Kath. Datenschutzzentrum
Frankfurt/M.

# Tätigkeitsbericht 2025

2026
2027
2028
2029
2030
2031

Kath. Datenschutzzentrum
Frankfurt/M.

# Tätigkeitsbericht 2025

Herausgegeben von der
Diözesandatenschutzbeauftragten für die (Erz-)Bistümer Freiburg, Fulda,
Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Kath. Datenschutzzentrum Frankfurt/M. KdöR
Roßmarkt 23
60311 Frankfurt/M.
Tel.: 069 / 58 99 755 10
Fax: 069 / 58 99 755 11
E-Mail: info@kdsz-ffm.de
www.kdsz-ffm.de

Aus redaktionellen Gründen wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen an einigen Stellen verzichtet. Die verkürzte Verwendung gilt im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter und enthält keine Wertung.
Bildnachweise: Titel-/Rückseite: A. Hoßfeld, KI-generiert mit Adobe Firefly,
S. 6, 39 u. 41: Olaf J. Lutz, KDSZ Ffm, S. 22, 24, 27: pikisuperstar/ Magnific, S. 40: HBDI/LfDI RLP

**Inhaltsverzeichnis** ..... 3

**Vorwort** ..... 5

**1 Aus der Datenschutzaufsicht** ..... 6

**2 Entwicklung des Datenschutzes** ..... 7
2.1 Staatliche Gesetzgebung ..... 8
2.1.1 Data Act ist seit Herbst 2025 anwendbar ..... 8
2.1.2 Digital Omnibus ..... 8
2.1.3 Entwurf für ein „KI-Marktüberwachungs- und Innovationsförderungsgesetz“ vorgelegt ..... 9
2.1.4 Orientierungshilfen der Datenschutzkonferenz ..... 10
2.1.5 Leitlinie des EDPS zum Risikomanagement von KI-Systemen ..... 11
2.1.6 Faktenblatt des Europäischen Gerichtshofs zum Schutz personenbezogener Daten ..... 11
2.2 Kirchliche Gesetzgebung ..... 12
2.2.1 Datenschutzhinweise für neue Kirchengemeinden im Erzbistum Freiburg ..... 12
2.2.2 Neue Betreuungsvertragsbedingungen und Datenschutzhinweise für katholische Kitas im Bistum Fulda ..... 13
2.2.3 Umfangreiches Regelwerk zum IT-Einsatz im Bistum Speyer ..... 14
2.2.4 Bistum Speyer regelt Umsetzung des Hinweisgeberschutzgesetzes ..... 14
2.2.5 Einsichts- und Auskunftsrechte von Betroffenen sexuellen Missbrauchs in Sachakten des Bistums Trier geregelt ..... 15
2.3 Ausgewählte Rechtsprechung staatlicher Gerichte ..... 17
2.3.1 Auf den Charakter kommt es an ..... 17
2.3.2 Sorge und Ärger als immaterieller Schaden ..... 18
2.3.3 Keine Entschädigung bei rein hypothetischem Risiko ..... 18
2.3.4 Keine zu hohen Anforderungen an Darlegung eines immateriellen Schadens ..... 19
2.3.5 Verspätete Auskunft begründet keinen immateriellen Schadensersatzanspruch ..... 20
2.3.6 Verzicht auf Auskunftsrecht in arbeitsgerichtlichem Vergleich möglich ..... 21
2.3.7 Kirchliche oder staatliche Gerichtsbarkeit – manchmal keine leichte Abgrenzung ..... 22
2.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte ..... 23
2.4.1 Meldedaten für die Abo-Gewinnung ..... 23
2.4.2 Eigen-Verordnung keine Grundlage für Aktenvernichtung ..... 23
2.4.3 Handschriftliches Spendenverzeichnis unterfällt Datenschutz ..... 25
2.4.4 Einsichtnahme in Mitarbeiter-Account ..... 26

**3 Schwerpunkte der Tätigkeiten im Berichtszeitraum** ..... 28
3.1 Datenschutzverletzungen ..... 28
3.1.1 Ist der Mailversand ohne BCC in einer Kita quasi „der Standard“? ..... 29
3.1.2 „Stay Informed“, aber nicht alle Informationen sind auch für alle gedacht! ..... 29
3.1.3 Keine Schlüsselrückgabe trotz Beendigung des Beschäftigungsverhältnisses ..... 30
3.2 Beschwerden ..... 31
3.2.1 TikTok-Challenge führt zu „verschlüsseltem“ Toilettenzugang ..... 31
3.2.2 Kein Recht auf Auskunft um jeden Preis ..... 32
3.3 Anfragen ..... 32
3.4 Gerichtsverfahren ..... 33
3.5 Prüfungen ..... 34
3.6 Umfrage zum Umgang mit Datenschutzverletzungen ..... 35

**4 Veranstaltungen und Öffentlichkeitsarbeit** ..... 39

**5 Vernetzung mit anderen Datenschutzaufsichten** ..... 41

**6 Ausblick** ..... 42

**7 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland** ..... 43

## KI lässt Beschwerdewelle schwappen

Der vorliegende Tätigkeitsbericht des Kath. Datenschutzzentrums Frankfurt/M. gibt einen Einblick in die gesetzlichen Neuerungen des Berichtsjahrs 2025 sowohl im staatlichen wie auch im kirchlichen Datenschutz. Zudem werden die Kernaufgaben der Datenschutzaufsicht dargestellt: Bearbeitung von Beschwerden, Beurteilung von Datenschutzverletzungen, Beratung bei konkreten Fragestellungen, Überwachung der Einhaltung der gesetzlichen Vorgaben durch anlasslose und anlassbezogene Prüfungen und nicht zuletzt Sensibilisierung der Verantwortlichen in Veranstaltungen und durch Hinweise und Handreichungen.

Eine große, für alle Datenschutzaufsichten gleichermaßen herausfordernde Aufgabe, ist die Bewältigung der eingehenden Beschwerden, deren Zahl im Berichtsjahr stark zugenommen hat. Die Gründe dafür sind mannigfaltig, neben einem erhöhten Bewusstsein für den Schutz personenbezogener Daten und den sich daraus ergebenden Betroffenenrechten, spielt sicher die KI-gestützte Formulierung von Beschwerden auch eine Rolle. Diese steigert zwar die Anzahl, nicht aber zwingend die inhaltliche Qualität der Beschwerden.

