Viele E-Commerce-Websites verlangen von Nutzern vor dem Kauf oder Zugriff auf Angebote, ein Online-Nutzerkonto einzurichten. Solche Konten werden üblicherweise durch Authentifizierungsmechanismen mit Benutzername und Passwort realisiert, und sie sind oft Voraussetzung für die Nutzung der Internetseite oder für den Kaufprozess.

Der EDSA hebt hervor, dass die Schaffung solcher Konten datenschutzrechtliche Auswirkungen hat, da die Nutzerkonten zusätzliche Daten über Nutzer aggregieren und längerfristig speichern können. Ziel der Empfehlungen ist es daher, klarzustellen, unter welchen Bedingungen das verpflichtende Anlegen eines Nutzerkontos datenschutzrechtlich zulässig ist.

Ein Online-Nutzerkonto wird im Dokument definiert als ein persönlicher, dauerhaft zugänglicher Online-Bereich, der durch ein Authentifizierungsverfahren (z. B. Passwort, Identifikator) geschützt ist. Temporäre Sessions oder Zugänge ohne Passwort fallen nicht unter diese Definition.

Der EDSA identifiziert mehrere wichtige Risiken, die mit verpflichtenden Nutzerkonten verbunden sind. So könne das ständige Einloggen dazu führen, dass mehr personenbezogene Daten gesammelt und verarbeitet werden, als für den Kauf oder die Nutzung der Internetseite nötig wäre. Ebenso führten Konten dazu, dass Daten über den eigentlichen Zweck (z. B. Kaufabwicklung) hinaus gespeichert blieben, was dem Grundsatz der Speicherbegrenzung widerspreche. Außerdem seien länger gespeicherte Daten in aktiven Konten potenziell stärker gefährdet für unbefugte Zugriffe oder Sicherheitsrisiken. Zuletzt könnten Konten die Verknüpfung von Nutzeraktivitäten erleichtern, wodurch weitergehende Verhaltensdaten erhoben würden.

Diese Risiken bilden den Kontext für die folgenden rechtlichen Bewertungen.

Der EDSA analysiert drei mögliche Rechtsgrundlagen, die für das verpflichtende Erstellen eines Nutzerkontos in Betracht kommen:

1) Vertragserfüllung (Art. 6 Abs. 1 lit. b) DSGVO)

Diese Rechtsgrundlage gilt nur dann, wenn die Erstellung eines Kontos objektiv notwendig ist, damit der Vertrag zwischen Nutzer und Anbieter erfüllt werden kann. Die Daten, die für einen einmaligen Kauf notwendig

⁴⁸ https://www.edpb.europa.eu/system/files/2025-12/edpb-recommendations-202502-mandatory-user-accounts_en.pdf

seien (z. B. Name, Lieferadresse), könnten häufig ohne ein Konto erhoben werden. Die Pflicht zur Kontoerstellung sei daher in solchen Fällen nicht gerechtfertigt, wenn ein „Gast-Checkout“ möglich sei. Hingegen könne ein Konto erforderlich sein, wenn es technisch notwendig sei, um regelmäßige Leistungen oder Abonnements zu verwalten. Ebenso könne beim Zugriff auf exklusive Angebote ein Konto gerechtfertigt sein, wenn der Zugang nur über eine eindeutige, authentifizierte Nutzeridentifikation erfolgen könne.

2) Gesetzliche Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO)

Der EDSA prüft, ob nationale oder EU-rechtliche Pflichten die Erstellung von Konten erzwingen könnten. Aus Sicht des EDSA sei dafür keine generelle gesetzliche Pflicht ersichtlich, die das zwingend erforderlich mache.

3) Berechtigtes Interesse (Art. 6 Abs. 1 lit. f) DSGVO)

Einige Unternehmen führen betriebliche Gründe wie Betriebs- oder Bestellverwaltung an. Der EDSA betont jedoch, dass legitime Interessen nicht ohne Weiteres die Pflicht zur Kontoerstellung rechtfertigen, wenn es weniger eingriffsintensive Alternativen gebe (z. B. Gast-Checkout).

Deutlich wird in den Empfehlungen vor allem Folgendes: Wenn kein zwingender Grund für die Erstellung eines Kontos besteht, sollte die Website den Nutzern die Wahl bieten, entweder ein Nutzerkonto zu erstellen oder als Gast fortzufahren. Diese Option ist nach Ansicht des EDSA häufig die datenschutzfreundlichere Lösung, die im Einklang mit der DSGVO steht. Verpflichtende Nutzerkonten auf E-Commerce-Websites sind nur in sehr engen und klar definierten Situationen zulässig.

1.5.3 Leitlinien für den Einsatz generativer KI

Der Europäische Datenschutzbeauftragte hat Leitlinien für den Einsatz generativer KI herausgegeben.⁴⁹ Die Leitlinien des Europäischen Datenschutzbeauftragten richten sich an die Organe, Einrichtungen, Ämter und Agenturen der EU und sollen sie beim datenschutzkonformen Einsatz generativer KI-Systeme unterstützen. Sie geben praxisnahe Orientierung zur Verarbeitung personenbezogener Daten und zur Einhaltung der Vorgaben der Verordnung (EU) 2018/1725⁵⁰, ohne konkrete technische Maßnahmen vorzuschreiben. Im Mittelpunkt stehen vielmehr die allgemeinen datenschutzrechtlichen Grundsätze, die auf eine Vielzahl von Anwendungsfällen übertragbar sind. Die überarbeitete Fassung trägt sowohl den technischen Entwicklungen im Bereich generativer KI als auch den bisherigen Aufsichts- und Kontrolltätigkeiten des EDPS Rechnung.

⁴⁹ https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf

⁵⁰ Amtsblatt der Europäischen Union, L 295/39: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1725>

1.6 Aufarbeitung des Missbrauchs

Die Aufarbeitung des Missbrauchs in der katholischen Kirche muss gelingen und vergangenes Unrecht adressieren und zukünftiges Leid verhindern. Das Katholische Datenschutzzentrum versucht hier im Rahmen seiner Aufgaben einen Beitrag zum Gelingen dieses Vorhabens zu leisten.

Der Datenschutz gibt bei der Verarbeitung personenbezogener Daten einen Rahmen vor, der zu beachten ist. Der Datenschutz ist aber kein Werkzeug, um die Arbeit der Aufklärung der verschiedenen Formen des Missbrauchs in der Kirche zu verhindern oder zu erschweren. In jedem Einzelfall sind die Möglichkeiten auszuloten, wie die Aufklärungsarbeit innerhalb des gegebenen Rahmens gelingen kann.

Datenschutz verhindert nicht die Aufklärung. Im Gespräch lassen sich für fast alle Anliegen auch praktikable Lösungen finden. Der Diözesandatenschutzbeauftragte steht für Gespräche immer zur Verfügung, wie sie vom Katholischen Datenschutzzentrum z. B. mit den fünf Unabhängigen Aufarbeitungskommissionen der nordrhein-westfälischen (Erz-) Bistümer geführt wurden.⁵¹

1.6.1 Austausch mit den fünf Unabhängigen Aufarbeitungskommissionen in den nordrhein-westfälischen (Erz-) Diözesen

Auch in den fünf nordrhein-westfälischen (Erz-)Diözesen sind Unabhängige Aufarbeitungskommissionen auf Basis der gemeinsamen Erklärung der Unabhängigen Bundesbeauftragten gegen sexuellen Missbrauch von Kindern und Jugendlichen (UBSKM) und der deutschen (Erz-)Bischöfe eingerichtet worden. Aus der Arbeit dieser Kommissionen bekam das KDSZ immer wieder Fragen vonseiten der (Erz-)Bistümer oder der Kommissionen zu datenschutzrechtlichen Fragestellungen mit. Neben der Veröffentlichung des Beschlusses der Konferenz der Diözesandatenschutzbeauftragten im November 2024 zu einzelnen Aspekten der Arbeit der diözesanen Unabhängigen Aufarbeitungskommissionen⁵² führte dies auch dazu, dass im Berichtszeitraum und im Jahr 2026 Gespräche mit den einzelnen Unabhängigen Aufarbeitungskommissionen in den nordrhein-westfälischen (Erz-)Diözesen geführt wurden. Auch ein Termin mit den fünf Vorsitzenden der Kommissionen gemeinsam mit der Landesdatenschutzbeauftragten wurde vom Diözesandatenschutzbeauftragten durchgeführt.

Ziel dieser Gespräche war es, datenschutzrechtliche Fragen, die aus Sicht der Kommissionen ihre Arbeit erschwerten, zu adressieren und einer Lösung zuzuführen.

So wurde im Rahmen der Gespräche immer wieder thematisiert, dass die fünf (Erz-)Diözesen in NRW den Zugang zu Akten mit personenbezogenen Daten für die Kommissionen sehr unterschiedlich ausgestaltet

⁵¹ Zu Gesprächen mit den fünf Unabhängigen Aufarbeitungskommissionen in den nordrhein-westfälischen (Erz-)Diözesen siehe den nachfolgenden Abschnitt 1.6.1 des Jahresberichts.

⁵² Siehe Abschnitt 4.2 des Jahresberichts 2024.

hatten, inkl. der Frage, ob der Zugang nur zu geschwärzten oder auch zu ungeschwärzten Akten gewährt wird. Die Erkenntnisse aus diesen Gesprächen haben sicherlich auch ihren Teil dazu beigetragen, dass die fünf nordrhein-westfälischen (Erz-)Diözesen die gesetzlichen Regelungen zum Zugriff der Unabhängigen Aufarbeitungskommissionen auf relevante Akten vereinheitlicht haben.⁵³

Neben dieser Frage konnten auch viele andere Themen im Rahmen der offenen und konstruktiven Gespräche angesprochen und Lösungsmöglichkeiten entwickelt werden. Außerdem konnte das Katholische Datenschutzzentrum im Zusammenhang mit diesen Gesprächen auch praktische Hilfestellungen für die Verarbeitung der Daten durch die Mitglieder der Kommissionen geben.

1.6.2 Diözesangesetze zur Regelung von Einsichts- und Auskunftsrechten

Mit dem Diözesangesetz zur Regelung von Einsichts- und Auskunftsrechten (AktAuskG) haben die (Erz-)Diözesen im Zuständigkeitsbereich des KDSZ eine weitgehend einheitliche Grundlage für den Zugang zu sensiblen Aktenbeständen, insbesondere durch die Unabhängigen Aufarbeitungskommissionen, im Kontext der Aufarbeitung sexualisierter Gewalt geschaffen.⁵⁴ Als Vorlage diente ein bereits im Jahr 2023 in Kraft getretenes Gesetz aus der Erzdiözese Paderborn. Das AktAuskG stellt ein Spezialgesetz im Verhältnis zum KDG dar. Seine Regelungen gehen denen des KDG vor, insofern sie abweichen. Dabei dürfen sie aber den Schutzstandard des KDG nicht unterlaufen.

Das Gesetz regelt, unter welchen Voraussetzungen und in welcher Form Unterlagen im Zusammenhang mit der Aufarbeitung von sexuellem Missbrauch offengelegt werden dürfen. Zur Auskunft und Einsicht werden die Unabhängigen Aufarbeitungskommissionen, wissenschaftliche Forschungsvorhaben sowie Rechtsanwaltskanzleien berechtigt. Die Regelungen gelten für die Offenlegung von Unterlagen aller kirchlichen Rechtsträger und ihrer Einrichtungen in den (Erz-)Diözesen, unabhängig von der Rechtsform. Erfasst sind insbesondere Personalakten von Klerikern und Kirchenbeamten⁵⁵ sowie Sach-, Verfahrens- und Registraturakten und vergleichbare Bestände der laufenden Schriftgutverwaltung. Hervorzuheben ist, dass die Einsicht und Auskunft in Personalakten sonstiger und nicht klerikaler Beschäftigter nicht Teil des AktAuskG ist.⁵⁶

Für die Unabhängigen Aufarbeitungskommissionen schafft § 4 AktAuskG eine eigenständige Rechtsgrundlage. Eine Offenlegung ohne Einwilligung der betroffenen Personen an die Unabhängige Aufarbeitungskommission ist zulässig, wenn sie erforderlich ist, eine Anonymisierung nicht möglich oder unverhältnismäßig wäre und das kirch-

⁵³ Siehe den nachfolgenden Abschnitt 1.6.2 des Jahresberichts.

⁵⁴ Veröffentlichung: Erzdiözese Paderborn KABl. 2023 Stück 4 Nr. 36; Erzdiözese Köln ABl. 2025 Stück 12 Nr. 284; Diözese Aachen ABl. 2025 Stück 8 Nr. 96; Diözese Essen KABl. 2025 Stück 7 Nr. 61; Diözese Münster KABl. 2025 Stück 8 Nr. 145; für eine Übersicht der Entwicklungen und des aktuellen Bestands der Einsichtsnormen vgl. Neumann, Einheitliche Aufarbeitungsnormen in NRW-Bistümern, Artikel 91 v. 06.08.2025.

⁵⁵ In allen Diözesen außer Aachen werden auch Kirchenbeamte genannt. Vgl. auch Neumann, Einheitliche Aufarbeitungsnormen in NRW-Bistümern.

⁵⁶ Hier gibt es weiterhin uneinheitliche beziehungsweise gar keine Einsichtsregelungen.

liche Interesse an der Aufarbeitung die schutzwürdigen Interessen der Betroffenen erheblich überwiegt. Forschungsvorhaben erhalten in § 5 AktAusKG und Rechtsanwaltskanzleien in § 6 AktAusKG eine Rechtsgrundlage. Zusätzlich zu den in § 4 genannten Tatbestandsvoraussetzungen muss hier eine Einwilligung des jeweiligen (Erz-)Bischofs oder einer durch ihn bestimmten verantwortlichen Person zur Offenlegung vorliegen. Nur nach dem Gesetz der Erzdiözese Köln ist außerdem eine Einwilligung der Betroffenen (von sexuellem Missbrauch) notwendig.⁵⁷ In allen Diözesengesetzen wird allerdings klargestellt, dass es dieser Einwilligung(en) nicht bedarf, sofern die Verarbeitung im Auftrag der Unabhängigen Aufarbeitungskommission erfolgt. Veröffentlichungen der so erlangten personenbezogenen Daten werden an noch engere Voraussetzungen geknüpft.

Aus Sicht des Katholischen Datenschutzzentrums ist das Gesetz vor allem deshalb bedeutsam, weil es einheitliche Regelungen für hochsensible Aktenzugriffe schafft und diese mit konkreten, prüfbaren Sicherungen verbindet. Dadurch kann Rechtssicherheit im Datenschutz für die Arbeit der Unabhängigen Aufarbeitungskommissionen erreicht werden. Das Katholische Datenschutzzentrum unterstützt sowohl die Unabhängigen Aufarbeitungskommissionen als auch Verantwortliche bei der Umsetzung der Regelungen des AktAusKG. Wünschenswert wäre darüber hinaus eine deutschlandweite Vereinheitlichung der Regelungen für die Arbeit der Unabhängigen Aufarbeitungskommissionen.

1.6.3 Verlängerte Aufbewahrungspflichten bestimmter Akten in der Kinder- und Jugendhilfe durch das UBSKM-Gesetz

Mehrfach erreichten das Katholische Datenschutzzentrum Anfragen zum Gesetz zur Stärkung der Strukturen gegen sexuelle Gewalt an Kindern und Jugendlichen (UBSKM-Gesetz)⁵⁸. Thema war ein nunmehr veränderter Umgang mit Akten von Jugendhilfeeinrichtungen.

Das Gesetz ist überwiegend am 01.07.2025 in Kraft getreten und soll den Schutz von Kindern und Jugendlichen vor sexueller Gewalt und Ausbeutung verbessern und betroffene Menschen bei der Aufarbeitung unterstützen. Zu den zentralen Bestandteilen des Gesetzes gehören die dauerhafte gesetzliche Verankerung des Amtes der Unabhängigen Bundesbeauftragten, des Betroffenenrats und der Aufarbeitungskommission.

Aus datenschutzrechtlicher Sicht erwähnenswert ist aber vor allem ein anderer Teil des Gesetzes. Mit Artikel 2 des Gesetzes wurden auch Änderungen am Achten Buch des Sozialgesetzbuches (SGB VIII) vorgenommen. In das SGB VIII wurde mit § 9b eine Norm zur Aufarbeitung eingefügt. In Absatz 1 der neuen Regelung wird für betroffene Personen ein Einsichtsrecht in die sie als Minderjährige betreffenden Erziehungshilfe-, Eingliederungshilfe-, Heim- oder Vormundschaftsakten geregelt. Dabei muss bei Vorliegen eines berechtigten Interesses Einsicht in und Auskunft über diese Akten gestattet werden. Dabei wird in

⁵⁷ Vgl. auch Neumann, Einheitliche Aufarbeitungsnormen in NRW-Bistümern.

⁵⁸ BGBl. 2025 I Nr. 107.

Absatz 3 der Vorschrift geregelt, wann ein berechtigtes Interesse vorliegt. Die zuständigen Behörden werden dort zusammen mit der Unabhängigen Aufarbeitungskommission des Bundes zur Entwicklung von Grundsätzen und Maßstäben zur Beurteilung eines berechtigten Interesses beauftragt.

Daneben sticht aber noch die Änderung der Aufbewahrungsfristen für Erziehungshilfe-, Eingliederungshilfe-, Heim- und Vormundschaftsakten heraus. Dieser Aspekt war für die anfragenden Einrichtungen maßgeblich. In § 9b Absatz 2 SGB VIII ist nunmehr eine 70-jährige Aufbewahrungsfrist ab Vollendung des 30. Lebensjahres der betroffenen Person vorgesehen. Im Regelfall sind solche Akten durch Verantwortliche bis zum 100. Geburtstag der betroffenen Person aufzubewahren.

Die Verpflichtung nach der neuen Regelung trifft die nach Landesrecht zuständigen Träger der öffentlichen Kinder- und Jugendhilfe. Die öffentlichen Träger haben aber nach Abs. 2 der neuen Regelung mit den Trägern von Einrichtungen und Diensten, die Leistungen nach SGB VIII erbringen, die Aufbewahrung, Einsicht und Auskunft dieser Akten in einer Vereinbarung zu regeln.

Hinweis für kirchliche Einrichtungen

In der Beratung der anfragenden Einrichtungen hat das Katholische Datenschutzzentrum insbesondere immer wieder auf die äußerst langen Aufbewahrungspflichten hingewiesen. Aus Sicht des KDSZ sollten alle katholischen Einrichtungen im Tätigkeitsfeld der Jugendhilfe, falls noch nicht geschehen, ihre internen Prozesse und Verarbeitungsverzeichnisse im Hinblick auf diese veränderten Aufbewahrungs- und Löschfristen überprüfen.

1.6.4 Aufarbeitung und personenbezogene Daten in Archivakten

Im Rahmen des Austausches mit den (Erz-)Diözesen und den Unabhängigen Aufarbeitungskommissionen im Zuständigkeitsbereich erreichte das KDSZ u. a. die Frage, ob die Unabhängige Aufarbeitungskommission bzw. von ihr beauftragte Forscher im Rahmen ihres Auftrages auch auf personenbezogene Archivakten zugreifen könnten, deren Schutzfrist noch nicht abgelaufen sei. Hierbei war auch das Zusammenspiel zwischen dem überarbeiteten Diözesangesetz zur Regelung von Einsichts- und Auskunftsrechten⁵⁹ und der Kirchlichen Archivordnung (KAO), im Speziellen die Abwägung der Interessen der verschiedenen Betroffenen im Rahmen von § 10 KAO, ein Thema.

Aus Sicht des Katholischen Datenschutzzentrums stellt das AktAuskG ein Spezialgesetz im Sinne des § 2 Abs. 2 KAO dar, da in § 2 AktAuskG der Vorrang der Kirchlichen Archivordnung unter den Vorbehalt einer anderweitigen Regelung im AktAuskG gestellt wird („soweit sich aus diesem Gesetz nichts Abweichendes ergibt“). Damit wäre im AktAuskG

⁵⁹ Siehe Abschnitt 1.6.2 dieses Jahresberichts.

ein ausdrücklicher Vorrang im Sinne des § 2 Abs. 2 KAO enthalten. Im Ergebnis sind damit die Vorgaben des AktAuskG auch für archivierte Akten anwendbar.

Im Rahmen der möglichen Alternativen des § 10 Abs. 1 KAO sind die schutzwürdigen Belange der Betroffenen im datenschutzrechtlichen Sinne auf unterschiedliche Weise zu berücksichtigen.

Bei der Anwendung des § 10 Abs. 1 Nr. 2 KAO muss sichergestellt werden, dass „schutzwürdige Belange Betroffener nicht beeinträchtigt werden“. Hier muss also erst einmal festgestellt werden, welche „schutzwürdigen Belange“ in diesem konkreten Fall überhaupt vorliegen. Diese Belange können je nach geplanter Nutzung der Archivbestände variieren. Nach der Auflistung der Belange muss im zweiten Schritt noch geschaut werden, ob die einzelnen Belange bei der geplanten konkreten Nutzung des Archivgutes auch wirklich schutzwürdig sind. Hier ist also eine Abwägung vorzunehmen.

Die Berufung auf § 10 Abs. 1 Nr. 3 KAO ist möglich, wenn die Nutzung des Archivgutes „im überwiegenden kirchlichen Interesse“ liegt. Hier fließen die Interessen der Betroffenen im Sinne des Datenschutzrechts in die Interessenabwägung ein, mit der für den konkreten Einzelfall festgestellt werden muss, dass die konkret geltend gemachten kirchlichen Interessen (in diesem Fall die Aufklärung des Missbrauchs) überwiegen. Hier reicht also nicht die abstrakte Berufung auf das Interesse der Kirche an der Aufklärung der Missbrauchsfälle, sondern es ist konkret darzulegen, warum dieses Interesse eventuelle entgegenstehende Interessen der Betroffenen überwiegt.

Zumindest für die eigentliche wissenschaftliche Untersuchung sollte das Interesse der Kirche an der Aufarbeitung die Interessen der Betroffenen im Regelfall überwiegen, was aber – wie ausgeführt – im konkreten Fall darzulegen wäre. Sollen die ausgewerteten personenbezogenen Daten dann auch Gegenstand einer Veröffentlichung sein und damit einem weiteren Kreis von Personen bekannt werden, so ist die Interessenabwägung für die Veröffentlichung der Daten gesondert durchzuführen. Hier dürfte – zumindest für die Betroffenen des Missbrauchs – nur schwer zu begründen sein, warum diese Personen erkennbar – also nicht anonymisiert – in einer Veröffentlichung zu der Untersuchung genannt werden müssen.

1.7 Schwerpunkt Cyberangriffe/IT-Sicherheit

Die Gefahr für eine Verletzung des Schutzes personenbezogener Daten im Rahmen eines Cyberangriffs steigt auch für kirchliche Einrichtungen seit Jahren kontinuierlich an. Angriffsmethoden und -werkzeuge werden immer ausgefeilter. Und der Schutz der Systeme und Anwendungen und damit auch der Daten ist noch nicht durchgehend auf einem guten Niveau.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt dazu in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2025 aus:



„Die Angriffsflächen in Deutschland – insbesondere Web-Angriffsflächen – zeigen dagegen nach wie vor einen besorgniserregenden Zustand. Web-Angriffsflächen müssen mehr professionelle Aufmerksamkeit durch wirksames Angriffsflächenmanagement erhalten. So werden beispielsweise viel zu oft bekannte Schwachstellen in Perimetersystemen zu spät oder gar nicht gepatcht.“⁶⁰

Die vom KDG geforderten angemessenen technischen und organisatorischen Schutzmaßnahmen sind kontinuierlich an eine sich ändernde Bedrohungslage anzupassen und müssen daher regelmäßig überprüft werden.

In den vergangenen Jahren waren – soweit bekannt geworden – mehrheitlich kirchliche Krankenhäuser das Ziel von Cyberangriffen. Dass auch andere kirchliche Stellen ein Ziel solcher Angriffe werden können, zeigte im Berichtszeitraum der Cyberangriff auf den Verband der Diözesen Deutschlands bzw. das Sekretariat der Deutschen Bischofskonferenz.⁶¹



„Die vom KDG geforderten angemessenen technischen und organisatorischen Schutzmaßnahmen sind kontinuierlich an eine sich ändernde Bedrohungslage anzupassen und müssen daher regelmäßig überprüft werden.“

1.7.1 Cyberangriff auf die IT-Systeme des Sekretariates der Deutschen Bischofskonferenz

Am 10.02.2025 wurde ein Cyberangriff auf die internen IT-Systeme des Sekretariates der Deutschen Bischofskonferenz festgestellt. Zu dem Vorfall hat sich eine Tätergruppe aus dem Bereich der organisierten Kriminalität bekannt.

Die Ermittlungsbehörden wurden ebenso wie der Leiter des Katholischen Datenschutzzentrums in seiner Funktion als Verbandsdatenschutzbeauftragter als zuständige Datenschutzaufsicht über den Cyberangriff informiert. Von Seiten des Sekretariates der Deutschen Bischofskonferenz wurden externe Forensiker mit der Untersuchung des Vorfalls beauftragt.

Der Verbandsdatenschutzbeauftragte hat versucht, durch Befragungen vor Ort und schriftliche Stellungnahmen die aus seiner Sicht wesentlichen Sachverhaltsaspekte für die Bewertung des Vorfalls zusammenzutragen und für sich zu bewerten.

In der Folge des Vorfalls gingen beim Katholischen Datenschutzzentrum auch mehrere Beschwerden zu dem Vorfall ein. Die Bewertung des Vorfalls und die Bearbeitung der Beschwerden konnten im Berichtszeitraum noch nicht abgeschlossen werden.

⁶⁰ BSI, Die Lage der IT-Sicherheit in Deutschland 2025 (Zusammenfassung), Seite 3.

⁶¹ Zum Cyberangriff auf die DBK siehe den nachfolgenden Abschnitt 1.7.1 dieses Berichts.

Hinweise für kirchliche Stellen

Auch dieser Vorfall zeigt einmal mehr, dass ein Cyberangriff jede (kirchliche) Einrichtung treffen kann. Man muss kein großes Krankenhaus oder eine andere wichtige Einrichtung sein. Ziel eines solchen Angriffs kann jede Einrichtung werden. Wichtig ist daher, dem Risiko und dem Schutzbedarf der verarbeiteten personenbezogenen Daten entsprechend adäquate technische und organisatorische Schutzmaßnahmen zu treffen und diese auch stets aktuell zu halten.

Außerdem sind für solche Angriffe – je nach Sensibilität der Daten – Szenarien im Umgang mit solchen Vorfällen zu entwickeln. Im Vorfeld ist zu klären, wie lange die Datenverarbeitung durch einen solchen Vorfall gestört werden oder sogar ausfallen darf, bevor z. B. Patienten in einem Krankenhaus geschädigt werden. Anhand dieses Zeitfensters sind im Vorfeld eines Angriffes Vorkehrungen zu treffen, die im Falle eines Falles dafür sorgen sollen, dass die Unterbrechung der Datenverarbeitung durch einen Angriff nicht über das kritische Zeitfenster hinausgeht.

Es ist daher auch für kirchliche Einrichtungen wichtig, sich vorab mit diesen Szenarien zu beschäftigen und risikoorientierte Reaktionspläne auf einen Angriff vorzuhalten und gleichzeitig zu überlegen und umzusetzen, wie in diesem Fall die Datenverarbeitung aufrechterhalten werden kann (Incident Response und Business Continuity).

1.7.2 Was ist der „Stand der Technik“?

Der Begriff „Stand der Technik“ wird nicht nur in § 26 KDG oder § 6 KDG-DVO verwendet, sondern findet sich auch sonst in vielen Rechtsbereichen und Gesetzen wieder. Da die technische Entwicklung schneller voranschreitet als Gesetze angepasst werden können, wird im Gesetz durch die Referenzierung auf den „Stand der Technik“ eine neutrale Formulierung gewählt, die deutlich macht, dass stets aktuelle Maßnahmen zu ergreifen sind, ohne konkrete technische Maßnahmen im Gesetz zu nennen, die dann immer wieder zu aktualisieren wären. Was aber ist der Stand der Technik zu einem bestimmten Zeitpunkt?

In der Kalkar-Entscheidung im Jahr 1978 nahm das Bundesverfassungsgericht anhand der drei Begriffe „Stand der Technik“, „Stand der Wissenschaft und Technik“ und „allgemein anerkannte Regeln der Technik“ eine Bewertung technischer Maßnahmen vor.⁶²

„Allgemein anerkannte Regeln der Technik“ werden in der Literatur oft verkürzt als „anerkannte Regeln der Technik“ bezeichnet. Eine technische Regel ist dann allgemein anerkannt, wenn sie die vorherrschende Ansicht der technischen Fachleute darstellt. Vorausgesetzt wird allerdings, dass sich diese Regel in der Wissenschaft als zumindest theoretisch richtig durchgesetzt hat und in der Praxis erprobt und bewährt ist. Gängige Regelwerke wie beispielsweise DIN-Normen oder VDI-Richtlinien können als Konkretisierungshilfen für die allgemein anerkannten

⁶² BVerfGE, 49, 89 (135 f.).

Regeln der Technik herangezogen werden. Maßnahmen auf Basis der allgemein anerkannten Regeln der Technik bilden also so etwas wie die notwendige Basis von Maßnahmen zur Absicherung der Verarbeitung der Daten.

Deutlich weitergehender und anspruchsvoller sind Maßnahmen, die den „Stand von Wissenschaft und Technik“ abbilden sollen. Hier werden die neuesten technischen und wissenschaftlichen Erkenntnisse behandelt. Dieser Standard wird nicht durch das gegenwärtig Realisierte und Machbare begrenzt. Durch die extreme Dynamik und Entwicklung ist es äußerst schwierig, den „Stand der Wissenschaft und Technik“ präzise zu beschreiben.

Zwischen diesen beiden Kategorien steht die Gruppe der Maßnahmen, die dem „Stand der Technik“ entsprechen. Der „Stand der Technik“ beinhaltet den Entwicklungsstand fortschrittlicher Verfahren, die zur Erreichung bestimmter praktischer Schutzzwecke als gesichert angesehen werden dürfen. Der „Stand der Technik“ gibt wieder, was technisch notwendig, geeignet, angemessen und vermeidbar ist.

Es handelt sich demnach beim „Stand der Technik“ um die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, oder kurz gesagt, um die am Markt verfügbare Bestleistung einer Maßnahme oder eines Maßnahmenbündels zur Erreichung eines gesetzlichen IT-Sicherheitszieles.⁶³

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum orientiert sich bei Bewertungen am gesetzlich geforderten „Stand der Technik“, da die „allgemein anerkannten Regeln der Technik“ allein oft unzureichende (Basis-) Anforderungen an die technischen und organisatorischen Schutzmaßnahmen abbilden. Die notwendigen technischen Maßnahmen sind für jeden Fall gesondert zu betrachten. Daher ist es auch nicht möglich, einen allgemeingültigen „Stand der Technik“ zu beschreiben.

1.7.3 Überblick zu ausgewählten IT-Sicherheit-Standards

Die Umsetzung von IT-Sicherheits-Standards ist heute ein zentraler Bestandteil moderner Informations- und Kommunikationssysteme. Mit der zunehmenden Digitalisierung von Wirtschaft, Verwaltung und Gesellschaft wuchs auch die Notwendigkeit, Daten, Netzwerke und Systeme systematisch vor Bedrohungen zu schützen. Erste strukturierte Ansätze zur Informationssicherheit entstanden bereits in den 1980er- und 1990er-Jahren. Internationale Normen und Rahmenwerke wurden entwickelt, um einheitliche Anforderungen, Prozesse und Kontrollmechanismen festzulegen.

⁶³ Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 2018, 214 (216).

Organisationen benötigen klare Leitlinien, um Risiken zu identifizieren, zu bewerten und angemessen zu behandeln. Standards schaffen dabei Vergleichbarkeit, Transparenz und Vertrauen – sowohl innerhalb von Unternehmen als auch gegenüber Kunden und Partnern.

Heute bilden IT-Sicherheits-Standards die Grundlage für ein strukturiertes Informationssicherheitsmanagement. Sie helfen, gesetzliche Anforderungen zu erfüllen, Haftungsrisiken zu minimieren und die Resilienz gegenüber Cyberbedrohungen nachhaltig zu stärken.

Betreiber kritischer Infrastrukturen und weiterer wichtiger Einrichtungen werden gesetzlich verpflichtet, IT-Sicherheit zu implementieren. Um diese auch prüfbar zu machen, werden anerkannte Standards und deren Zertifizierung als Nachweis der erfolgreichen Implementierung in Unternehmen eingesetzt. Mit der nachfolgenden Übersicht werden einige dieser Standards und der relevanten Regelungen in diesem Bereich kurz vorgestellt.

NIS-2

In Europa wurde Ende 2022 die NIS-2-Richtlinie⁶⁴ verabschiedet. Vor dem Hintergrund der steigenden Abhängigkeit von digitalen Technologien soll NIS-2 ein gemeinsames, hohes Sicherheitsniveau in Europa gewährleisten. Die Richtlinie verpflichtet Betreiber kritischer Infrastrukturen zu IT-Risikomanagement, Meldepflichten und Sicherheitsmaßnahmen. Das Gesetz zur Umsetzung der NIS-2-Richtlinie der EU in nationales Recht wurde Ende 2025 beschlossen. Durch NIS-2 wurde der Kreis der Stellen, die zur Umsetzung dort genannter Maßnahmen verpflichtet sind, erheblich erweitert.

BSIG

Das BSIG (BSI-Gesetz)⁶⁵ enthält Regelungen für das Bundesamt für Sicherheit in der Informationstechnik, legt die Anforderungen an KRITIS⁶⁶-Betreiber und weitere wichtige Einrichtungen fest. Hier wurden auch die Anforderungen der NIS-2-Richtlinie in deutsches Recht umgesetzt. Das BSI stellt in Deutschland das Meldeportal für IT-Sicherheitsvorfälle bereit, die nach NIS-2 und BSIG gemeldet werden müssen.

ISO 27001

Einer der bekanntesten Standards, um ein Informationssicherheitsmanagementsystem (ISMS) zu implementieren und zu betreiben. Die ISO 27001 spezifiziert die Anforderungen für die Implementierung von Sicherheitsmaßnahmen. Diese sind an der zu schützenden Organisation auszurichten. Die Maßnahmen aus dem Anhang A der ISO 27001 werden in der folgenden ISO 27002 genauer erläutert. Die ISO 27001 verlangt zudem ein Risikomanagement der IT-Sicherheitsrisiken. Hierzu kann z. B. die ISO 27005 herangezogen werden. Die ISO 27001 ist ein modulares Framework. Für die Umsetzung von Maßnahmen muss nicht zwingend die ISO 27002 herangezogen werden. Die Maßnahmen können auch aus dem BSI-Grundschutz entnommen werden und das Risikomanagement kann in ein bereits bestehendes Risikomanagement der Einrichtung integriert werden.

⁶⁴ Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. Siehe auch Abschnitt 1.2.6 dieses Jahresberichts zum NIS-2-Umsetzungsgesetz.

⁶⁵ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen.

⁶⁶ KRITIS (Kritische Infrastruktur) bezeichnet in Deutschland Organisationen und Einrichtungen, deren Ausfall gravierende Folgen für die Gesellschaft hätte.

BSI IT-Grundschutz

1994 wurde der erste Vorgänger des heutigen IT-Grundschutzes veröffentlicht. Er sollte Behörden und Unternehmen eine praxisnahe Anleitung zur IT-Sicherheit geben. Nach mehreren Überarbeitungen und stärkerer Orientierung an internationalen Standards – wie der ISO 27001 – besteht der IT-Grundschutz heute aus vier Standards.

- 200-1: Anforderungen an ein ISMS
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikoanalyse
- 200-4: Business Continuity Management (BCM)

Zusätzlich zu diesen vier Standards gibt es das IT-Grundschutz-Kompendium. Im IT-Grundschutz-Kompendium existieren verschiedene Bausteine, z. B. Organisation, Personal, Server, Netzwerke. In den Bausteinen werden Gefährdungen und Anforderungen definiert sowie Maßnahmen zur Implementierung genannt. Die Anforderungen gliedern sich in Basis-, Standard- und erhöhte Anforderungen, je nachdem, welcher Sicherheitsbedarf besteht.

Mit dem Grundschutz++⁶⁷ wird das BSI die nächste Entwicklungsstufe des Grundschutzes zur Verfügung stellen. Grundschutz++ ist vollständig prozessorientiert aufgebaut. Jede Anforderung wird als Regel in einem standardisierten Format erfasst und ermöglicht dadurch die Interpretation und Auswertung durch Computerprogramme.

Das Kompendium-Grundschutz++ ist mit den Sicherheitsanforderungen Teil der Stand-der-Technik-Bibliothek. Checklisten wie z. B. „Weg in die Basis-Absicherung“ haben sich bewährt und werden fester Bestandteil des Grundschutz++. Mit diesen Checklisten können auch durch kleine Organisationen grundlegende Sicherheitsanforderungen umgesetzt und kontrolliert werden, ohne ein komplettes ISMS aufzubauen und zu betreiben.

CyberFundamentals Framework (CyFun)

Das CyberFundamentals Framework⁶⁸ der belgischen Cybersicherheitsbehörde CCB⁶⁹ bietet Unternehmen eine Möglichkeit, Maßnahmen gegen die häufigsten Cyberangriffe zu implementieren. CyFun basiert auf drei Reifegraden der Cybersicherheit: Basic, Important und Essential.

Anhand einer Risikobetrachtung, die ebenfalls durch die CCB zur Verfügung gestellt wird, wird das potenzielle Risiko des Unternehmens ermittelt. Mit dem ermittelten Risiko wird die Implementierung von IT- und Cybersicherheitsmaßnahmen der bis zu drei Reifegrade in einem Selbst-Audit ermittelt. Das Ergebnis zeigt die Bereiche auf, die Verbesserungsmöglichkeiten in der implementierten IT- und Cybersicherheit haben und bietet gleichzeitig Hinweise zur Korrektur. Jeder Reifegrad

⁶⁷ Näheres zum Standard auf der Website des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Grundschutz-in-der-Informationssicherheit/Grundschutz-Plus-Plus/grundschutz-plus-plus_node.html.

⁶⁸ <https://www.cyfun.eu/de>

⁶⁹ Centre for Cybersecurity Belgium

wirkt statistisch unterschiedlichen Cyberangriffen entgegen, die in folgender Tabelle dargestellt werden.

Reifegrad/Stufe	(zusätzliche) Maßnahmen auf dieser Stufe	Cyberangriffen entgegengewirkt
Basic	34	82 %
Important	99	94 %
Essential	85	100 %

Die Stufe *Basic* umfasst die Standardmaßnahmen zur Informationssicherheit für alle Unternehmen. In der Stufe *Important* werden Risiken gezielter Cyberangriffe durch Akteure mit gängigen Fähigkeiten und Ressourcen zusätzlich zu den Maßnahmen der Stufe *Basic* behandelt. *Essential* hat zusätzlich zu den Stufen *Basic* und *Important* Maßnahmen, um Risiken fortgeschrittener Cyberangriffe durch Akteure mit umfangreichen Fähigkeiten und Ressourcen entgegenzuwirken.

Zum Einstieg in die Umsetzung strukturierter IT-Sicherheit bietet das CCB einen Katalog mit zehn Maßnahmen an, die mit wenig Aufwand ein Mindestmaß an IT-Sicherheit bringen. Alle Unterlagen und Dokumente zu CyFun werden vom CCB kostenlos zur Verfügung gestellt.

CISIS12

CISIS12 ist ein Informationssicherheitsmanagementsystem, das speziell für kleine und mittlere Unternehmen entwickelt wurde. CISIS12 steht dabei für Compliance-Informationen-Sicherheits-Management-System in 12 Schritten. In 12 Schritten wird strukturiert ein ISMS implementiert. Dabei wird ein verständlicher Ablauf gewährleistet sowie eine umfassende Betrachtung und Lösung. Viele Teilschritte können durch die Unternehmen selbst erledigt werden. Das Vorgehensmodell kann jederzeit Kataloge und Maßnahmen anderer Systeme – wie z. B. BSI IT-Grundschutz, ISO 27001 oder B3S – mit einbinden. Für die Implementierung und Nutzung von CISIS12 wird die Nutzung einer unterstützenden Software empfohlen. Die Software ist dabei das Werkzeug zum Aufbau und zur Etablierung des ISMS, das die CISIS12 Kataloge z. B. mit Schritten und Maßnahmen mitbringt. Die Dokumentation wird zentral in dieser Software abgelegt und steht dann für Audits und Bearbeitungen zur Verfügung.