Dabei zeigt sich bedauerlicherweise auch, dass der Datenschutz vermehrt als Vehikel zur Durchsetzung anderweitiger Forderungen benutzt wird, denn einem Teil der Beschwerden ist die datenschutzrechtliche Komponente nicht oder nicht direkt zu entnehmen. Datenschutz wird dadurch instrumentalisiert, was bedeutet, dass die Steigerung der Zahl der Beschwerden nicht unbedingt auf eine erhöhte Datenschutzsensibilität zurückzuführen ist. In den Datenschutzaufsichten werden so Kapazitäten gebunden und die Bearbeitung tatsächlicher datenschutzrechtlicher Belange verzögert sich möglicherweise.

Es ist und bleibt die zentrale Aufgabe des Kath. Datenschutzzentrums Frankfurt/M. in seinem Zuständigkeitsbereich „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten bei der Verarbeitung dieser Daten zu schützen“ – was vor allem beratend und nur wenn erforderlich repressiv geschieht.

Die rechtsmissbräuchliche Nutzung gesetzlich festgeschriebener Datenschutzrechte hemmt nicht nur eine zügige und effiziente Arbeitsweise in der Aufsichtsbehörde, sondern sie diskreditiert zudem den Datenschutz zum bloßen Werkzeug. In einer Zeit zunehmenden Datenmissbrauchs eine kontraproduktive Entwicklung, der es entgegenzuhalten gilt.

An dieser Stelle danke ich den Kolleginnen und Kollegen im Kath. Datenschutzzentrum Frankfurt/M. herzlich, die an der Erstellung dieses Berichts mitgewirkt haben.

Ursula Becker-Rathmair
Diözesandatenschutzbeauftragte
und Leiterin des Kath. Datenschutzzentrums Frankfurt/M.

# 1 Aus der Datenschutzaufsicht

Kontakte pflegen und aufrechterhalten, Besucher empfangen und im Austausch Neues erfahren, gemeinsam mit anderen Datenschutzaufsichten Projekte durchführen und dadurch Synergien ausschöpfen – so lässt sich die seit vielen Jahren gelebte Arbeitsweise des Kath. Datenschutzzentrums Frankfurt/M. kurz zusammenfassen.

Neben den Besuchen der Generalvikare „unserer“ (Erz-)Bistümer, den regelmäßig stattfindenden Treffen mit Vertretern verschiedenster Datenschutzaufsichten und der Teilnahme der Mitarbeitenden an diversen Datenschutz- und Weiterbildungsveranstaltungen gehören auch die vom Kath. Datenschutzzentrum Frankfurt/M. meist im Herbst angebotenen Informations- und Fortbildungsveranstaltungen zum festen jährlichen Programm (mehr dazu in den Kapiteln 4 und 5).

> **„Die unabhängige Wahrnehmung aufsichtsrechtlicher Verpflichtungen im Datenschutz der katholischen Kirche ist eine wichtige vertrauensbildende Aufgabe. Sie hat für mich glaubwürdigkeitsfördernde Bedeutung.“**

Im Februar des Berichtsjahres durfte sich das Team des Kath. Datenschutzzentrums Frankfurt/M. über einen besonderen Besuch freuen: Bischof Dr. Georg Bätzing (Limburg), der zu diesem Zeitpunkt Vorsitzender der Deutschen Bischofskonferenz war, kam zu einem Besuch nach Frankfurt. Er besichtigte die im Jahr 2023 bezogenen Räumlichkeiten am Roßmarkt im Herzen der Stadt und tauschte sich mit dem Team inhaltlich über zahlreiche Themen aus. In ungezwungener Atmosphäre bei Kaffee und Kuchen wurde unter anderem über die Wahrnehmung des Datenschutzes und dessen Umsetzung in allen Bereichen des kirchlichen Lebens gesprochen.

**Bischof Dr. Georg Bätzing zu Besuch im Kath. Datenschutzzentrum Frankfurt/M.**

„Die unabhängige Wahrnehmung aufsichtsrechtlicher Verpflichtungen im Datenschutz der katholischen Kirche ist eine wichtige vertrauensbildende Aufgabe. Sie hat für mich glaubwürdigkeitsfördernde Bedeutung“, sagte Bätzing.

Für das gesamte Team des Kath. Datenschutzzentrums Frankfurt/M. waren sowohl der Besuch von Bischof Dr. Bätzing als auch sein im Gespräch deutlich erkennbares Interesse für datenschutzrechtliche Themen eine besondere Wertschätzung.

# 2 Entwicklung des Datenschutzes

Fortschreitende Digitalisierung im Allgemeinen und die Einbindung KI-gestützter Funktionen an mittlerweile vielen Stellen des öffentlichen Lebens waren auch im Jahr 2025 weiterhin deutliche Merkmale dafür, dass Datenschutz und Datensicherheit wechselseitig ohneeinander nicht mehr denkbar sind.

Dies zeigt sich auch in der staatlichen datenschutzrechtlichen Gesetzgebung und vor allem in den Hinweisen, Handreichungen und anderen Hilfestellungen, die zu diesen Themen erstellt wurden – beispielhaft sind hier die Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (DSK) zu nennen (siehe Punkt 2.1.4).

Im Bereich der Datenschutzgesetzgebung sowohl der evangelischen als auch der katholischen Kirche hat sich 2025 Entscheidendes getan:

Die Überarbeitung des „Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)“ wurde – nachdem sie im November 2024 beschlossen worden war – im Januar des aktuellen Berichtszeitraums im Amtsblatt der EKD veröffentlicht und ist somit in Kraft getreten.

Im Ausblick des Tätigkeitsberichts des Jahres 2024 wurde bereits auf die Veröffentlichung des ersten Entwurfs der novellierten Fassungen des „Gesetz über den Kirchlichen Datenschutz (KDG)“ und der „Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)“ hingewiesen. Nach weiteren Überarbeitungen sind beide Novellierungen im November 2025 vom Verband der Diözesen Deutschlands (VDD) beschlossen worden. Die Veröffentlichungen in den jeweiligen Amtsblättern der Diözesen werden sich im Jahr 2026 anschließen, über das Inkrafttreten und die sich aus der Novellierung ergebenden Änderungen wird also im Tätigkeitsbericht für das Jahr 2026 zu berichten sein.