B3S – Branchenspezifische Sicherheitsstandards

Die KRITIS-Betreiber oder deren Verbände können in branchenspezifischen Sicherheitsstandards konkretisieren, wie der Stand der Technik für eine bestimmte Branche erfüllt werden kann. Die Erstellung eines B3S ist für die jeweilige Branche eine Chance, die speziellen Anforderungen zu definieren und sich auch danach prüfen und zertifizieren zu lassen. Die Erstellung eines B3S ist keine gesetzliche Pflicht. Beispielsweise haben die folgenden Branchen bereits B3S erstellt: Energie, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen. Jeder B3S ist nur eine begrenzte Zeit gültig und muss dann erneut überprüft,

aktualisiert und freigegeben werden. Alle aktuell vorhandenen B3S sind auf der Webseite des BSI einsehbar.⁷⁰

Hinweis für kirchliche Einrichtungen

Alle hier betrachteten IT-Sicherheits-Standards arbeiten nach dem PDCA-Zyklus⁷¹. Damit wird eine kontinuierliche Verbesserung und Weiterentwicklung des IT-Sicherheitsstandards im Unternehmen gewährleistet. Auf welchen Standard die Wahl fällt, hängt vom Unternehmen ab. Es ist z. B. zu beachten, ob gesetzliche Vorgaben wie NIS-2 gelten oder Kunden oder die Branche einen bestimmten Standard erwarten.

IT-Sicherheitsstandards sind schon lange nichts mehr nur für große Unternehmen. Durch Angebote wie die BSI-Checklisten zum Weg in die Basisabsicherung, die Stufen Basic und Important im CyFun oder den CISIS12-Standard haben kleine Unternehmen die Möglichkeit, mit vergleichsweise wenig Aufwand strukturierte und standardisierte IT-Sicherheit zu implementieren und im Unternehmen zu leben.

1.7.4 Passwörter und Passkeys

Passwörter sind ein zentraler Bestandteil der Computersicherheit. Sie werden unter anderem verwendet, um lokale Geräte zu sichern, Netzwerke im privaten oder betrieblichen Umfeld zu schützen oder um sich in Onlinedienste einzuloggen. Auch um den Zugriff auf Daten oder vor der unbefugten Weitergabe von Daten zu schützen, kommen Passwörter zum Einsatz. Sichere Passwörter haben deshalb eine enorme Bedeutung in der heutigen vernetzten Welt.

Die Kritikalität von Passwörtern wird oftmals (immer noch) unterschätzt. Zu einfache oder mehrmals verwendete Passwörter sind anfällig für Brute-Force-Attacken und Phishing-Angriffe. Zusätzliche Sicherheit wie z. B. Multi-Faktor-Authentisierung (MFA) ist immer noch nicht weit genug verbreitet und leidet vielerorts an der Akzeptanz der Anwender. Mit Passkeys steht eine neue Authentifizierungsmethode in den Startlöchern, die das Potenzial hat, die Verwendung von Passwörtern abzulösen oder zumindest deutlich zu reduzieren.

Was gilt heute als sicheres Passwort?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Rahmenbedingungen für ein sicheres Passwort auf einer Internetseite zusammengestellt.⁷²

⁷⁰ https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Branchenspezifische-Sicherheitsstandards-B3S/Uebersicht-der-B3S/uebersicht-der-b3s_node.html

⁷¹ PDCA – Plan Do Check Act, auch bekannt als Deming-Kreis (<https://de.wikipedia.org/wiki/Demingkreis>). Es handelt sich um eine Methode im Prozessmanagement.

⁷² https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Es gibt zwei Strategien, nach denen Passwörter erstellt werden können:

- Weniger komplexe Passwörter mit mindestens 25 Zeichen. Diese Passwörter kommen mit zwei Zeichenarten aus (z. B. Groß- und Kleinbuchstaben).
- Komplexe Passwörter können mit 8-12 Zeichen auskommen, wenn vier Zeichenarten kombiniert werden (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).

Komplexe Passwörter kommen auch mit 8 Zeichen aus, wenn eine Multi-Faktor-Authentisierung verwendet wird.

Für jeden Zugang sollte ein eigenes Passwort verwendet werden. Diese können in einem Passwortmanager verwaltet werden. Passwortmanager bringen oft auch einen Passwortgenerator mit, mit dem nach bestimmten Kriterien Passwörter generiert werden können. Grundsätzlich können alle Zeichen bei der Verwendung von Passwörtern mit einbezogen werden. Besondere Zeichen aus unserer Sprache wie z. B. ü, ö, ä, ß sollten nicht verwendet werden, da nicht immer gewährleistet ist, dass alle Systeme oder Dienste diese Zeichen auch interpretieren können.

Das BSI ist vor einiger Zeit von der Empfehlung, Passwörter regelmäßig zu wechseln, auf die Empfehlung zu längeren und komplexeren Passwörtern ohne regelmäßige Wechsel übergegangen. Regelmäßige Passwortwechsel verringern über die Zeit die Sicherheit, da Anwender beim erzwungenen Passwortwechsel oft nur Abwandlungen oder Vereinfachungen des vorherigen Passwortes verwenden. Passwörter sollten nur noch gewechselt werden, wenn der Verdacht besteht, dass jemand Unbefugtes Kenntnis über das Passwort haben könnte.

Eine zusätzliche Multi-Faktor-Authentisierung ist ergänzend zum Passwort empfehlenswert. Zusätzlich zum Passwort wird z. B. durch Gesichtserkennung, Fingerabdruck, Bestätigung in einer App oder Eingabe einer generierten PIN auf einem weiteren Gerät die Anmeldung mit Benutzername und Passwort vervollständigt. MFA kann auf einem Smartphone mit einer entsprechenden App oder auch als separates Gerät ausgeführt werden.

Das BSI hat das Thema Passwortsicherheit im IT-Grundschutz integriert. Im Baustein „ORP.4 Identitäts- und Berechtigungsmanagement“⁷³ wird auf die Grundschutz-Anforderungen zu Passwörtern eingegangen.

Ein Ausblick – Passkeys

Ein Passkey ist ein kryptografisches Verfahren bestehend aus einem privaten und öffentlichen Schlüssel und wurde von der FIDO-Allianz (nichtkommerzielle IT-Sicherheitsorganisation) entwickelt. Passkeys werden ähnlich wie Multi-Faktor-Authentisierung an einem Ort, z. B. einem Smartphone, gespeichert. Der enorme Vorteil ist, dass sich keine Passwörter ausgedacht, gemerkt oder diese verwaltet werden müssen. Es gibt auch keine zu kurzen oder nicht komplex genug gewählten Passkeys, da diese auf kryptografischen Berechnungen basie-

⁷³ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Edition_2023.pdf?__blob=publicationFile&v=3

ren. Bei Anbietern, die schon Passkeys einsetzen, wird der Anwender beim Log-in gefragt, ob sich mit Benutzername und Passwort oder mit Passkeys angemeldet werden soll. Bei der Wahl von Passkeys wird der Passkey auf z. B. einem Smartphone freigegeben und der Dienstanbieter und das Smartphone tauschen im Hintergrund die benötigten Daten und Berechnungen aus und der Nutzer wird angemeldet. Große Online-Shoppinganbieter, Foren, Finanzportale oder auch Messengerdienste unterstützen bereits Passkeys. Auch zu diesem Thema hat das BSI Informationen veröffentlicht.⁷⁴

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt, die Anforderungen des BSI bei der Wahl der Passwörter oder dem Einsatz einer Passwortrichtlinie zu übernehmen. Wenn möglich, sollte die Multi-Faktor-Authentisierung verwendet werden. Sind Passkeys in Zukunft weiter verbreitet, empfiehlt es sich, die Verwendung für genutzte Dienste zu prüfen.

⁷⁴ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html



2 Aus der Tätigkeit des Datenschutzzentrums

Im Jahr 2025 gab es insgesamt einen starken Anstieg an Vorgängen im Vergleich zum Vorjahr. Wie bisher überstiegen die dem KDSZ gemeldeten Datenschutzverletzungen zahlenmäßig die anderen Vorgänge. Besonders auffällig war aber, dass sich sowohl die Anzahl der Beschwerden als auch die der Hinweise im Vergleich zu den Vorjahren mehr als verdoppelt haben. Einige Schwerpunkte und Themen werden in diesem Abschnitt dargestellt.

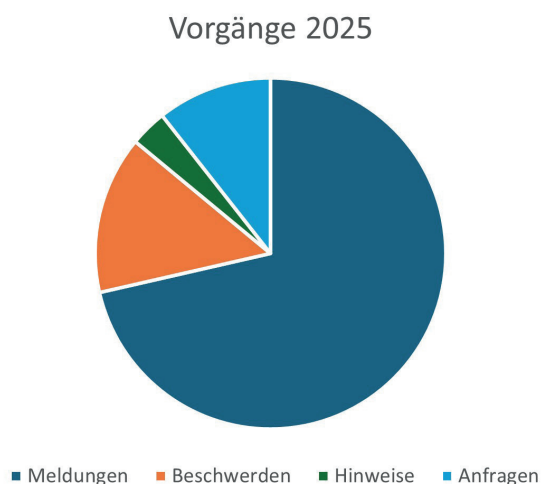


Abb. 1: Vorgänge beim Katholischen Datenschutzzentrum im Jahr 2025.

2.1 Beratungen und Anfragen

Die Beratungstätigkeit des Katholischen Datenschutzzentrums, welche die Beratung durch die betrieblichen Datenschutzbeauftragten in den Einrichtungen selbst ergänzt, blieb im Jahr 2025 weiterhin auf einem hohen Niveau. Viele Einrichtungen nutzten die Möglichkeit, sich an die Aufsicht zu wenden und datenschutzrechtliche Fragen zu klären, bevor es zu möglichen Datenschutzverstößen kommen kann.

Bekannte, aber auch neue Fragestellungen wurden dabei an das Katholische Datenschutzzentrum herangetragen. So wurde z. B. gefragt, ob ein Fotografierverbot in der Kirche zu überwachen oder wie die Information nach § 15 KDG nachzuweisen sei. In diesem Abschnitt werden diese und weitere Beratungsschwerpunkte dargelegt.

2.1.1 Datenschutz in der Flüchtlingsarbeit

Eine im Jahr 2025 an das KDSZ gerichtete Anfrage bezog sich auf den Austausch von personenbezogenen Daten von Flüchtlingen zwischen kommunalen Einrichtungen in der Flüchtlingshilfe und kirchlichen Flüchtlingsinitiativen. Für eine koordinierte Zusammenarbeit von

Kommunen und kirchlichen Flüchtlingsinitiativen zur Integration von Geflüchteten brauche es entsprechende Informationen über ankommende Flüchtlinge. Nur wenn eine Kommune die Flüchtlingsinitiative über das Ankommen von Flüchtlingen informiere, könnten Ehrenamtliche entsprechend aktiv werden.

Zunächst ist darauf hinzuweisen, dass das Katholische Datenschutzzentrum die Frage nicht abschließend beantworten konnte, da die Beurteilung, ob und wie eine Kommunal- oder Landesbehörde personenbezogene Daten weitergeben/offenlegen darf, nicht in den Zuständigkeitsbereich des Katholischen Datenschutzzentrums, sondern in den der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW fällt.

Allgemein könnte aber festgehalten werden, dass Sozialämter zum Zwecke der gesetzlichen Aufgabenerledigung personenbezogene Daten an Dritte, wie Sozialleistungsträger, übermitteln dürfen. Rechtsgrundlagen für diese Verarbeitungen finden sich beispielsweise in den Sozialgesetzbüchern (SGB). Ohne eine Rechtsgrundlage darf/kann das Sozialamt die personenbezogenen Daten der Flüchtlinge nicht weitergeben. Im Fall der kirchlichen Flüchtlingsinitiative dürfte als Rechtsgrundlage nur eine Einwilligung der betroffenen Person infrage kommen. Das Sozialamt der Stadt könnte z. B. auf das Angebot der Flüchtlingsinitiative hinweisen und auf Wunsch (Einwilligung) der betroffenen Person die personenbezogenen Daten zu einer Kontaktaufnahme weitergeben. Dieses Vorgehen ist in anderen Sozialhilfebereichen zwischen kommunalen und kirchlichen Einrichtungen üblich.

2.1.2 Einwilligung und leichte Sprache

Beratungsanfragen zur Ausgestaltung von Einwilligungserklärungen erreichen das Katholische Datenschutzzentrum recht häufig, wobei sich die Fragestellungen meist um den genauen Wortlaut der Erklärungen drehen. Selten geht es dabei aber um die eigentliche Verständlichkeit des Textes. Im Berichtszeitraum erreichte das KDSZ eine Anfrage, ob Einwilligungstexte in „Leichter Sprache“⁷⁵ zur Verfügung gestellt werden müssen, wenn Personen des Adressatenkreises überwiegend ein niedriges Sprach- und Wortverständnis aufweisen.

Zwar müssen schriftliche Einwilligungen nach § 8 Abs. 2 S. 2 KDG⁷⁶ in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfasst werden. Das bedeutet konkret, dass auch Leser mit einem niedrigen bis durchschnittlichen Leseverständnis die Erläuterungen verstehen müssen.⁷⁷ Die „einfache Sprache“ i. S. d. Norm erfordert aber keine Formulierung in Leichter Sprache. Die Formulierungen des Textes sind lediglich so auszuwählen, dass möglichst wenige Fachbegriffe und hauptsächlich einfache Satzstrukturen enthalten sind.



„... schriftliche Einwilligungen nach § 8 Abs. 2 S. 2 KDG [müssen] in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfasst werden ...“

⁷⁵ Gemeint ist die nach DIN SPEC 33429 speziell geregelte, sprachlich und inhaltlich vereinfachte Sprache. Siehe z. B. <https://www.netzwerk-leichte-sprache.de>.

⁷⁶ Bisherige Rechtslage bis 01.03.2026. Im novellierten Gesetz ist die Regelung in § 8 Abs. 3 KDG zu finden.

⁷⁷ In der Literatur zu Art. 7 Abs. 2 S. 1 DSGVO wird beides vertreten. Vgl. z. B. Heckmann/Paschke in Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl. 2024, DS-GVO Art. 7 Rn. 86.

Hinweis für kirchliche Einrichtungen

Grundsätzlich begrüßt es das Katholische Datenschutzzentrum, wenn Verantwortliche den betroffenen Personen die Informationen über Verarbeitungen möglichst zielgruppengerecht und verständlich anbieten. Dazu kann natürlich auch die Bereitstellung von Informationen in anderen Sprachen zählen.

2.1.3 Nachweis der Informationserteilung nach § 15 KDG

Das Katholische Datenschutzzentrum erreichte eine Anfrage, inwiefern die Information der von der Datenerhebung betroffenen Person nach § 15 KDG nachzuweisen ist.

Nach § 15 KDG ist der Verantwortliche verpflichtet, der betroffenen Person ohne besondere Aufforderung bestimmte Informationen über die Verarbeitung ihrer personenbezogenen Daten zur Verfügung zu stellen. Damit soll sichergestellt werden, dass die notwendige Transparenz gegenüber der betroffenen Person geschaffen wird. Es handelt sich um eine einseitige Informationspflicht des Verantwortlichen. Für die Erfüllung dieser Pflicht kommt es nicht darauf an, ob die betroffene Person die Informationen bestätigt, akzeptiert oder zur Kenntnis nimmt.

Die Modalitäten der Erfüllung dieser Informationspflicht sind in § 14 KDG geregelt. Es gibt keine gesetzliche Vorgabe für den Verantwortlichen, sich das Zurverfügungstellen oder die Kenntnisnahme der Information – überhaupt oder in einer bestimmten Form – von der betroffenen Person bestätigen zu lassen.

Allerdings hat der Verantwortliche nach § 7 Abs. 2 KDG auch die Pflicht, die Einhaltung der Grundsätze für die Verarbeitung nach § 7 Abs. 1 KDG und der damit einhergehenden Erfüllung seiner Pflichten – wie die Informationspflicht nach § 15 KDG – nachweisen zu können. Ein solcher Nachweis wird sich zwar grundsätzlich auch mit einer schriftlichen Bestätigung führen lassen, dass die Information nach § 15 KDG zur Verfügung gestellt wurde. Allerdings ist insofern zu beachten, dass die betroffene Person datenschutzrechtlich nicht verpflichtet ist, das Zurverfügungstellen oder die Kenntnisnahme der Information in irgendeiner Form zu bestätigen.

Hinweis für kirchliche Einrichtungen

Die Erfüllung der Informationspflicht kann indes auch auf andere Art und Weise nachgewiesen werden – je nach Sachverhalt. Bei einem Vertragsschluss kann sich z. B. Folgendes anbieten: Aufnahme eines expliziten Hinweises auf die Information nach § 15 KDG in das Anschreiben zu den Vertragsunterlagen mit den Informationen zur Datenverarbeitung, konkrete Handlungs-/Arbeits-/Dienstanweisung an die Beschäftigten zur Durchführung der Informationserteilung sowie deren Dokumentation (Kopie der gesamten Unterlagen einschließlich des Anschreibens), Dokumentation dieses Prozesses und regelmäßige Überprüfung.

2.1.4 Datenschutzrechtliche Verantwortlichkeit in den Beratungsstellen

Die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung von personenbezogenen Daten in den Beratungsstellen einer (Erz-)Diözese war Kern einer Anfrage an das KDSZ. Dort wird ein zentrales Klientenmanagementprogramm im Rahmen der Beratung für Ehe-, Familien- und Lebensfragen eingesetzt. Das Programm wird von den Beratungsstellen zur Erfassung personenbezogener Daten verwendet und von der (Erz-)Diözese für die Erfassung und statistische Auswertung zur Verfügung gestellt. Für die Organisation und Verwaltungsführung der Beratungsstellen sind jeweils die Gemeindeverbände rechtlich verantwortlich. Die Gemeindeverbände stellen jeweils sicher, dass die für die Errichtung und den Betrieb der Beratungsstelle erforderlichen Mitarbeitenden und finanziellen Mittel zur Verfügung stehen.

Die Frage der datenschutzrechtlichen Verantwortlichkeit ist bei mehreren an einer Verarbeitung beteiligten bzw. involvierten Stellen häufig nicht einfach zu beantworten. Sind mehrere Stellen in eine Verarbeitung involviert, sind auch kombinierte Beteiligungsmöglichkeiten denkbar. Anknüpfungspunkt dafür ist der konkrete Vorgang bzw. die konkrete Vorgangsreihe einer Verarbeitung.

Datenschutzrechtlich Verantwortlicher ist nach § 4 Nr. 9 KDG die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Es kommt darauf an, wer von den beteiligten Stellen das „Ob“ und das „Wie“ der Verarbeitung beeinflusst und steuert, in welchem Umfang und wie detailgenau Instruktionen erteilt werden und Kontrolle über die Verarbeitung ausgeübt wird bzw. die Stelle hierzu jeweils in der Lage ist.

Legen zwei oder mehr Verantwortliche i. S. d. § 4 Nr. 9 KDG gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, sind es nach § 28 Abs. 1 Satz 1 KDG gemeinsam Verantwortliche. Der Umstand, dass mehrere Verantwortliche in Bezug auf eine oder mehrere Vorgänge, Vorgangsreihen oder Phasen von Verarbeitungen involviert sind und dabei zusammenarbeiten, mitwirken oder personenbezogene Daten austauschen, begründet als solcher noch keine gemeinsame Verantwortlichkeit i. S. d. § 28 Abs. 1 Satz 1 KDG. Es bedarf einer gemeinsamen Festlegung bzw. Entscheidung hinsichtlich der Zwecke und Mittel, wobei hier jeweils eine weite Auslegung angezeigt ist. Es ist weder eine Absprache noch eine explizite Vereinbarung erforderlich. Es bedarf auch keiner gleichmäßig verteilten Entscheidungsgewalt bzw. Einflussmöglichkeit. Vielmehr kann bereits ein relativ geringer Grad an Mitwirkung und Einflussnahme aufgrund entsprechender Beiträge der beteiligten Stellen ausreichen. Das ist im Wege einer Gesamtschau unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen.

Der Gegenstand der datenschutzrechtlichen Verantwortlichkeit und zugleich Anknüpfungspunkt dafür ist der konkrete Vorgang bzw. die konkrete Vorgangsreihe einer Verarbeitung, für die entsprechende Entscheidungsgewalt vorliegen muss.

Die Frage der datenschutzrechtlichen Verantwortlichkeit kann nur im konkreten Einzelfall unter Berücksichtigung aller Umstände beantwortet werden, was Aufgabe des etwaig Verantwortlichen bzw. der beteiligten Stellen ist. Die in der Anfrage an das Katholische Datenschutzzentrum geschilderte Konstellation konnte anhand der vorliegenden Informationen nicht abschließend beurteilt werden, aber es sind folgende Möglichkeiten denkbar.

1. Es ist möglich, dass die Gemeindeverbände jeweils Verantwortliche i. S. d. § 4 Nr. 9 KDG sind und im Verhältnis zur (Erz-)Diözese eine Auftragsverarbeitung nach § 29 KDG vorliegt. Das wäre der Fall, wenn die (Erz-)Diözese weder Zweck noch Mittel der Verarbeitung festlegt und kein Eigeninteresse an der Verarbeitung hat, sondern lediglich die Anwendung sowie das Hosting zur Verfügung stellt. Die Gemeindeverbände bzw. die Beratungsstellen verarbeiten die Daten im Rahmen der Beratung jedenfalls zu eigenen Zwecken. Es kommt nicht darauf an, ob die Daten lokal gespeichert werden. Bei einer Auftragsverarbeitung gelten die Vorgaben nach § 29 KDG. Es müsste also u. a. zwischen der (Erz-)Diözese und den Gemeindeverbänden jeweils eine Vereinbarung nach § 29 Abs. 3 KDG geschlossen werden.
2. Es ist ebenso möglich, dass eine gemeinsame Verantwortlichkeit der (Erz-)Diözese und des jeweiligen Gemeindeverbands nach § 28 Abs. 1 Satz 1 KDG besteht. Das wäre beispielsweise der Fall, wenn die (Erz-)Diözese auf die personenbezogenen Daten im Klientenmanagementprogramm zugreift, um für sich statistische Auswertungen durchzuführen. Bei einer gemeinsamen Verantwortlichkeit gelten die Vorgaben von § 28 KDG. Hierzu zählt insbesondere die Pflicht der gemeinsam Verantwortlichen, eine Vereinbarung nach § 28 Abs. 1 Satz 2 und Abs. 2 Satz 1 KDG zu schließen und die Informationspflicht nach § 28 Abs. 2 Satz 2 KDG.
3. Allerdings liegt eine gemeinsame Verantwortlichkeit nur soweit vor, wie die gemeinsame Festlegung der Zwecke und Mittel der Verarbeitung reicht. Die gemeinsame Verantwortlichkeit erstreckt sich nicht auf vor- und nachgelagerte Vorgänge bzw. Phasen der Verarbeitung, wie sie z. B. für die jeweilige Fallbearbeitung durch die Beratungsstellen wohl vorliegt. Für diese Vorgänge bliebe es bei einer jeweils eigenen Verantwortlichkeit der Gemeindeverbände und einer Auftragsverarbeitung durch die (Erz-)Diözese.

Hinweis für kirchliche Einrichtungen

Vor diesem Hintergrund empfahl das Katholische Datenschutzzentrum, die relevanten Verarbeitungsprozesse daraufhin zu prüfen, welche Zwecke im Einzelnen von den Beteiligten jeweils verfolgt werden und welche Daten hierzu jeweils verarbeitet werden. In einem zweiten Schritt ist zu prüfen, welche der oben erwähnten Vereinbarungen zur gemeinsamen Verantwortlichkeit und Auftragsverarbeitung noch geschlossen werden müssen. Zudem gilt es – je nach Einschlägigkeit – die weiteren Vorgaben von § 28 und 29 KDG zu beachten und umzusetzen.

2.1.5 Aufbewahrungsdauer der Dokumentation zu Datenschutzverletzungen

Dem Katholischen Datenschutzzentrum wurde eine Fragestellung bzgl. der Aufbewahrungsdauer der Dokumentation zu Datenschutzverletzungen vorgelegt.

§ 33 Abs. 5 KDG regelt die Verpflichtung des Verantwortlichen, eine Datenschutzverletzung zu dokumentieren, eine konkrete Aufbewahrungsdauer für die Dokumentation von Datenschutzverletzungen wird dabei nicht genannt. Wichtig hierbei ist, dass auch Datenschutzverletzungen zu dokumentieren sind, bei denen der Verantwortliche nach seiner Risikoeinschätzung ein Risiko verneint hat und daher keine Meldung an die Datenschutzaufsicht erfolgt ist.

Aus Sicht des Katholischen Datenschutzzentrums sollte die Dokumentation so lange aufbewahrt werden, wie sie für den Nachweis gegenüber der Aufsicht und für die Verteidigung gegen eventuelle Rechtsansprüche benötigt wird. Der Verantwortliche hat eine angemessene Frist festzusetzen. Die allgemeinen Verjährungsfristen oder die Fristen nach OWiG können eine Orientierungshilfe geben.

2.1.6 Fotos demenziell erkrankter Personen im Krankenhausinformationssystem

Im Berichtszeitraum erhielt das Katholische Datenschutzzentrum eine Anfrage eines katholischen Krankenhauses, welches regelmäßig demenziell erkrankte Patienten mit sog. Weglauftendenzen behandelt. Bei dieser Erkrankung ist es nicht unüblich, dass Menschen, die das Haus verlassen, orientierungslos werden und nicht mehr den Weg zurück ins Krankenhaus finden. So kam es in der Vergangenheit bereits mehrfach zu Polizeieinsätzen, bei denen demenziell erkrankte Personen gesucht wurden. Um künftig die Polizei bei der Suche der vermissten Patienten besser unterstützen zu können, plant das Krankenhaus nun, Fotos von demenziell erkrankten Personen im Krankenhausinformationssystem zu hinterlegen. Der betriebliche Datenschutzbeauftragte fragte an, ob so eine Speicherung von Fotos der Patienten gemäß § 11 Abs. 2 lit. h) KDG zulässig sei und somit auf eine Einwilligung der gesetzlichen Betreuenden verzichtet werden könne.

Nach der Einschätzung des Katholischen Datenschutzzentrums ist der Ausnahmetatbestand des § 11 Abs. 2 lit. h) KDG in diesem Fall nicht einschlägig. Es kommt lediglich die Möglichkeit einer Einwilligung durch den Betroffenen selbst bei Vorlage der nötigen Einsichtsfähigkeit oder seines Betreuers in Betracht. Dabei ist besonderer Wert auf die umfassende und genaue Information des Betroffenen zu legen.

In dem Zusammenhang wurde das Krankenhaus insbesondere an die Informationspflichten der §§ 14, 15 KDG und die Voraussetzungen für eine wirksame Einwilligung erinnert. Ferner ist innerorganisatorisch sicherzustellen, dass die angefertigten Fotos ausschließlich für den Zweck der Suche von abgängigen Personen eingesetzt werden. Außerdem wurde auf eine angemessene Speicherfrist bezogen auf die Speicherung der Fotos im Krankenhausinformationssystem (KIS) hingewie-

sen. Sobald die entsprechenden Patienten das Krankenhaus verlassen oder eine Weglauftendenz aus anderen Gründen nicht mehr besteht, sind die Fotos zu löschen.

2.1.7 Auskunftsanspruch getrenntlebender Eltern mit gemeinsamem Sorgerecht

Häufig erreichen das Katholische Datenschutzzentrum Anfragen und Beschwerden zur Ausübung des Auskunftsanspruchs Minderjähriger durch getrenntlebende Eltern. In der Praxis besteht dabei oft Unsicherheit, ob und unter welchen Voraussetzungen einem einzelnen Elternteil Auskunft erteilt werden darf, oder ob zwingend beide Eltern beteiligt werden müssen.

Damit Verantwortliche weder unberechtigt Daten offenlegen noch berechnigte Anträge unnötig verzögern, kommt es auf eine saubere Prüfung der Vertretungsbefugnis an.

Grundsätzlich können Betroffenenrechte, insbesondere auch das Recht auf Auskunft nach § 17 KDG, für minderjährige Kinder durch die Eltern geltend gemacht werden. Eltern handeln dabei nicht „als Dritte“, sondern regelmäßig als gesetzliche Vertreter ihres Kindes (vgl. §§ 1626 ff., 1629 BGB).⁷⁸ Eine Vollmacht ist bei gesetzlicher Vertretung nicht erforderlich.⁷⁹ Aber auch in Fällen der gesetzlichen Vertretung bleibt die Pflicht, Identität und Vertretungsbefugnis in angemessenem Umfang zu verifizieren, etwa anhand vorhandener Aktenangaben oder geeigneter Nachweise, wenn die Umstände unklar sind.

Leben Eltern nicht dauerhaft getrennt, üben sie das Sorgerecht, zumindest nach gesetzlicher Fiktion, stets einvernehmlich und gemeinsam aus. Solange keine Anhaltspunkte für eine Meinungsverschiedenheit bestehen, ist ein Antrag von nur einem Elternteil daher wirksam.

Anders liegt es bei Eltern, die dauerhaft getrennt leben und gemeinsam sorgeberechtigt sind. Nach § 1687 BGB⁸⁰ hat der Elternteil, bei dem sich das Kind gewöhnlich aufhält, zwar Entscheidungsbefugnisse in Angelegenheiten des täglichen Lebens, Angelegenheiten von erheblicher Bedeutung sind jedoch grundsätzlich im Einvernehmen zu regeln. Auskunftersuchen und die Ausübung weiterer Betroffenenrechte sind regelmäßig als Angelegenheiten von erheblicher Bedeutung einzuordnen, weil sie typischerweise einen umfassenden Einblick in personenbezogene Daten des Kindes ermöglichen und damit erhebliche Auswirkungen auf das Kind, den anderen Elternteil und die weitere



„Auskunftersuchen und die Ausübung weiterer Betroffenenrechte sind regelmäßig als Angelegenheiten von erheblicher Bedeutung einzuordnen ...“

⁷⁸ Minderjährige können bei vorhandener Reife ihre Betroffenenrechte auch selbst ausüben.

⁷⁹ In anderen Konstellationen, in denen keine gesetzliche Vertretung vorliegt, obliegt es Verantwortlichen zu ermitteln, ob eine Vollmacht zur Ausübung des Rechts vorliegt. Das geschieht häufig bei der Vertretung von Angehörigen im medizinischen Kontext beispielsweise durch die Vorlage von entsprechenden Vollmachten und Entbindungen von der ärztlichen Schweigepflicht.

⁸⁰ § 1687 Absatz 1 BGB (Auszug): Leben Eltern, denen die elterliche Sorge gemeinsam zusteht, nicht nur vorübergehend getrennt, so ist bei Entscheidungen in Angelegenheiten, deren Regelung für das Kind von erheblicher Bedeutung ist, ihr gegenseitiges Einvernehmen erforderlich. Der Elternteil, bei dem sich das Kind mit Einwilligung des anderen Elternteils oder auf Grund einer gerichtlichen Entscheidung gewöhnlich aufhält, hat die Befugnis zur alleinigen Entscheidung in Angelegenheiten des täglichen Lebens. Entscheidungen in Angelegenheiten des täglichen Lebens sind in der Regel solche, die häufig vorkommen und die keine schwer abzuändernden Auswirkungen auf die Entwicklung des Kindes haben.

Betreuungssituation haben können. In diesen Fällen sollte eine Auskunft daher grundsätzlich nur erteilt werden, wenn der Antrag von beiden Eltern gestellt wird oder der antragstellende Elternteil die Zustimmung beziehungsweise nachträgliche Genehmigung des anderen sorgeberechtigten Elternteils nachweist. Liegt ein Widerspruch des anderen Elternteils vor oder ist ein Konflikt erkennbar, ist eine Auskunftserteilung an nur einen Elternteil regelmäßig nicht angezeigt, solange die Berechtigung nicht geklärt ist, etwa durch eine übereinstimmende Erklärung beider Eltern oder eine familiengerichtliche Entscheidung zur Vertretung.⁸¹

Hinweis für kirchliche Einrichtungen

Das Gesetz erwartet im Ergebnis von Verantwortlichen eine sehr genaue Prüfung von Berechtigungen antragstellender Personen (Eltern). Zunächst ist die Identität der antragstellenden Person festzustellen und die Elternstellung beziehungsweise Sorgerechtsanhand der vorhandenen Unterlagen zu plausibilisieren. Ist bekannt, dass die Eltern nicht dauerhaft getrennt leben und keine Anhaltspunkte für Uneinigkeit bestehen, kann der Antrag eines Elternteils bearbeitet werden. Bestehen hingegen Anzeichen für dauerhaftes Getrenntleben bei gemeinsamer Sorge oder ist die Sorgerechtslage unklar, sollten Verantwortliche geeignete Nachweise anfordern und die Auskunft von einer gemeinsamen Antragstellung oder einer dokumentierten Zustimmung des anderen Elternteils abhängig machen.

Das Katholische Datenschutzzentrum empfiehlt insbesondere Verantwortlichen, die häufig mit solchen Anträgen befasst sind (Kindertages-, Jugendhilfe- und Sozialeinrichtungen), die Sorgerechts- und Kontaktsituation bereits bei Aufnahme oder Beginn der Betreuung möglichst verlässlich zu erfassen und aktuell zu halten. So lässt sich im Einzelfall schneller entscheiden, ob ein Auskunftersuchen eines einzelnen Elternteils ausreicht oder ob wegen dauerhaft getrenntlebender Eltern mit gemeinsamer Sorge die Mitwirkung beider Elternteile einzuholen ist.

2.2 Meldungen von Datenschutzverletzungen

Die Meldung einer Datenschutzverletzung an die Datenschutzaufsicht hat nach § 33 KDG unverzüglich durch den Verantwortlichen zu erfolgen, wenn ein Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt oder vorliegen könnte. Das Gesetz nennt weiterhin Einzelheiten zu den notwendigen Informationen, die die Meldung beinhalten muss und dazu, wie diese zu dokumentieren sind. Das Katholische Datenschutzzentrum empfiehlt, für diese Meldungen das Online-Formular auf der Homepage⁸² zu verwenden. So ist sichergestellt, dass alle relevanten Informationen gemeldet und Nachfragen vermieden werden.

⁸¹ Die hier aufgestellten Leitlinien lassen sich kompakter auch in einem Praxistipp des LfDI-RLP finden, der hier abrufbar ist: https://www.datenschutz.rlp.de/fileadmin/datenschutz/Dokumente/Publikationen/Praxistipp_03_Auskunftsanspruch-Minderjaehrige.pdf

⁸² <https://www.katholisches-datenschutzzentrum.de/meldungen/meldung-dsv/>

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 im Berichtsjahr gemeldete Zahl der Datenschutzverletzungen ist weiterhin hoch und im Vergleich zum Vorjahr noch gestiegen. Die gemeldeten Datenschutzvorfälle behandeln oft wiederkehrende Thematiken, eine grobe Einteilung verdeutlicht die folgende Grafik.

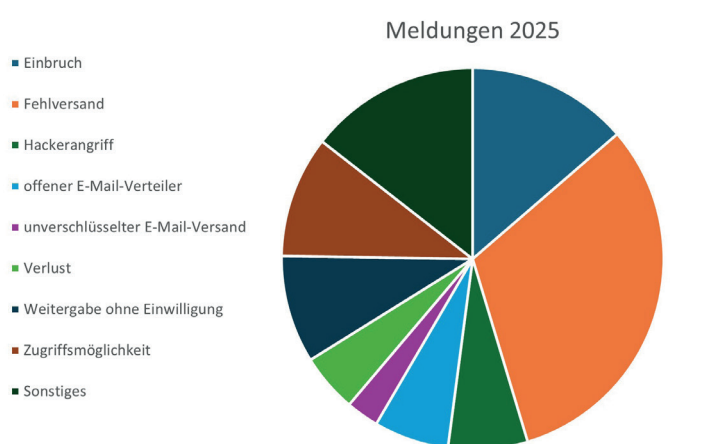


Abb. 2: Meldungen an das Katholische Datenschutzzentrum im Jahr 2025.

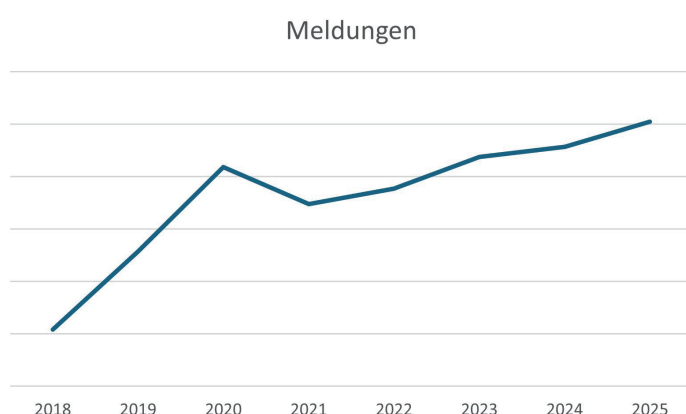


Abb. 3: Meldungen an das KDSZ im Verlauf der Jahre 2018 bis 2025.

In diesem Abschnitt werden aus den Meldungen im Berichtszeitraum einige Themen aufgegriffen, über die das Katholische Datenschutzzentrum in den vorherigen Jahresberichten noch nicht berichtet hat. Hierzu gehören z. B. ein auf Social Media veröffentlichtes Foto, auf dem im Hintergrund ein Monitor mit Patientendaten zu sehen war und ein Papier mit personenbezogenen Daten, welches als Malblatt verwendet worden ist.

2.2.1 Falscher Name in E-Mail einer medizinischen Studie

Die Erinnerung an die Teilnahme an einer medizinischen Studie wurde an eine falsche E-Mail-Adresse versandt. In dieser Erinnerung wurde der Name der betroffenen Person („Sehr geehrte(r) XY“), das Thema der medizinischen Studie und der Absender (spezifische Fachrichtung) erwähnt. Die falsche E-Mail-Adresse gehört einem anderen Studienteilnehmer, welcher auf den Fehlversand hinwies.

Zwar wurden in der E-Mail nicht direkt Gesundheitsdaten verarbeitet, aber die genannten Daten waren aus dem Kontext heraus als Gesundheitsdaten zu werten, weshalb von einem Risiko für die Rechte der betroffenen Person auszugehen war.

Hinweis für kirchliche Einrichtungen

Das vorliegende Fallbeispiel verdeutlicht, wie die alleinige Nennung eines (falschen) Namens im Kontext mit anderen Daten dazu führen kann, dass sensible Daten an Unbefugte preisgegeben werden.

2.2.2 E-Mail für die Mitarbeitervertretung an den falschen Verteiler gesendet

Dem Katholischen Datenschutzzentrum wurde gemeldet, dass eine E-Mail zwecks Zustimmung zu Änderungen des Beschäftigungsumfangs eines Mitarbeitenden (MA) an die Mitarbeitervertretung (MAV) verfasst worden ist. Darin wurde u. a. erwähnt, dass aufgrund der Erkrankung von MA A der Beschäftigungsumfang von MA B geändert werde. Außerdem werde der Beschäftigungsumfang von MA A gesenkt und MA A gehe nicht vorzeitig in Rente. Versehentlich wurde diese E-Mail nicht an den Verteiler der MAV, sondern an alle Mitarbeitenden gesendet.

In der Meldung wurde weiterhin angegeben, dass die Tatsache, dass MA A erkrankt ist (Kuraufenthalt), allgemein bekannt sei und die Änderungen der Beschäftigungsumfänge im Rahmen der Vertretungsregelung auch bekannt geworden wären, daher würden den Mitarbeitenden keine negativen Folgen drohen. Auch sei eine Information der betroffenen Personen nicht nötig. Diese seien schon dadurch informiert, da sie in dem Verteiler enthalten sind, an den die E-Mail gesendet worden ist.