Doch auch an anderen Stellen gibt es im kirchlichen Bereich datenschutzrechtliche Entwicklungen, die möglicherweise erst auf den zweiten Blick sichtbar werden: Beispielhaft seien hier zum einen die umfassenden Änderungen, die sich durch den Zusammenschluss von Kirchengemeinden ergeben, genannt, die sich durchaus auch auf den Bereich des Datenschutzes auswirken. Im Erzbistum Freiburg beispielsweise trägt man dieser Tatsache durch die Herausgabe von FAQs zum Thema „Datenschutzhinweise für neue Kirchengemeinden“ Rechnung (siehe Kapitel 2.2.1).

Zum anderen sei darüber hinaus die Schließung von kirchlichen Krankenhäusern erwähnt, ein weiteres Thema, das in diesem Kontext nicht vernachlässigt werden sollte. Große Mengen besonderer Kategorien personenbezogener Daten gilt es hier weiterzugeben, zu archivieren oder zu vernichten, und das häufig sowohl in analoger als auch in digitaler Form.

## 2.1 Staatliche Gesetzgebung

### *2.1.1 Data Act ist seit Herbst 2025 anwendbar*

Die am 11. Januar 2024 in Kraft getretene „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act)“ ist seit dem 12. September 2025 EU-weit direkt anwendbares Recht geworden. Mit dieser Verordnung werden Unternehmen zu neuen Transparenz-, Zugänglichkeits- und Vertragsanforderungen rund um die Nutzung und Weitergabe von Daten verpflichtet. Dabei geht es nicht nur um die Hersteller vernetzter Produkte (wie Fahrzeuge oder Konsumgüter), sondern auch um Anbieter verbundener digitaler Dienste oder Cloud- und Plattformdienste.

Durch den Data Act sollen zum einen Verbraucher vollständige Zugangs- und Nutzungsrechte für ihre Daten erhalten, zum anderen sollen auch Verbesserungen für Unternehmen erzielt werden, die besseren Zugang zu von Geräten für unternehmerische Zwecke gesammelten Daten erhalten.

Von nun an gelten Datenschutzgrundverordnung (DSGVO) und Data Act parallel, was zwangsläufig zu Überschneidungen führen kann. Dabei ist zu beachten, dass der Data Act den Schutz personenbezogener Daten, wie er durch die DSGVO gewährleistet wird, unberührt lässt. Soweit es zu Kollisionen kommt, tritt der Data Act hinter der Grundverordnung zurück (Art. 1 Abs. 5 Data Act).

### *2.1.2 Digital Omnibus*

Im November 2025 hat die Europäische Kommission einen Vorschlag für ein Digital-Omnibus-Paket veröffentlicht. Dieser Vorschlag ist Teil der Vereinfachungsagenda, mit der bestehende Vorschriften zu den Bereichen Künstliche Intelligenz (KI), Cybersicherheit und Verarbeitung von Daten vereinfacht werden sollen. Omnibusverfahren werden dann gewählt, wenn mehrere bestehende Gesetze in einem Zug geändert bzw. miteinander kompatibel gemacht werden sollen.

Das vorliegende Paket besteht aus zwei Verordnungen, dem Digital Omnibus und dem Digital Omnibus on AI. Während es im Digital Omnibus on AI ausschließlich um Anpassungen in der KI-Verordnung geht, sieht der Digital Omnibus Änderungen im Data Act, in der DSGVO und in Cybersicherheitsgesetzen (zum Beispiel in der NIS-2-Richtlinie) vor.

Deutliche Kritik an den vorgeschlagenen Änderungen in der DSGVO kommt von verschiedenen Datenschützern vor allem bezüglich der Anpassung der Begrifflichkeiten von Personenbezug und Pseudonymisierung, eine Absenkung des Schutzniveaus der DSGVO wird dadurch befürchtet.

Der Vorschlag muss nun das europäische Gesetzgebungsverfahren durchlaufen, weitere inhaltliche Änderungen oder Anpassungen sind folglich noch möglich. Welchen Weg das Verfahren im weiteren Verlauf eingeschlagen haben wird, darüber wird der nächste Tätigkeitsbericht informieren.

### *2.1.3 Entwurf für ein „KI-Marktüberwachungs- und Innovationsförderungsgesetz“ vorgelegt*

Der im Mai 2024 vom Rat der 27 Mitgliedsstaaten der Europäischen Union verabschiedete AI-Act (KI-Verordnung) hätte bis August 2025 in nationales Recht umgewandelt werden sollen. Deutschland hat diese Frist wegen des Regierungswechsels im Frühjahr 2025 verpasst, sodass am 12. September 2025 ein neuer – an den vorherigen aus dem Dezember 2024 anknüpfender – Referentenentwurf für ein „KI-Marktüberwachungs- und Innovationsförderungsgesetz“ (KI-MIG) vorgelegt wurde.

Bezüglich der Aufsichts- und Behördenstruktur sieht der Referentenentwurf vor, dass bestehende Strukturen genutzt und die Bundesnetzagentur als zentrale Instanz eingesetzt werden soll. Dort soll ein zentrales Koordinierungs- und Kompetenzzentrum (KoKIVO) eingerichtet werden, das Koordinierungsstelle für die Zusammenarbeit aller zuständigen Marktüberwachungsbehörden ist.

Eine Unabhängige KI-Marktüberwachungskammer (UKIM) speziell für KI-Hochrisikosysteme, die von Strafverfolgungs-, Einwanderungs- oder Asylbehörden genutzt werden sollen, soll ebenfalls bei der Bundesnetzagentur eingerichtet werden. Eine Übertragung dieser Aufgabe an die Datenschutzbehörden – wie in der KI-Verordnung als Alternative vorgesehen – soll nicht erfolgen. Die beabsichtigte zentrale Funktion der Bundesnetzagentur wird darüber hinaus auch dadurch deutlich, dass sie sowohl zentrale Beschwerdestelle sein als auch die Zuständigkeit für die Wissensvermittlung und Innovationsförderung erhalten soll.

Bis zum Ende des Berichtszeitraums wurde der Referentenentwurf nicht verabschiedet, die abschließende Umsetzung der KI-Verordnung in nationales Recht wird im nächsten Tätigkeitsbericht voraussichtlich zu erläutern sein.

### *2.1.4 Orientierungshilfen der Datenschutzkonferenz*

**DSK-Orientierungshilfe zu TOMs bei Entwicklung und Betrieb von KI-Systemen**
Dass die datenschutzrechtliche Einordnung eines KI-Systems nicht erst bei seiner Anwendung, sondern bereits während seiner Konzeption beginnt, ist mittlerweile allgemeiner Konsens.