Das Katholische Datenschutzzentrum empfahl der verantwortlichen kirchlichen Stelle, MA A separat, z. B. per Briefpost, zeitnah vor Rückkehr an den Arbeitsplatz zu informieren. Alle Mitarbeitenden hatten die E-Mail datenschutzkonform zu löschen. Außerdem sollte sichergestellt werden, dass in Zukunft durch zusätzliche Kontrollmaßnahmen und weitere Maßnahmen die Prozesssicherheit des Versendens von personenbezogenen Daten erhöht wird. Insbesondere Daten der besonderen Kategorie in jeder Form sollten nicht als unverschlüsselte E-Mail versendet werden.

Hinweis für kirchliche Einrichtungen

Die Namensgebung von E-Mail-Verteilern sollte so eindeutig gestaltet werden, dass eine Verwechslung (möglichst) ausgeschlossen werden kann und durch die Vorschläge der Autovervollständigen-Funktion der E-Mail-Programme nicht ungewollt ein falscher Verteiler ausgewählt wird.

2.2.3 Foto in sozialen Medien enthält Patientendaten auf dem Monitor im Hintergrund

In einem Krankenhaus wurden für eine Social-Media-Kampagne Fotos erstellt. Von den auf den Fotos dargestellten Mitarbeitenden lag eine entsprechende Einverständniserklärung vor, jedoch nicht von den Patienten, deren personenbezogene Daten im Hintergrund eines Fotos auf einem Monitor zu sehen waren. Bei entsprechender Vergrößerung des Fotos waren diese Daten zu erkennen.

Bei der Bearbeitung der Bilder durch das Marketing wurde durch den Fachbereich ein separates Bild zur Verfügung gestellt. Dieses wurde in das Originalbild mit einer Fotobearbeitungssoftware eingefügt und der abgebildete Monitor unscharf dargestellt.

Nachdem das bearbeitete Bild in verschiedenen Social-Media-Kanälen gepostet wurde, fiel auf, dass bei entsprechender Betrachtung des Bildes immer noch der Patientennamen abgelesen werden konnte.

Direkt nach Bekanntwerden wurde das Bild aus den Postings entfernt. Bis dahin wurde das Posting bereits rund 4.500-mal angezeigt. Das Marketingteam wurde nochmals geschult und zukünftige Unkenntlichmachungen werden durch Zensurierung oder Schwärzung vorgenommen. Vor der Veröffentlichung von Bildern werden diese in Zukunft nochmals auf personenbezogene Daten geprüft.

Einen ähnlich gelagerten Fall meldete eine Marketing- und Kommunikationsabteilung eines Klinikverbundes. Zu den Aufgaben dieser Abteilung gehört es auch, Einverständniserklärungen zur Bildnutzung an Organe der Presse zu übermitteln. Üblicherweise wird dabei ein Link übermittelt, der zu der freigegebenen Abbildung führt. Im vorliegenden Fall war aber nicht nur das Bild des entsprechenden Mediziners zu sehen, welches veröffentlicht werden sollte, sondern auch dessen Unterschrift. Die handschriftliche Unterschrift eines Menschen hat im Rechtsverkehr nach wie vor eine hohe Bedeutung. Gerät sie in unbefugte Hände, besteht die Gefahr der missbräuchlichen Verwendung.

Die Marketingabteilung hat daher unverzüglich alle internen Stellen über den Vorfall informiert. Die Empfängerin der unberechtigt übersendeten Unterschriftsvorlage wurde zudem zur Löschung aufgefordert. Ferner wurde das Verfahren zur Übermittlung von Einverständniserklärungen zur Bildnutzung überarbeitet. Die Empfängerin der unberechtigt übersendeten Unterschriftsvorlage bestätigte deren Löschung.

Hinweis für kirchliche Einrichtungen

Werden Fotos veröffentlicht, sollte der Verantwortliche immer prüfen, ob eine Einwilligung für abgebildete Personen vorliegt und ob sich auf dem Bild erkennbare personenbezogene Daten befinden, die dann zu entfernen oder unkenntlich zu machen sind.

2.2.4 Diebstahl von Gehaltsabrechnungen aus dem Briefkasten der Einrichtung

Auf dem Gelände einer Kita haben sich an einem Wochenende unbefugte Personen aufgehalten. Aus dem Briefkasten wurden Briefe entfernt, die aufgrund ihrer Größe durch den Briefschlitz greifbar waren. In dem Umschlag befanden sich Gehaltsabrechnungen von allen Mitarbeitenden. Die Umschläge der Gehaltsabrechnungen wurden geöffnet und die enthaltenen Gehaltsabrechnungen angezündet oder in den Mülleimer der angrenzenden Schule entsorgt.

Nach Bekanntwerden der Datenschutzverletzung wurden alle Gehaltsabrechnungen, die noch gefunden werden konnten, eingesammelt. Alle Mitarbeitenden wurden über den Vorfall informiert. Am Briefkasten wurde ein Hinweis angebracht, dass beim Einwurf von Umschlägen darauf zu achten ist, dass diese nicht wieder herausgezogen werden können.

Hinweis für kirchliche Einrichtungen

Nicht immer liegen die Ursachen für Datenschutzverletzungen im Machtbereich des Verantwortlichen. Schwer beeinflussbar ist, wie hier dargestellt, das Verhalten von Post- und Paketdienstleistern. Eventuell können zusätzliche Maßnahmen, wie die Zustellung digitaler Gehaltsabrechnungen geprüft werden.

2.2.5 Ausdrucke mit personenbezogenen Daten als Malpapier in der Kita

Eine dem Katholischen Datenschutzzentrum angezeigte Meldung behandelte die Verwendung der Rückseite eines Papierblattes als Malpapier. Kindern in einer Kindertagesstätte wurde, aus Nachhaltigkeitsgesichtspunkten, Malpapier zur Verfügung gestellt, das auf einer Seite bereits beschrieben/bedruckt war. Ein Kind hatte sein Blatt, mit Kunstwerk auf der einen und personenbezogenen Daten auf der anderen Seite, mit nach Hause genommen. Dort fiel der Mutter des Kindes die bedruckte Vorderseite mit den Daten auf. Das Blatt wurde von der Mutter an die KiTa zurückgegeben, wo es vernichtet wurde.

Der Vorgang berührt mehrere für den Datenschutz relevante Bereiche. Dazu gehört die erforderliche Sorgfalt beim Umgang mit Daten, deren Speicherung und die sichere Vernichtung für den Fall, dass die Daten in der vorgehaltenen Form nicht mehr benötigt werden. Auch wenn die

Weiterverwendung von einseitig bedrucktem Papier als Malpapier aus Gründen der Nachhaltigkeit zu begrüßen ist, geht der Schutz von personenbezogenen Daten vor. Die Verwendung als Malpapier verbietet sich somit.

Hinweis für kirchliche Einrichtungen

Besteht kein Grund bzw. keine Rechtsgrundlage mehr, in Papierform vorgehaltene Daten weiter zu erhalten, sind diese unverzüglich zu vernichten. Ein einfaches Zerreißen reicht hierbei nicht aus. Durch den Träger von Kindertagesstätten bzw. den für die Verarbeitung von personenbezogenen Daten Verantwortlichen sind technische und organisatorische Maßnahmen einzurichten, welche den Mitarbeitenden vor Ort die Möglichkeit geben, Papierdaten auf eine datenschutzgerechte Weise zu vernichten bzw. zu entsorgen. Dies kann durch entsprechend geeignete Datenmüll-Sammelbehälter und die ordnungsgemäße Weiterbehandlung des Inhalts erfolgen. Für kleinere Einrichtungen, in denen nur gelegentlich Papierdatenmüll anfällt, empfiehlt es sich, auf Büro-Aktenvernichter zurückzugreifen, die mindestens den Vernichtungsstandard P4 erfüllen.

2.2.6 Vertauschter Patientenaufkleber

Beim Erstellen einer Verordnung für ein Sanitätshaus wurde versehentlich ein falscher Patientenaufkleber verwendet. Der Aufkleber enthielt zusätzlich die Telefonnummer des Notfallkontaktes des Patienten. Durch das Sanitätshaus wurde diese Telefonnummer genutzt, um den Patienten zu kontaktieren, da die Angabe der Versichertennummer auf der Verordnung fehlte.

Durch dieses Versehen wurden also nicht nur die Daten des Patienten, sondern zusätzlich Daten des Notfallkontaktes an (unberechtigte) Dritte weitergegeben (zwei betroffene Personen). Der Meldende gab an, da auch zukünftig nicht hundertprozentig ausgeschlossen werden könne, dass versehentlich ein falscher Aufkleber verwendet werde, sei die Löschung der Notfalltelefonnummern von jeglichen Patientenaufklebern veranlasst worden.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt, solche Thematiken als Beispiele in den regelmäßig stattfindenden Datenschutzschulungen aufzugreifen und die internen Prozesse generell in Bezug auf Datenminimierung zu überprüfen.

2.2.7 Weitergabe von Patientendaten an Polizei

In einem Krankenhaus wurde eine alkoholisierte Patientin mit einem Rettungswagen (RTW) eingeliefert. Kurz darauf traf eine ebenfalls alko-

holisierte Freundin der Patientin mit einem Pkw am Krankenhaus ein. Nach der Entlassung wurde durch Mitarbeitende der Aufnahme beobachtet, wie die beiden alkoholisierten Frauen mit dem Auto der Freundin wegfuhrten. Auf dem Parkplatz des Krankenhauses rammten und beschädigten sie ein parkendes Motorrad und flüchteten vom Unfallort.

Durch die informierte Polizei wurde der Unfall aufgenommen. Das RTW-Protokoll wurde auf Nachfrage der Polizei von den Mitarbeitenden der Aufnahme an die Polizei ausgehändigt. Das Protokoll nimmt Bezug auf die Patientin. Die Namen der RTW-Besatzung sind ebenfalls im Protokoll vermerkt. Da der Parkplatz des Krankenhauses über keine Videoüberwachung verfügt, wurde vermutet, dass die Polizei über die personenbezogenen Daten der Patientin die Unfallverursacherin einfacher identifizieren kann.

Auf Rückfrage des Verantwortlichen bei der Polizei wurde mitgeteilt, dass das RTW-Protokoll nicht in die Ermittlungsakte der Polizei eingeflossen ist, da es irrelevant und nicht Bestandteil des Verfahrens sei. Das Dokument wurde gemäß dem Dokumentenvernichtungsprozess bei der Polizei vernichtet. Die Besatzung des RTW wurde über die Weitergabe der Daten an die Polizei durch den Verantwortlichen informiert. Betroffene Bereiche im Krankenhaus, die mit Ermittlungsbehörden in Kontakt kommen können, wurden speziell geschult.

Hinweis für kirchliche Einrichtungen

Nicht nur der Aufnahmebereich in Krankenhäusern, sondern alle Bereiche in Einrichtungen und Unternehmen, die mit Ermittlungsbehörden in Kontakt kommen können, sollten speziell geschult werden, unter welchen Voraussetzungen personenbezogene Daten an die Behörden weitergegeben werden dürfen und müssen und wann nicht.

2.2.8 Ransomware-Angriff bei ehrenamtlicher Tätigkeit auf dienstlichem PC

Ein ehrenamtlicher Mitarbeiter eines kirchlichen Verantwortlichen ist Partner in einer Rechtsanwaltskanzlei und hat für die Erledigung der ihm übertragenen Aufgaben beim kirchlichen Verantwortlichen seinen beruflich genutzten PC verwendet. Er wurde Opfer eines Ransomware-Angriffs.

In der Folge waren alle Computer in der Kanzlei von dem Angriff betroffen und wurden verschlüsselt. Der Verantwortliche hat den Vorfall umgehend bei der Polizei zur Anzeige gebracht. Der ehrenamtliche Mitarbeiter konnte mithilfe einer Sicherungskopie die verschlüsselten Daten des Verantwortlichen wiederherstellen. Die Bereinigung der IT von Schadsoftware und die Prüfung der Backups auf Schadsoftware haben ca. eine Woche in Anspruch genommen. Sämtliche Daten des Verantwortlichen stehen nach der Rücksicherung wieder zur Verfügung.

Alle Versuche, die Ursache des Angriffs mithilfe von Spezialisten der Cyber-Risk-Versicherung herauszufinden, blieben erfolglos. Die Spe-

zialisten konnten einen Abfluss der Daten nicht bestätigen. Eine Veröffentlichung oder ein Verkaufsangebot der Daten im Darknet konnte ebenfalls nicht bestätigt werden.

Hinweis für kirchliche Einrichtungen

Funktionierende und getestete Backups sind bei einem Ransomware-Angriff essenziell. Backups auf Medien, die vom Netzwerk physikalisch getrennt sind (Offline-Backup), sind aufwendiger in der Handhabung, bieten aber größte Sicherheit bei so einem Angriff. Weitere technische Maßnahmen wie z. B. Virens Scanner oder Netzwerksegmentierung können wirksam die Ausbreitung von Ransomware in einem Netzwerk verhindern oder eindämmen. Da eines der Haupt-Einfallstore für Ransomware immer noch E-Mails mit manipulierten Anhängen sind, ist die Schulung und Sensibilisierung der Mitarbeitenden ein großer Baustein im gesamten Sicherheitspaket eines Unternehmens.

Um das Risiko der Betroffenheit von Ransomware-Angriffen zu vermindern, sollten Verantwortliche, wo möglich, auf den Einsatz privater IT-Hardware verzichten.

2.2.9 Mitarbeiter verschafft sich unbefugt Zugriff auf E-Mail-Account

Eine kirchliche Einrichtung aus dem Zuständigkeitsbereich des Katholischen Datenschutzzentrums meldete, dass ein Mitarbeiter sich unbefugten Zugriff auf den dienstlichen E-Mail-Account des Vorgesetzten verschafft hatte. Ursache dafür war, dass der Vorgesetzte seinen PC nicht gesperrt hatte, nachdem er aufgrund eines Notfalls bei einem Patienten bzw. Bewohner der Einrichtung das Büro kurzfristig verlassen musste. Während seiner Abwesenheit setzte sich der Mitarbeiter an den ungesperrten Computer und rief E-Mails ab, in denen es um seine Person in arbeitsrechtlich relevanten Themen ging.

Der betreffende PC wurde grundsätzlich von mehreren Personen genutzt, die sich jeweils mit ihren eigenen Zugangsdaten anmelden konnten. Da der Benutzerzugang des Vorgesetzten jedoch offen war, konnte der Mitarbeiter auf die E-Mails des Vorgesetzten zugreifen. Der Vorgesetzte wurde nochmal sensibilisiert, auch bei kurzen Abwesenheiten den PC zu sperren. Der Zugriff des Mitarbeiters war (nicht nur) datenschutzrechtlich unzulässig, auch wenn er sich nur E-Mails angeschaut hat, die ihn betrafen.

Hinweis für kirchliche Einrichtungen

Dieser Fall zeigt einmal mehr, dass es notwendig ist, seinen PC bei Abwesenheit zu sperren. Es zeigt auch, dass die Gefahr unbefugter Zugriffe auf die IT-Systeme einer Einrichtung nicht nur von außen kommt, sondern in ganz vielen Fällen die Angriffe oder Zugriffsversuche aus dem Haus heraus versucht und durchgeführt werden.



2.3 Beschwerden und Hinweise

Betroffene haben aus § 48 KDG das Recht auf Beschwerde an die Datenschutzaufsicht, soweit sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen Datenschutzvorschriften verstößt. Beschwerden, die nicht die eigenen Daten, sondern die einer anderen Person betreffen, werden als Hinweis gewertet.

Nach dem Eingang einer Beschwerde prüft das Katholische Datenschutzzentrum den Sachverhalt im Hinblick auf das Vorliegen einer Datenschutzverletzung. Im Anschluss daran werden Beschwerdegegner und Beschwerdeführer (teilweise mehrfach) um Stellungnahme zum Sachverhalt bzw. zum Vorbringen der anderen Verfahrensbeteiligten aufgefordert, bevor das KDSZ eine Entscheidung trifft.

Für eine zeitnahe Bearbeitung ist es sehr wichtig, dass die Beschwerde alle wichtigen Informationen zum Beschwerdesachverhalt und zur betroffenen Person enthält. Damit es hier nicht zu Verzögerungen kommt, empfiehlt das Katholische Datenschutzzentrum, die Beschwerde über das Beschwerdeformular auf der Homepage⁸³ einzureichen.

Im Berichtsjahr 2025 hat sich die Anzahl an Beschwerden und Hinweisen im Vergleich zum Vorjahr stark erhöht, die Hinweise haben sich sogar verdreifacht. Eine grobe Einteilung wird durch die folgenden Grafiken verdeutlicht, einzelne Aspekte werden in diesem Abschnitt im Folgenden erläutert.

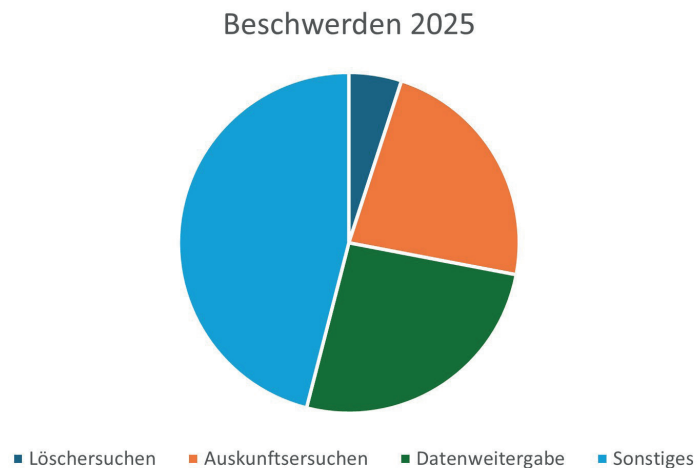


Abb. 4: Beschwerden an das KDSZ im Jahr 2025.

⁸³ Link zum Beschwerdeformular auf der Internetseite des Katholischen Datenschutzzentrums: <https://www.katholisches-datenschutzzentrum.de/beschwerde/>

Hinweise 2025

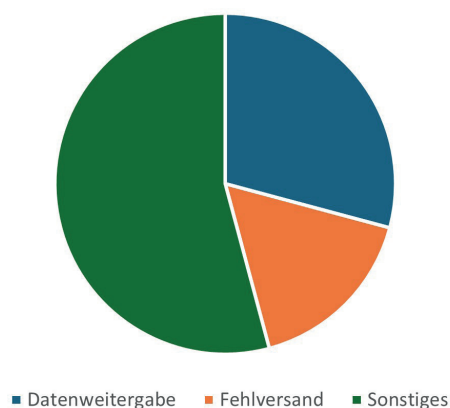


Abb. 5: Hinweise an das KDSZ im Jahr 2025.

2.3.1 Mängel bei der Datenbereitstellung über eine Online-Dateiablage

Über die Jahre ist das Bewusstsein für geeignete technische und organisatorische Maßnahmen bei vielen Verantwortlichen spürbar gestiegen. Verfahren, die eine Ende-zu-Ende-Verschlüsselung sicherstellen, sind heute beispielsweise deutlich bekannter als noch zum Inkrafttreten des KDG. Gleichzeitig zeigt sich in der Aufsichtspraxis des Katholischen Datenschutzzentrums immer wieder, dass gute Technik allein nicht ausreicht, wenn sie im Alltag nicht richtig angewendet wird. Gerade bei neuen Anwendungen kommt es vor, dass Mitarbeitende nicht ausreichend geschult werden und deshalb weder die Funktionsweise noch der eigentliche Zweck der eingesetzten Schutzmaßnahmen bei den Mitarbeitenden ankommt. Das führt dazu, dass sich das Katholische Datenschutzzentrum regelmäßig mit Beschwerden über fehlerhafte Verarbeitungen befasst, obwohl diese Fehler durch geeignete, bereits vorgesehene Prozesse vermeidbar gewesen wären.

Im Berichtszeitraum gab es etwa Beschwerden zu einer Cloud-Anwendung, die eine Ende-zu-Ende-Verschlüsselung garantierte, um sensible Dokumente bereitzustellen. Betroffene Personen erhielten Zugriff auf diese Dokumente, die Anmeldeinformationen (Zugangslink und Passwort) wurden jedoch von Mitarbeitenden des Verantwortlichen in einer unverschlüsselten E-Mail versandt. Damit war für diese Anmeldeinformationen allenfalls eine Transportverschlüsselung gewährleistet (also ein Schutz auf dem Übertragungsweg, der nicht denselben Schutz bietet wie eine Ende-zu-Ende-Verschlüsselung).

Die Beschwerden waren in diesen Fällen begründet. Zwar schreibt das Gesetz keine bestimmte Verschlüsselungsart für Übermittlungen personenbezogener Daten außerhalb eines geschlossenen und gesicherten Netzwerks vor. Verantwortliche müssen jedoch ein dem Stand der Technik entsprechendes und dem jeweiligen Sicherheitsbedarf bzw. der Sensibilität der Daten angemessenes Verfahren auswählen. Bei sehr sensiblen Daten kann grundsätzlich davon ausgegangen werden, dass der Schutzbedarf, wie hier, regelmäßig eine Ende-zu-Ende-Verschlüs-



„Zwar schreibt das Gesetz keine bestimmte Verschlüsselungsart für Übermittlungen personenbezogener Daten [...] vor. Verantwortliche müssen jedoch ein dem Stand der Technik entsprechendes und dem jeweiligen Sicherheitsbedarf bzw. der Sensibilität der Daten angemessenes Verfahren auswählen.“



selung erfordert. Wenn dann ausgerechnet die Anmeldeinformationen unverschlüsselt versandt werden, sind personenbezogene Daten zumindest nicht vollständig entsprechend dem erforderlichen Schutzniveau abgesichert.

Besonders ärgerlich war in dieser Konstellation, dass der Verantwortliche in seiner eigenen Prozessbeschreibung bereits geeignete Maßnahmen vorgesehen hatte, um die Anmeldeinformationen passend zum Schutzbedarf zu übermitteln, etwa den Zugangslink schriftlich zu versenden und das Passwort getrennt, zum Beispiel telefonisch, mitzuteilen. Diese Maßnahmen wurden jedoch im konkreten Arbeitsablauf nicht umgesetzt, weil Mitarbeitende dafür nicht ausreichend geschult oder angewiesen waren.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum begrüßt es ausdrücklich, wenn Verantwortliche die oft nicht einfachen Schritte zur Verbesserung ihrer Arbeitsprozesse angehen. Dazu gehört allerdings auch, dass die Mitarbeitenden so geschult werden, dass neue Anwendungen und Prozesse im Alltag zuverlässig funktionieren. Nur dann erreichen die vorgesehenen Schutzmaßnahmen auch tatsächlich ihr Ziel und es kommt nicht zu vermeidbaren Datenschutzverletzungen und infolgedessen zu Beschwerden der Betroffenen.

2.3.2 Offenlegung von personenbezogenen Daten in der Notaufnahme

Zu Anfang des Berichtszeitraums häuften sich Eingaben, in denen Patienten eine fehlende Vertraulichkeit bei der Anmeldung in Notaufnahmen, Krankenhäusern oder medizinischen Versorgungszentren schilderten. Wiederkehrendes Muster war, dass Angaben aus Aufnahmegesprächen im Wartebereich verständlich waren, etwa wegen ungünstiger Raumzuschnitte, fehlender Abschirmungen oder weil der Empfang akustisch offen zum Wartebereich lag. Dies führte wiederholt zu nachvollziehbaren Beschwerden und in mehreren Verfahren, teils bereits im Verlauf des Beschwerdeverfahrens, zu Nachbesserungen, deren Umsetzung von den Verantwortlichen nachzuweisen war.

Personenbezogene Daten sind nach § 7 Abs. 1 lit. f) KDG so zu verarbeiten, dass eine angemessene Sicherheit gewährleistet ist. Zum Schutzziel der Vertraulichkeit gehört insbesondere der Schutz vor unberechtigter oder unbefugter Verarbeitung, einschließlich der unbefugten Offenlegung. Verantwortliche haben deshalb nach § 26 Abs. 1 KDG geeignete technische und organisatorische Maßnahmen zu treffen und einzuhalten, um personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbefugter Offenlegung zu schützen. Werden besondere Kategorien personenbezogener Daten verarbeitet, wozu auch Gesundheitsdaten zählen, verlangt § 11 Abs. 4 KDG zudem angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person. Gesundheitsdaten als besondere Kategorie personenbezogener Daten im Sinne von § 4 Nr. 2 und Nr. 17 KDG unterfallen



nach § 13 KDG-DVO der Datenschutzklasse III und sind einem erhöhten Schutzniveau (Schutzniveau III) zuzuordnen.

Entscheidend für die Geeignetheit der Schutzmaßnahmen in der Praxis sind die konkreten Gegebenheiten am Empfang (z. B. Abstände, Blick- und Hörbeziehungen, Publikumsverkehr), die typischen Gesprächsinhalte sowie die Frage, ob Dritte die Inhalte ohne besondere Anstrengung wahrnehmen können.

Für Verantwortliche ergibt sich daraus, dass Aufnahme- und Wartebereiche so organisiert werden müssen, dass vertrauliche Inhalte nicht in den öffentlichen Bereichen wahrgenommen werden können. Wo möglich, ist eine bauliche Lösung vorzugswürdig (z. B. separater Aufnahme- und Warteraum, Türen/Trennwände, geeignete Anordnung von Warteflächen). Bei Planungen sollte außerdem geprüft werden, welche schallschutztechnischen Anforderungen für die Nutzung realistisch erforderlich sind (insbesondere bei Türen und Wandanschlüssen), um die Sprachverständlichkeit in angrenzenden Bereichen zu begrenzen. Wenn bauliche Änderungen nur eingeschränkt umsetzbar sind (etwa wegen baulicher Restriktionen), sind alternative Schutzkonzepte erforderlich. Dazu zählen beispielsweise akustisch wirksame Abschirmungen am Empfang (z. B. Trennsysteme, Kabinenlösungen), die gezielte Reduzierung der Sprachverständlichkeit im Wartebereich durch Beschallungslösungen sowie organisatorische Regeln für Gespräche und Telefonate: Vertrauliche Rückfragen sollten außerhalb öffentlich zugänglicher Bereiche geführt werden; wo das nicht geht, sind Inhalte strikt zu begrenzen (z. B. keine Kombination aus Namen und krankheitsbezogenen Details).⁸⁴

In zahlreichen Einrichtungen ließ sich der Vertraulichkeitsschutz bereits mit relativ geringen baulichen Maßnahmen wie beispielsweise Akustikdämmplatten im Wartebereich, einer beschallten Hintergrundkulisse im Wartebereich, Akustiktrennwänden oder Aufnahmekabinen sowie separat nutzbaren, geschlossenen Räumen für Erstaufnahme und vertrauliche Rückfragen deutlich verbessern. Entscheidend ist, dass die gewählte Kombination aus technischen, organisatorischen und baulichen Maßnahmen im konkreten Ablauf nachweisbar dazu führt, dass Dritte Inhalte von Aufnahmegesprächen nicht mehr ohne Weiteres mithören können.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt eine regelmäßige Prüfung der aktuellen Gegebenheiten in der Praxis. Kurze Testsituationen zu typischen Tageszeiten (Stoßzeiten vs. ruhige Zeiten) können zeigen, ob Dritte Inhalte mithören können. Ergänzend ist das Personal zu unterweisen, in Gegenwart Dritter besonders sparsam zu kommunizieren (z. B. keine Diagnosen/Befunde/Patientennamen im Wartebereich), und es sind Ausweichabläufe festzulegen (z. B. Rückruf aus einem separaten Raum).

⁸⁴ Zu akustischen Schutzmaßnahmen und organisatorischen Empfehlungen im Empfangs-/Wartebereich vgl. Hinweise zur Diskretion in Arztpraxen des LfDI Baden-Württemberg (<https://www.baden-wuerttemberg.datenschutz.de/diskretion-in-der-arztpraxis/>) sowie dessen 34. Tätigkeitsbericht (Abschnitt 7.1; <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf>).

2.3.3 Öffnung von Gehaltsabrechnungen durch Arbeitgeber

In der zweiten Jahreshälfte 2025 befasste sich das KDSZ mit der Frage, ob ein Dienstgeber die Gehaltsabrechnungen eines Beschäftigten öffnen durfte.

Der Beschwerdeführer hatte seine Gehaltsabrechnungen und Sozialversicherungsnachweise für mehrere Monate nicht in den Originalumschlägen des Abrechnungsdienstleisters erhalten, sondern in neutralen Umschlägen ohne Absender. Er vermutete daher, dass sein Arbeitgeber die ursprünglichen Sendungen geöffnet und anschließend neu verpackt hatte. Einen Grund dafür sah er nicht. Zwar war ihm im Juni 2025 versehentlich sein übliches Gehalt anstelle von Krankengeld ausgezahlt worden. Aus seiner Sicht rechtfertigte dies jedoch keine Öffnung der Gehaltsunterlagen.

Der Dienstgeber erklärte, dass mehrere Postsendungen für dieselbe Person aus Gründen der Portosparnis gemeinsam versandt würden. Die einzelnen Briefe würden dabei grundsätzlich nicht geöffnet. Zugleich teilte er mit, dass eine Öffnung im Einzelfall zu Kontrollzwecken möglich sei. Die Verwaltungsleitung verfüge über umfassende Befugnisse und könne die für die Beschäftigungsverhältnisse erforderlichen Angaben außerdem über ein Online-Portal einsehen.

Im Fall des Beschwerdeführers hielt der Dienstgeber es für möglich, dass die Gehaltsmitteilung für Juni 2025 geöffnet worden war. Hintergrund war die fehlerhafte Gehaltszahlung in diesem Monat. Für die Monate Juli bis September 2025 schloss er eine Öffnung dagegen aus.

Das KDSZ bewertete die Beschwerde hinsichtlich der Gehaltsabrechnung für Juni 2025 als begründet. Angaben zum Gehalt sind personenbezogene Daten. Auch die Einsichtnahme in eine Gehaltsabrechnung stellt eine Verarbeitung personenbezogener Daten im Sinne des KDG dar.

Zwar gehören Gehaltszahlungen und die dazugehörigen Abrechnungen zur Durchführung eines Beschäftigungsverhältnisses. Die Öffnung des an den Beschäftigten gerichteten Gehaltsbriefs war im konkreten Fall jedoch nicht erforderlich. Der Dienstgeber konnte die für die Kontrolle notwendigen Angaben bereits über das Online-Portal einsehen. Damit stand ihm ein gleich geeignetes, aber weniger eingriffsintensives Mittel zur Verfügung.

Auch eine andere Rechtsgrundlage für die Öffnung des Gehaltsbriefs war nicht ersichtlich. Weder lag eine Einwilligung des Beschwerdeführers vor noch griff ein anderer Erlaubnistatbestand des KDG ein. Die Öffnung der Gehaltsmitteilung für Juni 2025 war daher rechtswidrig.

Für die weiteren beanstandeten Monate fiel die Bewertung anders aus. Es ließ sich nicht mit der erforderlichen Sicherheit feststellen, dass der Dienstgeber auch diese Gehaltsbriefe geöffnet hatte. Insoweit war die Beschwerde unbegründet.

Hinweis für kirchliche Einrichtungen

Der Fall zeigt, dass auch bei berechtigten Kontrollinteressen des Dienstgebers stets zu prüfen ist, ob für die Verarbeitung von Beschäftigtendaten ein weniger eingriffsintensives, aber ebenso geeignetes Mittel zur Verfügung steht.

2.4 Prüfungen

Eine der Aufgaben der Datenschutzaufsicht ist es, die Einhaltung der Datenschutzgesetze zu überwachen. Um dies zu gewährleisten, werden regelmäßig Datenschutzüberprüfungen durch den Diözesandatenschutzbeauftragten beziehungsweise das Katholische Datenschutzzentrum durchgeführt, um den Schutz personenbezogener Daten zu sichern (§ 44 KDG).

Das Katholische Datenschutzzentrum führt anlassunabhängige Überprüfungen durch, bei denen verschiedene kirchliche Einrichtungen evaluiert und (vor Ort) im Rahmen einer Querschnittsprüfung geprüft werden. Der Zweck dieser Prüfungen ist, ein Bild über die Umsetzung des Datenschutzes zu erhalten und das Bewusstsein innerhalb der Einrichtungen zu erhöhen.⁸⁵ Darüber hinaus finden auch anlassbezogene Prüfungen statt, die auf Meldungen, Beschwerden oder anderen Erkenntnissen basieren.

2.4.1 Ist der betriebliche Datenschutzbeauftragte beim Katholischen Datenschutzzentrum gemeldet?

Die Verantwortlichen haben dem Diözesandatenschutzbeauftragten nach § 36 Abs. 4 Satz 2 KDG die Benennung eines betrieblichen Datenschutzbeauftragten anzuzeigen. Da eine große Anzahl der Meldungen der betrieblichen Datenschutzbeauftragten mit Inkrafttreten des KDG im Mai 2018 erfolgt ist und die Daten daher mittlerweile mehrere Jahre alt sind, hat das Katholische Datenschutzzentrum im Berichtsjahr damit begonnen, den Kontakt mit den kirchlichen Stellen im Rahmen der Bearbeitung von Meldungen von Datenschutzverletzungen oder von Beschwerden zu nutzen, um stichprobenartig zu prüfen, ob von der kirchlichen Stelle als Verantwortlicher im Sinne des KDG ein betrieblicher Datenschutzbeauftragter gemeldet wurde und ob diese Daten noch aktuell sind.

2.4.2 Prüfung von Datenschutzhinweisen auf Internetseiten

Den gesamten Berichtszeitraum hindurch hat das Katholische Datenschutzzentrum anlasslose Prüfungen der Datenschutzhinweise auf Internetseiten von Verantwortlichen aus dem Zuständigkeitsbereich durchgeführt. Dabei wurde keine vollständige datenschutzrechtliche

⁸⁵ Über die Prüfungen berichtet das KDSZ auf seiner Internetseite: <https://www.katholisches-datenschutzzentrum.de/themen/pruefungen/>

Prüfung des gesamten Internetauftritts durchgeführt. Es wurde nur geprüft, ob Datenschutzhinweise vorhanden sind und diese einfach für die Besucher der Webseiten zu erreichen sind. Der Fokus der Prüfung lag auf den Transparenz- und Informationspflichten aus Kapitel 3 des KDG.

Geprüft wurde unter anderem die Nennung der Betroffenenrechte und des Verantwortlichen, der Hinweis auf das Beschwerderecht bei einer Datenschutzaufsichtsbehörde sowie die Zwecke und Rechtsgrundlagen der Verarbeitungstätigkeiten von personenbezogenen Daten auf der Internetseite. Die Verwendung von Cookies und Einwilligungsbarren wurde nur in Ausnahmefällen geprüft.

Nach Hinweis an den Verantwortlichen wurden gefundene Mängel von den Verantwortlichen innerhalb der gesetzten Fristen abgestellt. Die Prüfungen werden im kommenden Berichtszeitraum fortgesetzt.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum empfiehlt, die Datenschutzhinweise regelmäßig zu kontrollieren, um Änderungen an der Internetseite auch direkt in den Datenschutzhinweisen abbilden zu können.

2.4.3 Prüfung des Einsatzes von Videoüberwachung in kirchlichen Einrichtungen

In den vergangenen Jahren hat das Katholische Datenschutzzentrum einen stetigen Strom von Beschwerden bezüglich verschiedener Varianten von Videoüberwachungen feststellen können. Die Videoüberwachung gehört neben dem Auskunftsrecht zu den klassischen Streitthemen in der datenschutzrechtlichen Aufsichtspraxis. In den meisten Fällen führte eine zu intransparente Information über die jeweilige Überwachung zur Beschwerde. Die überwiegende Anzahl der Verantwortlichen konnte Mängel bei der Verarbeitung recht einfach beheben, indem sie beispielsweise Informationsaushänge verbesserte oder Überwachungszeiträume einschränkte. In den wenigsten Fällen musste eine Unterlassung der Videoüberwachung angeordnet werden. Aufgrund der immer wiederkehrenden Thematik hat sich das Katholische Datenschutzzentrum dazu entschlossen, in diesem Bereich verstärkt zu prüfen. Daher wurde im Berichtszeitraum eine erste Querschnittsprüfung zur Videoüberwachung durchgeführt.

Ziel der Prüfung war es, einen Überblick über die in den Einrichtungen eingesetzten Videoüberwachungsanwendungen zu gewinnen und diese im Hinblick auf die datenschutzrechtlichen Anforderungen zu bewerten. Dabei wurde ein rechtlicher Schwerpunkt auf die Erfüllung der Dokumentationspflichten gesetzt. Hierzu gehörten insbesondere das Vorhandensein und die Qualität der einschlägigen Verzeichnisse von Verarbeitungstätigkeiten (VVT), gegebenenfalls durchgeführte Datenschutz-Folgenabschätzungen (DSFA) sowie ein nachvollziehbares Speicher- und Löschkonzept. Darüber hinaus wurden die von



„In den meisten Fällen führte eine zu intransparente Information über die jeweilige Überwachung zur Beschwerde.“

den Verantwortlichen festgelegten Zwecke der Videoüberwachung betrachtet. In diesem Zusammenhang wurde geprüft, ob die Zwecke hinreichend bestimmt und dokumentiert waren. Ein weiterer Schwerpunkt lag auf der Erforderlichkeit der Videoüberwachung, insbesondere auf der Frage, ob der jeweils verfolgte Zweck auch durch mildere, gleich geeignete Mittel hätte erreicht werden können und ob entsprechende Alternativen geprüft worden waren.

Die zu prüfenden Einrichtungen wurden zufällig aus den Kategorien Kirchengemeinden, Krankenhäuser und Schulen ausgewählt. Mit dieser Auswahl wurde ein breiter Querschnitt kirchlicher Einrichtungen angestrebt, um unterschiedliche tatsächliche und organisatorische Rahmenbedingungen abzubilden. Die Einrichtungsarten unterschieden sich hinsichtlich ihrer Aufgaben, räumlichen Gegebenheiten und Schutzbedarfe teils erheblich. Die hieraus gewonnenen Erkenntnisse sollen perspektivisch eine Grundlage dafür bilden, weitere thematische bzw. einrichtungsspezifische Schwerpunktprüfungen zu entwickeln.

Die Ergebnisse der Befragung entsprachen in etwa den Erwartungen des Katholischen Datenschutzzentrums. So spiegelten sich in einigen Einrichtungen die allgemeinen, schon aus den Beschwerdeverfahren der Vergangenheit bekannten Probleme, wie etwa eine unzureichende Dokumentation der Verarbeitung. Daneben gaben viele der befragten Einrichtungen, insbesondere im Schulbereich, an, dass sie gar keine Videoüberwachung durchführen. In wenigen Fällen blieben die Einrichtungen hinter den Erwartungen zurück. Diese Einrichtungen gaben an, zwar eine Videoüberwachung durchzuführen, aber über keinerlei Dokumentation zu verfügen. Das deutet auf erhebliche Mängel im datenschutzrechtlichen Bereich hin. Diese Einrichtungen werden umfassender vor Ort geprüft werden.

Die Prüfungsreihe ist zweiphasig angelegt. In der zweiten Phase sollen ausgewählte Einrichtungen im Einzelnen vertieft geprüft werden. Dabei soll die Videoüberwachung im konkreten Anwendungsfall im Vordergrund stehen; ergänzend sollen technische und räumliche Aspekte in den Einrichtungen stärker in den Blick genommen und bewertet werden.

2.5 Künstliche Intelligenz

Anwendungen Künstlicher Intelligenz (KI) sind so schnell und umfassend Bestandteil des täglichen Lebens aller Menschen geworden, dass eine umfassende Diskussion dieses Themas an dieser Stelle nicht möglich ist. Daher sollen hier nur einige datenschutzrechtlich interessante und relevante Hinweise zu dem Thema gegeben werden.