Im Mittelpunkt der im Juni 2025 veröffentlichten „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ der DSK steht aus diesem Grund der Lebenszyklus eines KI-Systems. Die DSK legt nun erstmals verbindlich dar, welche technischen und organisatorischen Anforderungen von der initialen Konzeption über die Datenaufbereitung und Modellentwicklung bis hin zu Einführung und Betrieb von KI-Systemen zugrunde zu legen sind.

Dabei wird der Lebenszyklus eines KI-Systems in vier entscheidende Phasen unterteilt (Design, Entwicklung, Einführung sowie Betrieb und Monitoring) und zur methodischen Überführung der abstrakten rechtlichen Anforderungen kommen die sieben Gewährleistungsziele des Standard-Datenschutzmodells (SDM) zum Einsatz (Datenminimierung, Verfügbarkeit, Vertraulichkeit, Integrität, Intervenierbarkeit, Transparenz und Nichtverkettung).

▶ DSK-Orientierungshilfe „TOMs bei KI-Systemen“

Eine innovative, dabei aber auch verantwortungsvolle KI-Landschaft kann nur dann entstehen, wenn Datenschutzmaßnahmen frühzeitig integriert werden. Die Notwendigkeit auch und gerade in KI-Systemen den „Privacy-by-Design“-Ansatz zu verfolgen, wird von der DSK durch diese Orientierungshilfe betont.

**Datenschutzrechtliche Besonderheiten generativer KI-Systeme mit RAG-Methode**
Am 17. Oktober 2025 wurde von der Datenschutzkonferenz eine Orientierungshilfe zu „KI-Systemen mit Retrieval Augmented Generation (RAG)“ veröffentlicht. Unternehmen und Behörden, die diese KI-Technologie bereits einsetzen oder einsetzen wollen, erhalten durch diese Orientierungshilfe rechtliche und technische Hinweise zur Nutzung solcher KI-Systeme bei gleichzeitiger Verringerung der Risiken für Betroffene.

Werden große Sprachmodelle durch den Zugriff auf behörden- oder unternehmenseigene Wissensquellen ergänzt, um so kontextspezifische Antworten zu liefern, so spricht man von RAG-Technologie. Wenngleich RAG-Systeme durch eigenständige Entwicklung, Betrieb und Kontrolle „Datenschutz-by-Design“ abbilden können, so bringen sie dennoch datenschutzrechtliche Risiken mit sich. Werden sie zum Beispiel auf der Basis eines rechtswidrig trainierten Large Language Models (LLM) aufgebaut, so bleiben die damit zusammenhängenden datenschutzrechtlichen Probleme auch im RAG-System bestehen.

▶ DSK-Orientierungshilfe „KI-Systeme mit RAG-Methode“

Die DSK bestätigt in dieser Orientierungshilfe, dass die Verwendung der RAG-Methode die Schwächen traditioneller KI-Systeme reduzieren kann, gleichwohl werden verantwortliche Stellen aufgefordert, die spezifischen Herausforderungen und Erleichterungen, die mit der RAG-Methode einhergehen, vor deren Einsatz sorgfältig zu prüfen.

### 2.1.5 *Leitlinie des EDPS zum Risikomanagement von KI-Systemen*

Die am 11. November 2025 veröffentlichte „Guidance for Risk Management of Artificial Intelligence Systems“ soll als praktischer Leitfaden dienen, der Risikoüberlegungen in den gesamten Lebenszyklus von KI-Systemen integriert. Von den verantwortlichen Stellen sollen bei der Entwicklung KI-gestützter Systeme nicht nur die Risiken hinsichtlich personenbezogener Daten, sondern auch die für grundlegende Rechte und Freiheiten von Beginn an mit- und fortlaufend weitergedacht werden.

Der European Data Protection Supervisor (EDPS) sieht dabei den dokumentierten und wiederholbaren Umgang mit Risiken als Grundlage für einen verantwortlichen KI-Einsatz, damit systematische Risiken für personenbezogene Daten und fundamentale Rechte frühzeitig erkannt und begrenzt werden können. Ziel ist es, Datenverantwortliche bei der rechtskonformen Steuerung und Überwachung von KI-Prozessen zu unterstützen.

Die Verknüpfung klassischer Datenschutzprinzipien (Sicherung der Datenqualität, Datenminimierung und Zweckbindung) mit technischen Risikobetrachtungen (Verhinderung von Datenlecks, unbefugter Zugriff und Fehlfunktionen des Systems) kann als ein zentraler Bestandteil der Guidance genannt werden. Der fortlaufenden Risikobewertung sowie Anpassung der technischen und organisatorischen Maßnahmen in Form eines dokumentierten Monitorings kommt ebenso eine große Bedeutung zu.

▶ **EDPS-Leitlinie „Risikomanagement von KI-Systemen“**

Der vom EDPS vorgelegte Leitfaden will sich als ergänzendes Instrument verstanden wissen, indem er bewährte Risikomanagementstandards mit den Anforderungen des europäischen Datenschutzrechts verknüpft. Die aufgezeigte Risikosteuerung kann helfen, den KI-Einsatz verantwortungsvoll und rechtssicher zu gestalten und so den zunehmenden regulatorischen und gesellschaftlichen Erwartungen gerecht zu werden.

### 2.1.6 *Faktenblatt des Europäischen Gerichtshofs zum Schutz personenbezogener Daten*

Zentrale Entscheidungen zur Auslegung des Datenschutzrechts sowohl aus der Zeit vor Inkrafttreten der DSGVO als auch danach hat der Europäische Gerichtshof (EuGH) in seinem am 28. April 2025 veröffentlichten Faktenblatt zum Schutz personenbezogener Daten zusammengefasst. Es entstand so eine Übersicht zur datenschutzrechtlichen Rechtsprechung und die Möglichkeit, die bestehenden Anforderungen an die Verarbeitung personenbezogener Daten besser zu verstehen.

Das 108 Seiten umfassende Dokument, das zunächst das Grundrecht auf Schutz personenbezogener Daten, den Art. 8 der EU-Grundrechtecharta, als verfassungsrechtliches Fundament darstellt, wendet sich im Weiteren verschiedenen Aspekten des Datenschutzes zu. Nach Entscheidungen zu allgemeinen Regelungen folgen solche, die sektorspezifische Regelungen betreffen (unter anderem auch im Bereich elektronischer Kommunikation). Und neben der Darstellung der Anforderungen an die Drittlandübermittlung werden auch

Entscheidungen dargestellt, die die Aufsicht über die Verarbeitung personenbezogener Daten betreffen.

Die vorliegende Zusammenstellung kann dabei unterstützen, zentrale Gerichtsentscheidungen besser zu verstehen, indem sie Struktur in eine komplexe Materie bringt.

▶ EuGH-Faktenblatt „Schutz personenbezogener Daten“

## 2.2 Kirchliche Gesetzgebung

### *2.2.1 Datenschutzhinweise für neue Kirchengemeinden im Erzbistum Freiburg*

Das Referat Datenschutz im Erzbischöflichen Ordinariat hat zusammen mit einigen Pfarreiökonomen Ende 2025 Hinweise zum Datenschutz für die neuen Kirchengemeinden in Form von FAQs herausgegeben, die bei Bedarf weitergeschrieben werden sollen. Denn die Neuerrichtung der Kirchengemeinden zum 1. Januar 2026 erfordert auch für Datenschutzthemen eine Klärung von Rechtsfragen und eine Neubewertung von organisatorischen Entscheidungen.

Darin werden Fragen beispielsweise zur Auflösung von Pfarrarchiven beantwortet, die Kirchengemeinden werden dabei vom Erzbischöflichen Archiv unterstützt. Es übernimmt vor Ort die Sichtung und Bewertung des Archivguts. Mittelfristig ist nach Angaben in der Handreichung eine zentrale Unterbringung der Pfarrarchive und deren Betreuung durch das Erzbischöfliche Archiv vorgesehen.

▶ EBFR-FAQs „Datenschutzhinweise für neue Kirchengemeinden“

Weitere Hinweise gibt es zur Erarbeitung von Berechtigungskonzepten, zur Gültigkeit von Einwilligungen, zur Implementierung von neuer Software und zum Umgang mit vorhandenen Verzeichnissen von Verarbeitungstätigkeiten, den so genannten VVTs.

FAQ Kirchengemeinden Neu/ Datenschutz

Inhaltsverzeichnis

Auflösung von (Pfarr) -verwaltungen; Auflösung von Archiven ..... 2
Berechtigungskonzept ..... 2
Einwilligung ..... 2
Newsletter ..... 2
Prozess Implementierung Software ..... 2
Verzeichnis von Verarbeitungstätigkeiten (VVT) ..... 3

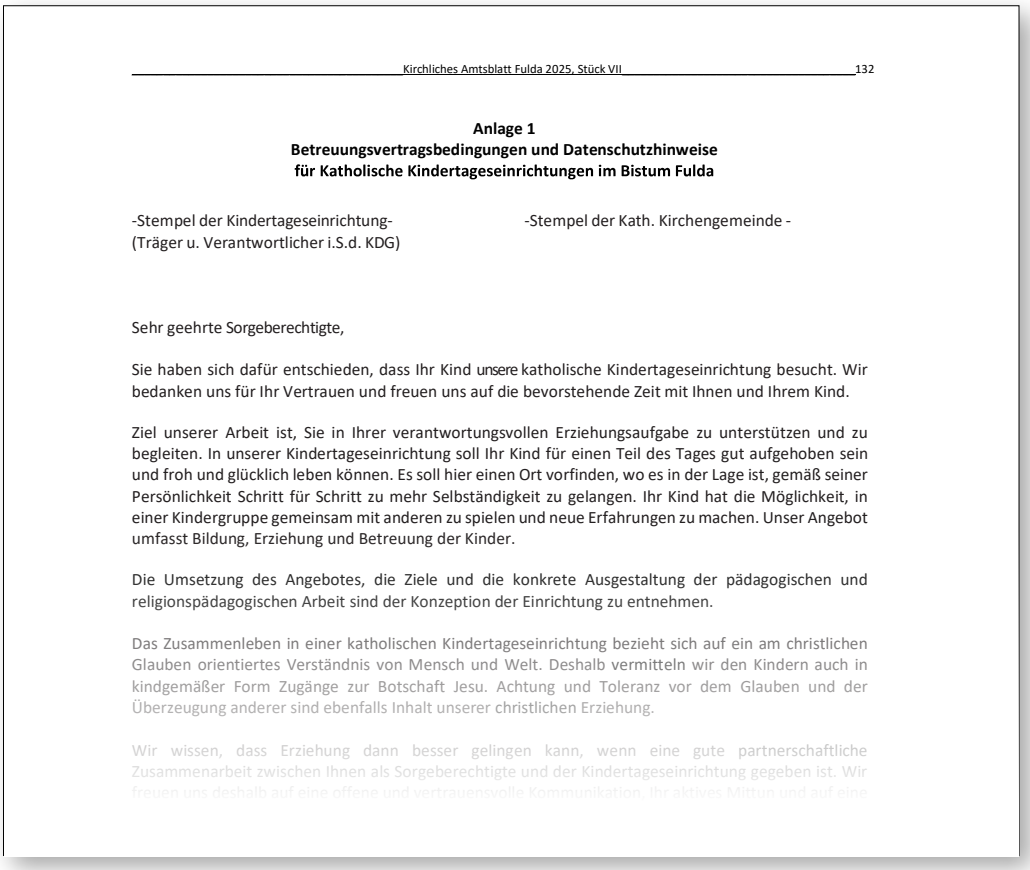
### *2.2.2 Neue Betreuungsvertragsbedingungen und Datenschutzhinweise für katholische Kitas im Bistum Fulda*

Das Bistum Fulda hat im Berichtsjahr 2025 ein neues Musteranschreiben für Betreuungsvertragsbedingungen und Datenschutzhinweise für katholische Kindertageseinrichtungen in seinem Amtsblatt (VII/25 Nr. 65) veröffentlicht. Der den Vertragsbedingungen beiliegende Betreuungsvertrag ist die Grundlage für die Aufnahme eines Kindes in eine Kita im Bistum Fulda.

Neben dem Hinweis auf eine Weitergabe von personenbezogenen Daten an das Jugendamt und sonstige staatliche Stellen zur Vermeidung von Kindeswohlgefährdungen nach § 8a Sozialgesetzbuch (SGB) VIII wird in dem Muster auch auf die ausführlichen Datenschutzhinweise für katholische Kitas zum Umgang mit personenbezogenen Daten hingewiesen, die den Sorgeberechtigten gesondert zur Verfügung gestellt werden.