2.5.1 Päpstliche Mahnungen und kirchliche Leitlinien

Schon kurz nach seiner Wahl zum neuen Papst machte Papst Leo XIV. deutlich, dass er das Thema Künstliche Intelligenz als eines der zentralen Zukunftsthemen unserer Zeit einschätze. Dabei betonte er immer wieder die sozialen und ethischen Herausforderungen, die sich durch

die fortschreitenden Entwicklungen im Bereich der Künstlichen Intelligenz ergeben. Trotz dieser Herausforderungen sieht er in der Künstlichen Intelligenz aber ein außergewöhnliches Potenzial zum Wohl der Menschheit. Papst Leo XIV. nimmt sich dieses Themas seit Beginn seines Pontifikates an und hat – nach Ende des Berichtszeitraumes dieses Berichtes – im Mai 2026 seine erste Enzyklika „Magnifica humanitas“ dem Thema Künstliche Intelligenz gewidmet.⁸⁶

Schon im Frühjahr 2025 hat die Verwaltungskommission des Verbandes der Diözesen Deutschlands mit einem Papier für den Einsatz von Künstlicher Intelligenz für Mitarbeitende im kirchlichen Dienst eine erste Orientierung zum dienstlichen Einsatz von Künstlicher Intelligenz gegeben. Datenschutzrechtliche Fragen werden in dem Leitfaden allerdings nur am Rande thematisiert.

2.5.2 Handreichungen für die Bundesverwaltung zum Umgang mit Künstlicher Intelligenz

Im Dezember 2025 veröffentlichte die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine Handreichung für die Bundesverwaltung zur Nutzung Künstlicher Intelligenz. Unter dem Titel „KI in Behörden – Datenschutz von Anfang an mitdenken“⁸⁷ gibt die BfDI umfangreiche Hilfestellungen zum datenschutzkonformen Umgang mit KI, wobei der Schwerpunkt der Handreichung auf der Nutzung großer Sprachmodelle (Large Language Models – LLMs) liegt. Ergänzend dazu enthält die Handreichung eine Übersicht mit Erläuterungen zu mitigierenden Maßnahmen im Verlauf des KI-Lebenszyklus.

Schon im März 2025 veröffentlichte das Bundesministerium des Innern und für Heimat „Leitlinien für den Einsatz Künstlicher Intelligenz in der Bundesverwaltung“⁸⁸, in denen anhand von Leitsätzen für Nutzende und für Behörden die wichtigen klärungsbedürftigen Fragen und Handlungsfelder thematisiert werden.

Hinweis für kirchliche Stellen

Auch wenn sich beide Papiere primär an die Bundesverwaltung richten, sind die dort thematisierten Punkte auch für die kirchlichen Stellen und Verwaltungen zu beachten und daher gut beschrieben.

Insbesondere der Ansatz mit den Leitsätzen für Nutzende und für Einrichtungen ist gut vermittelbar und einprägsam.

⁸⁶ Die Enzyklika „Magnifica Humanitas“ ist abrufbar unter <https://www.vatican.va/content/leo-xiv/de/encyclicals/documents/20260515-magnifica-humanitas.html>

⁸⁷ Die Handreichung ist abrufbar unter <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2025/Handreichung-KI.html>

⁸⁸ <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/ki/BMI25020-leitlinien-ki-bundesverwaltung.html>

2.5.3 Interne Vorgaben zur Nutzung von KI

Viele Anwendungsfälle Künstlicher Intelligenz lassen sich ohne die Eingabe personenbezogener Daten erledigen (siehe beispielsweise die Diskussion um KI-Predigten⁸⁹). Datenschutzrechtlich ist dies allerdings nur dann unproblematisch, wenn im gesamten Nutzungsvorgang, insbesondere bei der Anmeldung, der Eingabe, der Protokollierung, der Ausgabe und der weiteren Verwendung, keine personenbezogenen Daten verarbeitet werden. Dabei genügt es nicht immer, Namen und Anschriften zu entfernen; ein Personenbezug kann sich auch aus dem Zusammenhang ergeben. Unabhängig davon können dienstliche oder sonstige vertrauliche Informationen besonderen Geheimhaltungspflichten unterliegen.⁹⁰

In vielen Fällen kann die KI ihre Vorteile aber nur ausspielen, wenn ihr z. B. eine komplette Vorgangsakte zur Verfügung gestellt wird, um einen konkreten Sachverhalt auszuwerten und einen Entwurf für ein Schreiben an die Beteiligten zu erstellen. Dabei können viele, teils sehr sensible personenbezogene Daten verarbeitet werden. Die allgemeinen datenschutzrechtlichen Rahmenbedingungen für die Verarbeitung dieser Daten sind auch bei der Verarbeitung durch die KI zu beachten. Die Entscheidung für den Einsatz einer KI ersetzt weder die Festlegung eines konkreten Verarbeitungszwecks noch eine datenschutzrechtliche Rechtsgrundlage. Zu prüfen sind insbesondere die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung, die Datenminimierung, die Verantwortlichkeit der beteiligten Stellen, eine mögliche Auftragsverarbeitung, die technischen und organisatorischen Maßnahmen, etwaige Drittlandübermittlungen sowie die Informations- und Betroffenenrechte. Hat die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, ist vorab eine Datenschutz-Folgenabschätzung durchzuführen. Das Beicht- und Seelsorgegeheimnis sowie sonstige gesetzliche, berufliche oder besondere Amtsgeheimnisse bleiben unberührt.⁹¹

Unter welchen Voraussetzungen im konkreten Einzelfall eine KI-Nutzung möglich ist, muss anhand der konkreten Umstände des Einzelfalls abgewogen werden. Vor der Freigabe sollten daher insbesondere die zulässigen Zwecke, die betroffenen Datenkategorien, der Kreis der Nutzungsberechtigten sowie die zulässigen und unzulässigen Eingaben festgelegt werden. Der betriebliche Datenschutzbeauftragte ist frühzeitig einzubeziehen. Auch eine Beteiligung der Mitarbeitervertretung ist gegebenenfalls zu prüfen.⁹²

Unbedingt notwendig ist es, die Beschäftigten auf die Risiken für die (personenbezogenen) Daten der Einrichtung aufmerksam zu machen, die entstehen können, wenn die Beschäftigten eine von der kirchlichen

⁸⁹ Artikel „Expertin: KI-Predigten oft oberflächlich und theologisch bedenklich“ vom 17.08.2025 auf katholisch.de

⁹⁰ Vgl. Orientierungshilfe der DSK vom 06.05.2024: Künstliche Intelligenz und Datenschutz, Abschnitte 1.3, 1.7 und 3.1. Die DSK weist darauf hin, dass nur Einsatzfelder ohne Personenbezug im gesamten Anmelde-, Ein- und Ausgabe- sowie Verarbeitungsprozess nicht dem Datenschutzrecht unterliegen. Auch aus dem Zusammenhang kann sich ein Personenbezug ergeben; zudem können nicht öffentliche dienstliche Informationen gefährdet sein.

⁹¹ Vgl. Orientierungshilfe der DSK vom 06.05.2024 zu KI und Datenschutz, Abschnitte 1.1, 1.5 und 1.7-1.8.

⁹² Vgl. Orientierungshilfe der DSK vom 06.05.2024 zu KI und Datenschutz, Abschnitte 1.1, 1.12 sowie 2.1 bis 2.3. Die DSK empfiehlt die frühzeitige Einbindung des Datenschutzbeauftragten und die Prüfung der Beteiligungsrechte der Beschäftigtenvertretung.

Einrichtung für den Einzelfall nicht bewertete KI-unterstützte Hilfe aus dem Internet nutzen. Mögliche Risiken und Lösungen bei der Nutzung von nicht von der Einrichtung freigegebenen KI-Tools mit (personenbezogenen) Unternehmensdaten müssen gegenüber den Beschäftigten kommuniziert werden. Klare und dokumentierte interne Vorgaben sollten insbesondere festlegen, welche Anwendungen zu welchen Zwecken genutzt werden dürfen, welche Daten nicht eingegeben werden dürfen, ob eine Anonymisierung oder Pseudonymisierung erforderlich ist und wie die von einer KI erzeugten Ergebnisse fachlich überprüft werden müssen. Schulungen, Leitfäden und Gespräche können diese Vorgaben ergänzen. Anbieter und Betreiber von KI-Systemen müssen außerdem Maßnahmen treffen, um die Entwicklung der KI-Kompetenz der mit den Systemen befassten Personen zu unterstützen. Dabei sind unter anderem deren Kenntnisse und Erfahrungen, der konkrete Nutzungskontext und die von der KI betroffenen Personen zu berücksichtigen.⁹³

Wo es sinnvoll und vertretbar ist, sollte die Einrichtung aber eine dienstliche KI-Lösung anbieten, da andernfalls doch die unbewerteten KI-Tools als „Schatten-KI“ von den Beschäftigten heimlich genutzt werden.

Hinweis für kirchliche Stellen

Kirchliche Stellen sollten den Mitarbeitenden die Chancen, aber auch die Risiken im dienstlichen Umgang mit KI-Anwendungen vermitteln. Sie sollten klare, verständliche und regelmäßig zu überprüfende Vorgaben dazu erlassen, welche KI-Anwendungen zu welchen dienstlichen Zwecken genutzt und welche personenbezogenen oder vertraulichen Daten dabei verarbeitet werden dürfen. Soweit sie KI-Systeme anbieten oder betreiben, müssen sie zudem die Anforderungen des Art. 4 KI-VO zur Förderung der KI-Kompetenz beachten.

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

Das Katholische Datenschutzzentrum nahm auch im Jahr 2025 regelmäßig an den Treffen mit den betrieblichen Datenschutzbeauftragten der Generalvikariate und der Diözesan-Caritasverbände teil, um den ständigen Austausch mit den betrieblichen Datenschutzbeauftragten fortzuführen. Im Verlauf des Berichtsjahres gab es mehrere Treffen, in denen relevante aktuelle und grundsätzliche Themen besprochen wurden. In Zusammenarbeit mit dem Katholischen Datenschutzzentrum wurden beispielsweise Fragen bezüglich der Kirchenvorstandswahlen diskutiert. Die Neufassung des KDG⁹⁴ war – wie im letzten Jahr – häufig Thema in den Sitzungen und auch die Auswirkungen des Digitalen Omnibus⁹⁵.

⁹³ Vgl. Orientierungshilfe der DSK vom 06.05.2024 zu KI und Datenschutz, Abschnitte 2.2 und 2.7.

⁹⁴ Siehe Abschnitt 1.3.1 dieses Jahresberichts

⁹⁵ Siehe Abschnitt 1.1.4 dieses Jahresberichts

2.7 ZenDiS und opencode.de

Im Dezember 2022 wurde das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS⁹⁶) gegründet. Bereits 2019 hatte das Bundesministerium des Innern und für Heimat (BMI) eine Marktanalyse in Auftrag gegeben, die kritische Abhängigkeiten von einzelnen Technologieanbietern aufzeigte. Diese Analyse zeigte die Notwendigkeit, die digitale Souveränität in der öffentlichen Verwaltung zu steigern.

Das ZenDiS soll als Kompetenz- und Servicezentrum fungieren und die Verfügbarkeit moderner, leistungsfähiger und skalierbarer Open-Source-Software-Lösungen (OSS-Lösungen) für die Verwaltung sicherstellen. Verfolgt wird ein ganzheitlicher Ansatz mit drei Säulen:

1. Strategische Koordination und Entwicklung
Stärken der digitalen Unabhängigkeit auf allen Verwaltungsebenen; Entwickeln und Bereitstellen von bedarfsgerechten und passgenauen OSS-Lösungen.
2. Förderung und Vernetzung
Beratung und Förderung der Vernetzung von OSS-Projekten in der Verwaltung; Gewährleistung eines zuverlässigen Betriebes der ZenDiS-Lösungen.
3. Verantwortung für Schlüsselprojekte
Verantwortung für zentrale Projekte wie die openCode-Plattform oder den souveränen Arbeitsplatz openDesk.

Eines der zentralen Projekte des ZenDiS ist die Plattform „openCode“. Dies ist die zentrale Plattform der öffentlichen Verwaltung zum Austausch von Open-Source-Software. Die Plattform steht unter dem Motto: Von der öffentlichen Hand, für die öffentliche Hand. Anfang 2025 arbeiten auf der openCode-Plattform mehr als 5.300 Nutzende an mehr als 2.200 Projekten.

Die Projektbandbreite auf der openCode-Plattform erstreckt sich vom webbasierten Open-Source-Helpdesk-System „Zammad“ bis hin zum „openDesk“.

Das Projekt „openDesk“⁹⁷ ist die Weiterentwicklung des „Souveränen Arbeitsplatzes“, einer Initiative des BMI. OpenDesk ist eine Office- und Kollaborationssuite, die speziell für die öffentliche Verwaltung entwickelt wurde. Der openDesk-Arbeitsplatz ist browserbasiert und nutzt marktgängige Open-Source-Komponenten. Laut ZenDiS wird bei der Entwicklung der Fokus auf Modularität, Herstellerunabhängigkeit und Austauschbarkeit gelegt, um möglichst flexibel zu bleiben.

Die Roadmap der in den nächsten Monaten zu erwartenden Funktionen und Updates zeigt, dass es sich um ein lebendiges Projekt handelt. Auch der Einsatz des openDesk bei z. B. dem Robert-Koch-Institut oder dem Bundesamt für Seeschifffahrt und Hydrografie belegt dessen praxistauglichen Ansatz.

⁹⁶ Die hier gemachten Ausführungen orientieren sich an den offiziellen Angaben. Vgl. Zentrum für Digitale Souveränität der Öffentlichen Verwaltung, Über das ZenDiS, abrufbar unter: <https://www.zendis.de>

⁹⁷ <https://opendesk.eu/>

2.8 Nicht-Benachrichtigung nach § 34 KDG

Immer wieder kommt es bei Verantwortlichen zu Unsicherheiten bezüglich der Benachrichtigungspflicht aus § 34 Abs. 1 KDG, wobei die Risikobewertung die häufigsten Probleme verursacht.

Neben der eigentlichen Risikoeinschätzung kann es aber auch zu Abwägungen durch Verantwortliche kommen, ob das eigentliche Ziel des § 34 Abs. 1 KDG, der Schutz der Rechte betroffener Personen, durch eine Benachrichtigung erreicht oder im Einzelfall durch eine Benachrichtigung sogar beeinträchtigt werden kann.

Diese Frage stellt sich beispielsweise in Fallkonstellationen, in denen Patienten einer stationären psychiatrischen Einrichtung von einer Datenschutzverletzung betroffen sind. Teil dieser Fallkonstellationen war ein meist (gesichertes) hohes Risiko für die Rechte und Freiheiten der betroffenen Personen durch die Datenschutzverletzung. Diese Risikoeinschätzung wurde zumeist stark durch die äußerst sensiblen (Behandlungs-)Daten der Personengruppe beeinflusst. In den durch das Katholische Datenschutzzentrum zu beurteilenden Fällen war es nicht selten, dass zumindest ein Teil dieser Betroffenenengruppe (starke) suizidale Tendenzen aufwies oder als Symptom ihrer Erkrankung an Wahnvorstellungen litt. Eine Benachrichtigung könnte daher, so zumindest die Befürchtung einiger Verantwortlicher in diesen Fällen, weitere Schäden bei den betroffenen Personen verursachen, da diese durch Kenntnis einer Datenschutzverletzung in ihren Tendenzen verstärkt werden könnten. In einigen Fällen gingen Verantwortliche von einer akuten Gefahr durch Selbstschädigung der betroffenen Personen aus.

Grundsätzlich kennt § 34 Abs. 3 KDG zwar Gründe dafür, dass die Benachrichtigungspflicht des § 34 Abs. 1 KDG entfällt. Keiner dieser Gründe sieht jedoch die (gesundheitliche) Verfassung der betroffenen Person vor. In den oben genannten Fallkonstellationen müssten Verantwortliche, zumindest nach dem Wortlaut des Gesetzes, betroffene Personen benachrichtigen, obwohl ein (gesichertes) Risiko durch die Benachrichtigung für deren Gesundheit bestünde. Denkbar ist es, das Gesetz nach seinem Sinn und Zweck, dem Schutz der Rechte und Freiheiten der betroffenen Personen, auszulegen und zu überprüfen, ob dieser Zweck durch eine Benachrichtigung erreicht oder gar verhindert würde. Es erscheint, insbesondere bei entsprechender ärztlicher Einschätzung, denkbar, dass betroffenen Personen mit einer Benachrichtigung in der oben genannten Fallkonstellation eher geschadet als genützt würde. Das eigentliche gesetzgeberische Ziel würde daher nicht mehr erreicht.

Das Katholische Datenschutzzentrum hält es in sehr spezifischen Fallkonstellationen für denkbar, dass die Benachrichtigungspflicht nach § 34 Abs. 1 KDG, durch Reduzierung der Norm auf ihr eigentliches Schutzziel, entfällt. Dies ist aber an sehr enge Voraussetzungen geknüpft. Beispielsweise muss stets eine Einzelfallprüfung vorgenommen werden, d. h., eine pauschale Betrachtung einer gesamten Personengruppe reicht nicht aus. Zu dieser Einzelfallbetrachtung gehört insbesondere auch, dass nicht nur Mutmaßungen über den Gesundheitszustand angestellt werden, sondern eine gesicherte ärztliche Begutachtung für die Abwägung zugrunde gelegt wird. Außerdem ist in solchen Fällen stets zu prüfen, ob sich das Risiko der beispielsweise

suizidalen Tendenzen, die durch eine Information der betroffenen Personen evtl. hervorgerufen würden, gut beherrschen ließe, wenn den Betroffenen ausreichende und schnelle fachliche Hilfsangebote zur Verfügung gestellt würden. Ein Hilfsangebot könnte beispielsweise eine ärztliche Begleitung der Information sein. Wenn diese Hilfestellungen zur Verfügung stehen, kann die Abwägung zugunsten der Informationspflicht ausfallen. In die Erwägungen mit einzubeziehen ist auch, ob eventuelle Folgen bei den Personen sogar noch stärker ausfielen, wenn ein möglicher Datenverlust von Dritten verbreitet wird.

Die Ausnahme darf insbesondere nicht dazu führen, dass Informations- und Transparenzpflichten der Verantwortlichen verkürzt werden. Eine bloß erschwerte Ausgangslage bei der Benachrichtigung kann nie ausreichen.

2.9 Spam-Anrufe eines „Datenschutzentrums Dortmund“

Im Frühjahr 2025 warnte das Katholische Datenschutzzentrum auf seiner Internetseite vor unseriösen Telefonanrufen angeblicher „Datenschützer“.

Anlass dafür war, dass sich verunsicherte Personen beim Katholischen Datenschutzzentrum und bei der Kommende Dortmund⁹⁸ meldeten, die Anrufe angeblicher „Datenschützer“ bekommen hatten. Hierbei handelte es sich um betrügerische Telefonanrufe, bei denen sich die Anrufer als Beschäftigte des „Datenschutzentrums Dortmund“ ausgaben. Teilweise wurde sogar für Rückfragen die Rufnummer der Kommende Dortmund genannt.

Das Katholische Datenschutzzentrum ging davon aus, dass bei den Anrufen das Vertrauen in Datenschutzinstitutionen ausgenutzt wurde, um persönliche Daten zu erschleichen und Zahlungen zu bewirken. Die Anrufer teilten z. B. mit, dass die eigenen Daten bei internationalen Glücksspielgesellschaften gelistet seien und versprachen, dass die Daten gelöscht würden.

Das Katholische Datenschutzzentrum betonte, dass es nicht ungefragt anruft und persönliche Daten abfragt und dass es nicht mit einer ausländischen Rufnummer anruft – wie es bei einigen Anrufen der Fall war.

Das KDSZ empfiehlt, in solchen Telefonaten keine Fragen zu beantworten und auf keinen Fall persönliche Informationen, insbesondere keine Bankverbindungsdaten, herauszugeben. Falls ersichtlich, sollte man sich die Rufnummer notieren und dann das Gespräch beenden. Außerdem sollte man sich bei Betrugsverdacht schnellstens an die örtliche Polizeidienststelle wenden. Darüber hinaus können Rufnummernmissbrauch und unerlaubte Telefonwerbung der Bundesnetzagentur gemeldet werden.⁹⁹

⁹⁸ In den Räumen der Kommende Dortmund hat das Katholische Datenschutzzentrum seinen Sitz, vgl. Abschnitt 3.2 des Jahresberichts.