Diese Datenschutzhinweise geben einen Überblick darüber, wie die Daten im Rahmen des Betreuungsverhältnisses erhoben, weiterverarbeitet und genutzt werden. Diese Hinweise werden durch weitere Informationen des jeweiligen Trägers ergänzt, die auf besondere Umstände, Verfahren und Zwecke eingehen.

Darin werden detailliert die unterschiedlichen Rechtsgrundlagen für die verschiedenen Datenverarbeitungen in Kitas dargelegt und ausführlich die Datenschutzrechte der Sorgeberechtigten beschrieben.



Kirchliches Amtsblatt Fulda 2025, Stück VII 132

**Anlage 1**
**Betreuungsvertragsbedingungen und Datenschutzhinweise**
**für Katholische Kindertageseinrichtungen im Bistum Fulda**

-Stempel der Kindertageseinrichtung-
(Träger u. Verantwortlicher i.S.d. KDG)

-Stempel der Kath. Kirchengemeinde -

Sehr geehrte Sorgeberechtigte,

Sie haben sich dafür entschieden, dass Ihr Kind unsere katholische Kindertageseinrichtung besucht. Wir bedanken uns für Ihr Vertrauen und freuen uns auf die bevorstehende Zeit mit Ihnen und Ihrem Kind.

Ziel unserer Arbeit ist, Sie in Ihrer verantwortungsvollen Erziehungsaufgabe zu unterstützen und zu begleiten. In unserer Kindertageseinrichtung soll Ihr Kind für einen Teil des Tages gut aufgehoben sein und froh und glücklich leben können. Es soll hier einen Ort vorfinden, wo es in der Lage ist, gemäß seiner Persönlichkeit Schritt für Schritt zu mehr Selbständigkeit zu gelangen. Ihr Kind hat die Möglichkeit, in einer Kindergruppe gemeinsam mit anderen zu spielen und neue Erfahrungen zu machen. Unser Angebot umfasst Bildung, Erziehung und Betreuung der Kinder.

Die Umsetzung des Angebotes, die Ziele und die konkrete Ausgestaltung der pädagogischen und religionspädagogischen Arbeit sind der Konzeption der Einrichtung zu entnehmen.

Das Zusammenleben in einer katholischen Kindertageseinrichtung bezieht sich auf ein am christlichen Glauben orientiertes Verständnis von Mensch und Welt. Deshalb vermitteln wir den Kindern auch in kindgemäßer Form Zugänge zur Botschaft Jesu. Achtung und Toleranz vor dem Glauben und der Überzeugung anderer sind ebenfalls Inhalt unserer christlichen Erziehung.

Wir wissen, dass Erziehung dann besser gelingen kann, wenn eine gute partnerschaftliche Zusammenarbeit zwischen Ihnen als Sorgeberechtigte und der Kindertageseinrichtung gegeben ist. Wir freuen uns deshalb auf eine offene und vertrauensvolle Kommunikation, Ihr aktives Mittun und auf eine

**Das Bistum Fulda hat ein neues Musteranschreiben für Betreuungsvertragsbedingungen und Datenschutzhinweise für katholische Kitas veröffentlicht.**

### *2.2.3 Umfangreiches Regelwerk zum IT-Einsatz im Bistum Speyer*

Das Bistum Speyer hat Mitte 2025 ein Gesetz über den Einsatz elektronischer Informationstechnik im Bistum, kurz: IT-Gesetz, in Kraft gesetzt (siehe Oberhirtliches Verordnungsblatt Nr. 7/2025, Nr. 45). Ziel dieses Gesetzes ist die Sicherheit der elektronischen Datenverarbeitungssysteme sowie die Umsetzung der datenschutzrechtlichen Vorgaben in Bezug auf die elektronische Datenverarbeitung im Bistum Speyer, seinen Kirchengemeinden und dem Domkapitel. Organisatorisch bedingt erfolgt eine Unterscheidung zwischen Regelungen, die für alle Mitarbeiterinnen und Mitarbeiter des Bistums, der Kirchengemeinden sowie des Domkapitels gelten und besonderen Regelungen für Mitarbeitende des Bischöflichen Ordinariats.

Das umfang- und detailreiche Werk regelt zum Beispiel die Nutzung privater Geräte und Datenträger im dienstlichen Kontext, die Nutzung von betrieblicher Hard- und Software, die Pflicht zur Verwendung der zur Verfügung gestellten bistumseigenen E-Mail-Adressen in der täglichen Arbeit, den Gebrauch des Internetzugangs am Arbeitsplatz und von WLAN, die Verschlüsselung von Datenträgern und speziell für Beschäftigte des Bischöflichen Ordinariats den externen Zugang zum Ordinariatsnetzwerk über eine VPN-Clientsoftware oder andere webbasierte Techniken.

Der Dienstgeber wiederum hat den „reibungslosen" IT-Betrieb sicherzustellen und sich beispielsweise um die regelmäßige Sicherung der dienstlichen Daten und um deren Schutz zu kümmern.

### *2.2.4 Bistum Speyer regelt Umsetzung des Hinweisgeberschutzgesetzes*

Im Berichtszeitraum hat nun auch das Bistum Speyer ein Gesetz zur Umsetzung des Hinweisgeberschutzgesetzes erlassen – das „HinSchGUmsetzungG" (siehe Oberhirtliches Verordnungsblatt Nr. 7/2025, Nr. 46). Hinter der sperrigen Abkürzung verbirgt sich die Regelung, die das bundesweit geltende Hinweisgeberschutzgesetz (HinSchG) in seiner jeweils geltenden Fassung für das Bistum umsetzen soll sowie den Schutz von hinweisgebenden Personen, denen durch eine Meldung keine Nachteile entstehen dürfen, und insbesondere den Betrieb einer zentralen internen Meldestelle. Der Betrieb der Meldestelle bezieht sich auf die Funktionsweise sowie die Pflichten des Betreibers der Meldestelle.

Die bistumsinterne Meldestelle wird von einer Kanzlei geführt – erreichbar unter anderem über die E-Mail-Adresse: hinschg@bfs-nw.de. Im Übrigen bildet die Abteilung „Innenrevision" nach den Angaben im Amtsblatt die zentrale interne Meldestelle im Sinne des HinSchG. Sie wird dabei – auf ihr Verlangen – durch die Leitungen der Abteilungen „Bischöfliche Kanzlei", „Bischöfliches Rechtsamt", „EDV-Abteilung", „Betrieblicher Datenschutz" und „Personalverwaltung" unterstützt.

Hinweise zu Verstößen speziell gegen das KDG in seiner jeweils geltenden Fassung werden nach § 3 Abs. 4 des Umsetzungsgesetzes dem betrieblichen Datenschutzbeauftragten zugeleitet, ohne dass eine eigene Prüfung durch die interne zentrale Meldestelle erfolgt.

Im Übrigen wird in § 9 HinSchGUmsetzungG nochmals ausdrücklich klargestellt, dass im Rahmen des Hinweisgeberschutzes personenbezogene Daten vertraulich und entsprechend der geltenden kirchlichen Datenschutzvorschriften sowie der Datenschutzerklärung behandelt werden.

### *2.2.5 Einsichts- und Auskunftsrechte von Betroffenen sexuellen Missbrauchs in Sachakten des Bistums Trier geregelt*

Die Ordnung zur Regelung von Einsichts- und Auskunftsrechten von Betroffenen sexuellen Missbrauchs und Dritten in Sachakten des Bistums Trier ist zum 1. April 2025 in Kraft getreten (siehe dazu das Kirchliche Amtsblatt für das Bistum Trier 3/2025, Nr. 81). Diese Rechte gelten ausdrücklich nur für Unterlagen in Sachakten, die einen Bezug zu dem betreffenden Missbrauchsvorwurf oder der Missbrauchstat haben.

Was unter dem Begriff „Sachakten“ zu verstehen ist, wird in § 3 der Ordnung erklärt: Sachakten sind danach insbesondere Verfahrensakten des Interventionsbeauftragten des Bistums, vergleichbare Aktenbestände der laufenden Schriftgutverwaltung im Sinne der Ordnung zur Regelung von Einsichts- und Auskunftsrechten für die Aufarbeitungskommissionen, für Forschungszwecke und für Anwaltskanzleien sowie Unterlagen gemäß § 1 Abs. 2 Ziff. 3 bis 6 des Allgemeinen Dekrets über die Verwaltung des Geheimarchivs (ADVG) – also Verwarnungen und Verweise gemäß can. 1339 § 3 CIC, die Akten der Voruntersuchungen gemäß can. 1719 CIC und der Strafverfahren bei Sittlichkeitsdelikten gemäß can. 489 § 2 CIC sowie Akten der staatlichen Strafverfolgungsbehörden und Gerichte, die Kleriker betreffen.

**Allgemeines Dekret über die Verwaltung des Geheimarchivs (ADVG)**

**§ 1 Archivgut**

(1) Archivgut im Sinne dieses Dekretes sind Dokumente, deren Geheimhaltung durch eine kirchenrechtliche Norm oder aufgrund der Natur der Sache verlangt ist und die an einem sicheren Ort fest verschlossen mit größter Sorgfalt aufzubewahren sind (can. 489 § 1 CIC).

(2) …

**§ 2 Aufbewahrungsfristen**

Soweit nicht durch eine spezielle Norm oder von der zuständigen Autorität etwas anderes festgelegt ist, sind diese Dokumente unbefristet und dauerhaft zu verwahren (cann. 486 § 1 und 489 § 2 CIC).

**§ 5 Herausgabe von Akten**

(1) Gemäß can. 490 § 3 CIC gilt grundsätzlich, dass aus dem Geheimarchiv außer an die in § 4 genannten Personen keine Dokumente an Dritte herausgegeben werden dürfen.

(2) …

[aus: Kirchliches Amtsblatt für das Bistum Trier 3/2025, Nr. 82: Allgemeines Dekret über die Verwaltung des Geheimarchivs (ADVG)].

Zum Schutz Dritter wird ausdrücklich darauf hingewiesen, dass deren personenbezogene Daten bei Bedarf vor einer Einsichtnahme zu anonymisieren oder pseudonymisieren sind. Das Anfertigen von Abschriften oder Kopien durch die Einsicht nehmende Person ist untersagt. Soweit es im Einzelfall rechtlich zulässig ist, sieht die Ordnung vor, dass das Bistum auf Antrag Kopien erstellt und der Einsicht nehmenden Person aushändigt.

Dritten, wie zum Beispiel Ehe-/Lebenspartnern, Kindern, Eltern und Geschwistern, stehen die aufgeführten Einsichts- und Auskunftsrechte nur insofern zu, als sie einen Bezug zu dem verstorbenen Betroffenen, dem betreffenden Missbrauchsvorwurf oder der Missbrauchstat haben. Sie müssen mit Antragstellung schriftlich darlegen, dass die Einsicht und Auskunft zur Verfolgung eines noch nicht verjährten geerbten Schmerzensgeldanspruchs oder zur Abwehr einer Beeinträchtigung des postmortalen Persönlichkeitsrechts des Betroffenen erfolgt.

**Detaillierte Richtlinie zur Regelung des Verfahrens zur Akteneinsicht und Aktenauskunft an Betroffene sexuellen Missbrauchs und Dritte erlassen**
Der Ablauf der Einsichtnahme und der Auskunftserteilung wird durch eine Richtlinie des Bischöflichen Generalvikars genauer geregelt (sie ist ebenfalls im Amtsblatt 3/2025 zu finden, dort unter Nr. 83).

Darin ist unter anderem niedergelegt, dass im Vorfeld der Akteneinsicht eine beauftragte und zur Verschwiegenheit verpflichtete Person die Akte durchsieht und sie datenschutzrechtlich überprüft. Das bedeutet insbesondere, dass in einer Kopie der Akte, die für die Einsichtnahme zur Verfügung gestellt wird, alle Hinweise unkenntlich gemacht werden, die dritte Personen oder nicht den Fall betreffen, auf den sich der Antrag bezieht. Dies gilt beispielsweise für Anschreiben oder Vermerke, die verschiedene Fälle und/oder Personen tangieren. Zuständig hierfür ist der Interventionsbeauftragte, dem im Übrigen auch grundsätzlich die Durchführung des Akteneinsichtstermins obliegt.