⁹⁹ Formblätter für entsprechende Beschwerden werden auf deren Internetseite https://www.bundesnetzagentur.de/DE/Vportal/AnfragenBeschwerden/Beschwerde_Aerger/start.html angeboten.

2.10 Alternativen zu den großen sozialen Netzwerken nutzen

Die großen sozialen Netzwerke prägen für viele Menschen die tägliche Kommunikation und Informationsnutzung. Zugleich geben die Verbreitung von Desinformation und Hassrede sowie die Debatte über Veränderungen bei der Faktenprüfung und Inhaltsmoderation Anlass zur Sorge. Vor diesem Hintergrund warb beispielsweise Anfang 2025 der damalige Leiter der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz, Prof. Andreas Büsch, für eine selbstkritische Überprüfung durch die kirchlichen Stellen, wen sie mit ihren Auftritten in den sozialen Medien erreichen.¹⁰⁰ Auch wenn eine Präsenz in den sozialen Medien wichtig sei, zeige ein realistischer Blick auf die Followerzahlen, dass es sich hier eher um kirchliche Bubbles handle und nicht automatisch eine größere Anzahl von Menschen erreicht werde.

Das Katholische Datenschutzzentrum möchte in diesem Zusammenhang darauf hinweisen, dass bei diesen Überlegungen zur Nutzung der sozialen Netzwerke auch datenschutzrechtliche Fragestellungen berücksichtigt werden müssen. Vor der Einrichtung oder Fortführung eines Auftritts ist insbesondere zu prüfen, welche personenbezogenen Daten durch den Plattformbetrieb verarbeitet werden, auf welcher Rechtsgrundlage dies geschieht, wie die Verantwortlichkeiten verteilt sind, ob die betroffenen Personen hinreichend transparent informiert werden und ob personenbezogene Daten in Drittländer übermittelt werden.¹⁰¹

Das Katholische Datenschutzzentrum begrüßt daher ausdrücklich die Aktivitäten des Katholischen Datenschutzzentrums Bayern, das sich die Förderung dezentraler sozialer Netzwerke zum Ziel gesetzt hat. Das KDSZ Bayern betreibt unter der Domain katholisch.social mehrere Dienste des Fediverse, darunter Mastodon, PeerTube, Pixelfed und Friendica. Das Angebot zeigt konkret, wie kirchliche Akteure ihre Kommunikation um offene und dezentrale Alternativen zu den großen kommerziellen Plattformen ergänzen können.¹⁰²



„Gerade im medizinischen Sektor sind aufgrund besonders sensibler personenbezogener Daten und Verarbeitungsprozesse streng geregelte Zugriffsberechtigungen erforderlich.“

2.11 Einsicht in Patientenakten durch Mitarbeitende

Gerade im medizinischen Sektor sind aufgrund besonders sensibler personenbezogener Daten und Verarbeitungsprozesse streng geregelte Zugriffsberechtigungen erforderlich. Einsichtnahmen in Patientenakten oder in die Behandlungsdokumentation sind vor allem wegen der besonderen Sensibilität der Daten und des geschärften Bewusstseins der betroffenen Personen wiederholt Gegenstand von Beschwerden gewesen. In den meisten Fällen kann der Verantwortliche Zugriffe

¹⁰⁰ Artikel „Präsenz kirchlicher Akteure auf Facebook zunehmend zwiespältig“ von Felix Neumann vom 08.01.2025 auf katholisch.de

¹⁰¹ An dieser Stelle soll darauf hingewiesen werden, dass gerade bei Facebook-Fanpages die rechtliche Beurteilung weiterhin nicht abschließend geklärt ist. Gegen das Urteil des Verwaltungsgerichts Köln vom 17.07.2025, mit dem der gegenüber dem Presse- und Informationsamt der Bundesregierung erlassene Untersagungsbescheid der Bundesbeauftragten für den Datenschutz und Informationsfreiheit aufgehoben wurde, hat diese Berufung eingelegt. Siehe Abschnitt 1.2.1 des Jahresberichts.

¹⁰² Internetauftritt des Katholischen Datenschutzzentrums Bayern: <https://kdsz.bayern/social-media/>

durch Mitarbeitende anhand seiner Berechtigungs- und Behandlungskonzepte plausibel erklären bzw. rechtfertigen.

Im Berichtszeitraum gab es jedoch auch Meldungen über Datenschutzverletzungen, bei denen sich der Zugriff von Mitarbeitenden des Verantwortlichen auf Patientenakten nicht rechtfertigen ließ. Beispielsweise kam es zu Zugriffen auf Akten von Personen aus dem Bekanntenkreis der Mitarbeitenden oder von Kolleginnen und Kollegen, die in der Einrichtung behandelt wurden. In solchen Konstellationen kann das Verhalten der Mitarbeitenden einen sogenannten Mitarbeiterexzess¹⁰³ darstellen, der dem Verantwortlichen unter Umständen nicht zuzurechnen ist. Grundsätzlich handeln Mitarbeitende bei Zugriffen auf dienstliche Systeme und der dabei erfolgenden Verarbeitung personenbezogener Daten nur dann im Rahmen ihrer Tätigkeit und damit für den Verantwortlichen, wenn diese Verarbeitung Teil ihrer dienstlichen Aufgaben ist.

Wird eine solche Verarbeitung zu eigenen Zwecken des Mitarbeitenden festgestellt, kann sie dem Verantwortlichen nur dann entgegengehalten werden, wenn dieser seiner Organisationspflicht zur Verhinderung solcher unberechtigten Zugriffe nicht ordnungsgemäß nachgekommen ist. Das bedeutet konkret, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, um solche unrechtmäßigen Verarbeitungen durch Mitarbeitende möglichst zu verhindern. Dies kann beispielsweise durch Schulungen der Mitarbeitenden, Dienstanweisungen oder entsprechende Zugriffsbeschränkungen in den jeweiligen Informationssystemen erfolgen.

Der Nachweis ausreichender präventiver Maßnahmen gelang nicht in jedem Fall. In allen Fällen konnten Verbesserungen allerdings schnell umgesetzt werden.

Hinweis für kirchliche Einrichtungen

Verantwortliche sollten Berechtigungskonzepte regelmäßig auf Aktualität und Aufgabenbezug prüfen, Zugriffsrechte konsequent entsprechend den dienstlichen Aufgaben vergeben sowie durch Schulungen, Dienstanweisungen und Zugriffsbeschränkungen unrechtmäßige Verarbeitungen möglichst verhindern. Zudem sollten die getroffenen technischen und organisatorischen Maßnahmen nachvollziehbar dokumentiert werden, um deren Nachweis im Anlassfall führen zu können. Außerdem sollten die getroffenen Maßnahmen regelmäßig überprüft werden.

¹⁰³ In einem solchen Fall ist das KDSZ für die Verarbeitung des Mitarbeitenden nicht zuständig. Das Verhalten von Privatpersonen außerhalb ihrer Tätigkeit bei kirchlichen Verantwortlichen kann nur von den zuständigen staatlichen Aufsichtsinstanzen beurteilt werden.



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

Kapitel 6 des Gesetzes über den Kirchlichen Datenschutz befasst sich mit der unabhängigen Datenschutzaufsicht (§§ 42 ff. KDG). Hiernach richtet jeder Diözesanbischof für den Bereich seiner Diözese eine Datenschutzaufsicht als unabhängige kirchliche Behörde ein (§ 42 Abs. 1 KDG). Grundlage für diese Möglichkeit bildet Art. 91 Abs. 2 DSGVO, der zur Überwachung der Einhaltung des kirchlichen Datenschutzrechts die Möglichkeit einer eigenen kirchlichen Datenschutzaufsicht vorsieht.

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

3.1 Der gemeinsame Diözesandatenschutzbeauftragte

Der Diözesandatenschutzbeauftragte 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.¹⁰⁴ Im Zuständigkeitsgebiet leben mehr als 5,8 Millionen Menschen römisch-katholischen Glaubens (Stand 2024).

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands¹⁰⁵ (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.¹⁰⁶

¹⁰⁴ 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.

¹⁰⁵ Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter“.

¹⁰⁶ Für eine ausführliche Darstellung der Aufgaben der Datenschutzaufsicht siehe Abschnitt 3.5 des Jahresberichts 2021.

Der Diözesandatenschutzbeauftragte, sein Stellvertreter und die Mitarbeiterinnen 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.

Wer der Ansicht ist, dass bei der Verarbeitung von personenbezogenen Daten durch eine (katholische) kirchliche Stelle datenschutzrechtliche Regelungen verletzt worden sind, kann sich gemäß § 48 KDG an die Datenschutzaufsicht wenden. Wichtig ist dabei das Benachteiligungsverbot des § 48 Abs. 3 KDG: „Niemand darf gemäßregelt oder benachteiligt werden, weil er sich im Sinne des Abs. 1 an die Datenschutzaufsicht gewendet hat.“

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.



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

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.¹⁰⁷ 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

¹⁰⁷ 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.

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.¹⁰⁸

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 KDG¹⁰⁹ 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 2025 sieht der Haushaltsplan für das Katholische Datenschutzzentrum ein Volumen in Höhe von 1.239.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben vor. Für das Folgejahr 2026 steigt das genehmigte Budget leicht auf 1.276.000 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.¹¹⁰

¹⁰⁸ 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.

¹⁰⁹ Bisherige Rechtslage bis 01.03.2026. Im novellierten Gesetz ist die Regelung in § 42 Abs. 5 KDG zu finden.

¹¹⁰ Ausführlich zum Leben und Wirken des hl. Ivo: Michael Streck / Annette Rieck, St. Ivo (1247–1303) – Schutzpatron der Richter und Anwälte, 2007; Artikel „Ivo Hélor“ auf Wikipedia (https://de.wikipedia.org/wiki/Ivo_Hélor). In dem Beitrag bei Wikipedia wird auch erwähnt, dass der hl. Ivo das Siegel des Katholischen Datenschutzzentrums ziert.

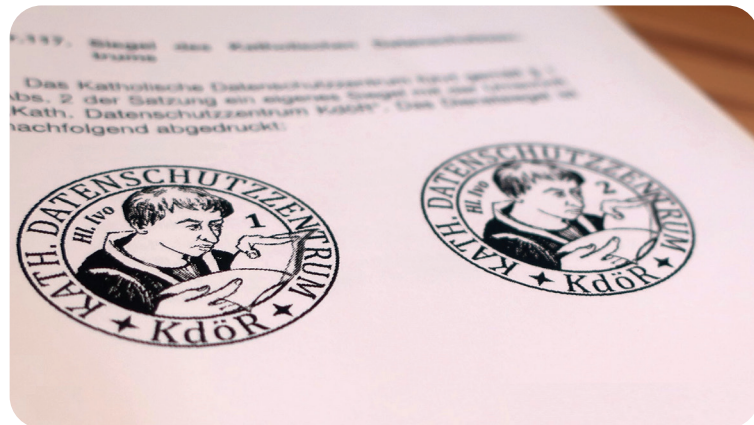


Abb. 7: Darstellung des Siegels des KDSZ im Amtsblatt der Erzdiözese Paderborn
(Bild: Katholisches Datenschutzzentrum)

3.4 Öffentlichkeitsarbeit

Das Katholische Datenschutzzentrum engagiert sich auf verschiedene Arten, um das Bewusstsein für den Datenschutz in der katholischen Kirche zu fördern und über seine Tätigkeiten zu informieren. Es informiert kirchliche Einrichtungen, betroffene Personen und die interessierte Öffentlichkeit. Dies umfasst u. a. Veröffentlichungen auf der Internetseite des Katholischen Datenschutzzentrums und die Beteiligung an Veranstaltungen und Fortbildungen, die sich auf Datenschutz und Informationstechnologie beziehen.

Im Jahr 2025 war das Katholische Datenschutzzentrum u. a. als Referent auf einem Fachtag zum Thema „Den Überblick im Technikdschungel behalten“ vertreten. Der Fachtag richtete sich an Träger, Dienste und Einrichtungen aus den Bereichen Altenhilfe, Hospiz und Sozialstationen. Es gab Vorträge zur Telematikinfrastruktur, zum Einsatz von künstlicher Intelligenz und zu ethischen Fragen im Zusammenhang mit technischen Entwicklungen – und natürlich zum Datenschutz, der überall eine Rolle spielt. Auch hielt das Katholische Datenschutzzentrum einen Vortrag zu den aktuellen Grundlagen und Herausforderungen des kirchlichen Datenschutzes im Rahmen eines Treffens der Mitarbeitervertretungen aus Einrichtungen von Caritas und Malteser. Daneben waren Vertreterinnen und Vertreter des Katholischen Datenschutzzentrums bei vielen Veranstaltungen und anderen Terminen für die kirchlichen Einrichtungen ansprechbar, um einen kontinuierlichen Dialog mit den kirchlichen Einrichtungen fortzuführen.

Die Internetseite www.katholisches-datenschutzzentrum.de des KDSZ ist eine wichtige Quelle für umfangreiche Informationen bezüglich des kirchlichen Datenschutzes und der Arbeit der Datenschutzaufsicht. Dort findet man alles von relevanten Gesetzestexten für die jeweilige (Erz-)Diözese bis hin zu Mustern und Vorlagen. Darüber hinaus werden regelmäßig Beiträge zu aktuellen Datenschutzthemen und der jährlich veröffentlichte Tätigkeitsbericht des Katholischen Datenschutzzentrums bereitgestellt.

Nach knapp 10 Jahren hat das Katholische Datenschutzzentrum im Berichtszeitraum auch einen Relaunch seiner Internetseite vorbereitet.

Der Wechsel der Seite konnte im Januar 2026 nach umfangreichen Vorarbeiten erfolgreich durchgeführt werden. Ziel des Katholischen Datenschutzzentrums ist es, die umfangreichen Informationen zum kirchlichen Datenschutz und zur Tätigkeit des KDSZ in bewährter Form, aber mit einem moderneren Aussehen anzubieten.

3.5 Verfahren vor dem Interdiözesanen Datenschutzgericht und dem Datenschutzgericht der Deutschen Bischofskonferenz

Im Berichtszeitraum sind drei erstinstanzliche Verfahren aus 2025 beim Interdiözesanen Datenschutzgericht (IDSG) und zwei zweitinstanzliche Verfahren vor dem Datenschutzgericht der Deutschen Bischofskonferenz (DSG-DBK), bei denen das Katholische Datenschutzzentrum als Antragsgegner oder Beteiligter geführt wird, anhängig. Die Verfahren laufen noch. In den teilweise noch anhängigen Verfahren aus den vorherigen Jahren (seit 2022) stehen die Entscheidungen des IDSG noch aus, die Entscheidung eines Verfahrens vor dem DSG-DBK steht ebenfalls noch aus.

Die Entscheidungen der 1. und 2. Instanz werden regelmäßig auf der Internetseite der Deutschen Bischofskonferenz veröffentlicht.¹¹¹ Die Verfahren vor den kirchlichen Gerichten in Datenschutzangelegenheiten richten sich nach der Kirchlichen Datenschutzgerichtsordnung (KDSGO)¹¹².

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.

Zweimal jährlich findet auf Einladung des DSK-Vorsitzes ein Austausch zwischen Mitgliedern der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder und spezifischen Datenschutzaufsichtsbehörden – den Datenschutzaufsichten aus Kirche und Rundfunk – statt.¹¹³ Unabhängig von diesen regelmäßigen Treffen tauschen sich die Datenschutzaufsichten untereinander regelmäßig aus.

Die katholischen Datenschutzaufsichten sind auch in verschiedenen fachspezifischen Arbeitskreisen (AK) der Datenschutzkonferenz präsent, die wichtige Entscheidungen vorbereiten und nach einer einheitli-

¹¹¹ <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>

¹¹² Siehe hierzu Abschnitt 1.3.2 im Jahresbericht 2018 und Abschnitt 2.5.1 im Jahresbericht 2019.

¹¹³ Protokolle stehen auf der Internetseite der DSK zur Verfügung: <https://www.datenschutzkonferenz-online.de/protokolle.html>

chen Anwendung des europäischen und nationalen Datenschutzrechts streben. Das KDSZ vertritt die katholischen Datenschutzaufsichten weiterhin im AK Grundsatz und seit 2025 auch im AK Künstliche Intelligenz. Der Arbeitskreis Künstliche Intelligenz wurde im Berichtsjahr neu gegründet und das KDSZ nimmt seit der ersten konstituierenden Sitzung im Januar 2025 an dieser regelmäßig tagenden Runde teil.

An dem seit 2024 stattfindenden Informationsaustausch der IT-Labore aller Datenschutzaufsichten in Deutschland hat das Katholische Datenschutzzentrum auch im Berichtsjahr wieder teilgenommen.¹¹⁴ Themen der Treffen in 2025 waren u. a. neue Trackingmethoden, forensische Laborarbeit, Hilfsmittel bei Laborprüfungen und die Automatisierung von Internetseitenprüfungen. Der Austausch der IT-Labore wird weitergeführt.

¹¹⁴ Ausführlich zum Austausch der IT-Labore siehe Abschnitt 3.6 des Jahresberichts 2024.

4 Dokumentation – 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 wahrgenommen¹¹⁵.

Für den Bereich der Ordensgemeinschaften päpstlichen Rechts hat die Deutsche Ordensobernkongferenz, der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung der Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.¹¹⁶

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

¹¹⁵ Siehe Abschnitt 3.1 des Jahresberichts

¹¹⁶ Siehe <https://datenschutz.orden.de/>.

eingeladen.¹¹⁷ Zur leichteren Erreichbarkeit und besseren Koordination ihrer Zusammenarbeit hat die Konferenz eine „Geschäftsstelle“ eingerichtet, die sich beim Katholischen Datenschutzzentrum in Dortmund befindet.



¹¹⁷ Ausführlich zur Konferenz der Diözesandatenschutzbeauftragten siehe Abschnitt 4.1.3 im Jahresbericht 2021.

Abkürzungsverzeichnis

AK	Arbeitskreis
AktAuskG	Diözesangesetz zur Regelung von Einsichts- und Auskunftsrechten
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BCM	Business Continuity Management (Betriebskontinuitätsmanagement)
BfD EKD	Der Beauftragte für den Datenschutz der EKD
BfDI	Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz; Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen
BVerfG	Bundesverfassungsgericht
CCB	Centre for Cybersecurity Belgium (belgische Cybersicherheitsbehörde)
CIC	Codex Iuris Canonici
DBK	Deutsche Bischofskonferenz
DDSB	Diözesandatenschutzbeauftragte/r
DOK	Deutsche Ordensobernkonferenz
DSFA	Datenschutz-Folgenabschätzung
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
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA	Europäischer Datenschutzausschuss (englisch EDPB – European Data Protection Board)
EKD	Evangelische Kirche in Deutschland
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum



IDSG	Interdiözesanes Datenschutzgericht – 1. Instanz
ISMS	Informationssicherheitsmanagementsystem
KAO	Kirchliche Archivordnung, Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDG-VDD	KDG für den Verband der Diözesen Deutschlands
KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
KI	künstliche Intelligenz
KIS	Krankenhausinformationssystem
KI-VO	Verordnung über künstliche Intelligenz (KI-Verordnung)
KMU	kleine und mittlere Unternehmen
KRITIS	Kritische Infrastruktur
LfD	Landesbeauftragte/r für Datenschutz
LG	Landgericht
MFA	Multi-Faktor-Authentisierung
MAV	Mitarbeitervertretung
MStV	Medienstaatsvertrag
NIS	Sicherheit der Netz- und Informationssysteme
OLG	Oberlandesgericht
OSS	Open-Source-Software
OWiG	Gesetz über Ordnungswidrigkeiten
RTW	Rettungswagen
SGB	Sozialgesetzbuch
UAK	Unabhängige Aufarbeitungskommissionen
UBSKM	Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs
UWG	Gesetz gegen den unlauteren Wettbewerb
VDD	Verband der Diözesen Deutschlands
VG	Verwaltungsgericht
VO	Verordnung
VVT	Verzeichnis von Verarbeitungstätigkeiten
ZenDiS	Zentrum für Digitale Souveränität der Öffentlichen Verwaltung



HI. 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