Nach Vorbereitung der Akte sieht die Richtlinie eine finale Sichtung durch die Stabsstelle Justiziariat vor. Ebenso verhält es sich bei der Aktenauskunft: Nach Vorbereitung der Zusammenfassung bzw. der Antwort durch den Interventionsbeauftragten erfolgt eine finale Sichtung durch die Stabsstelle.

Darüber hinaus schreibt die Richtlinie vor, dass eine Person aus dieser Stabsstelle beim Akteneinsichtstermin beratend zur Gewährleistung des ordnungsgemäßen Ablaufs der Durchführung der Akteneinsicht und insbesondere des Datenschutzes bereitsteht.

## 2.3 Ausgewählte Rechtsprechung staatlicher Gerichte

Der EuGH hat auch im Jahr 2025 reichlich Rechtsfortbildung betrieben. So hat er beispielsweise die Bedeutung des Begriffs der personenbezogenen Daten im Zusammenhang mit der Übermittlung pseudonymisierter Daten an Dritte sowie den immateriellen Schadensersatz im Datenschutzrecht präzisiert.

### *2.3.1 Auf den Charakter kommt es an*

Das mit Spannung erwartete Urteil des EuGH in der Rechtssache C-413/23 am 4. September 2025 sollte einen jahrelangen Streit um die Auslegung des Begriffs der personenbezogenen Daten – und was eigentlich Anonymität bedeutet – entscheiden. Es ging also ums Eingemachte – den sachlichen Anwendungsbereich des Datenschutzrechts. Denn: Werden personenbezogene Daten verarbeitet, gelten die Vorschriften der Europäischen Datenschutzgrundverordnung (DSGVO). Sind diese Daten dagegen anonym, ist der Anwendungsbereich der DSGVO gar nicht eröffnet.

Doch wie verhält es sich mit pseudonymisierten Daten? Hier haben die Europarichter nunmehr klargestellt, dass Anonymität und Personenbeziehbarkeit im Kontext und aus Sicht des jeweils Verantwortlichen zu sehen sind. Der bisher vielfach vertretenen Meinung, dass pseudonymisierte Daten niemals anonym sein können, weil irgendjemand schon die Pseudonymität der Daten wird aufheben können, ist der EuGH explizit nicht gefolgt.

Er beruft sich dabei auf die gesetzlichen Grundlagen und die dazu ergangene Rechtsprechung. Daraus ergebe sich, dass die Pseudonymisierung – je nach den Umständen des Falles – andere Personen als den Verantwortlichen tatsächlich daran hindern könne, die betroffene Person zu identifizieren, sodass diese für sie nicht oder nicht mehr identifizierbar sei. In diesem Zusammenhang verweist der Gerichtshof ausdrücklich auf die Lehren aus der Rechtsprechung zur Beurteilung der Identifizierbarkeit der betroffenen Person in Situationen, in denen sich die zur Identifizierung dieser Person erforderlichen Informationen nicht in den Händen verschiedener Personen befanden.

Es kommt also wie so oft auf den Charakter, hier auf die prozessualen, technischen und organisatorischen Umstände, unter denen die Daten verarbeitet werden, an. Dieser kann bei Daten von personenbezogen nach anonym wechseln, je nach den konkreten Umständen auf Seiten des Verantwortlichen.

### *2.3.2 Sorge und Ärger als immaterieller Schaden*

In einem weiteren sehr praxisrelevanten Verfahren befasste sich der EuGH auf Vorlage des Bundesgerichtshofs (BGH) ebenfalls am 4. September 2025 (Rechtssache: C-655/23) schwerpunktmäßig mit Ansprüchen auf immateriellen Schadensersatz.

Danach sei der Begriff „immaterieller Schaden“ weit zu verstehen. Die Europarichter verweisen in diesem Zusammenhang einmal mehr auf das Ziel der DSGVO, ein möglichst hohes Schutzniveau für natürliche Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten.

So könnten auch negative Gefühle, die die betroffene Person infolge einer unbefugten Übermittlung ihrer personenbezogenen Daten an einen Dritten empfinde, wie zum Beispiel Sorge oder Ärger – auch wenn sie im Übrigen Teil des allgemeinen Lebensrisikos sein könnten – und die durch einen Verlust der Kontrolle über diese Daten, ihre mögliche missbräuchliche Verwendung oder eine Rufschädigung hervorgerufen würden, einen immateriellen Schaden darstellen – aber nur sofern die betroffene Person nachweise, dass sie solche Gefühle samt ihrer negativen Folgen aufgrund des in Rede stehenden Verstoßes gegen die DSGVO empfindet.

Ausdrücklich verweist das Gericht darauf, dass Art. 82 Abs. 1 DSGVO den Ersatz eines immateriellen Schadens nicht davon abhängig mache, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht habe. Der von dieser Person geltend gemachte immaterielle Schaden müsse also keine „Bagatellgrenze“ überschreiten, damit dieser Schaden ersatzfähig sei.

### *2.3.3 Keine Entschädigung bei rein hypothetischem Risiko*

Eine weitere Präzisierung beim immateriellen Schadensersatz hat der BGH am 13. Mai 2025 (Aktenzeichen: VI ZR 186/22) vorgenommen. Er stellt in seinem der Entscheidung vorangestellten Leitsatz klar: „Ein rein hypothetisches Risiko der missbräuchlichen Verwendung personenbezogener Daten durch einen unbefugten Dritten kann nicht zu einer Entschädigung gemäß Art. 82 Abs. 1 DSGVO führen.“

Der bloße Verstoß gegen die DSGVO reiche nicht aus, um einen Schadensersatzanspruch gemäß deren Art. 82 Abs. 1 zu begründen. Denn das Vorliegen eines materiellen oder immateriellen Schadens stelle ebenso eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadensersatzanspruch dar, wie das Vorliegen eines Verstoßes gegen die DSGVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ seien. Insofern muss, so Deutsch-

lands höchste Zivilrichter, die Person, die auf der Grundlage dieser Bestimmung Ersatz eines immateriellen Schadens verlangt, nicht nur den Verstoß gegen Bestimmungen dieser Verordnung nachweisen, sondern auch, dass ihr durch diesen Verstoß ein solcher Schaden entstanden ist. Ein solcher Schaden könne daher nicht allein aufgrund des Eintritts dieses Verstoßes vermutet werden. Insbesondere müsse eine Person, die von einem DSGVO-Verstoß betroffen sei, der für sie nachteilige Folgen gehabt habe, den Nachweis erbringen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO darstellen.

Nach Erwägungsgrund 85 der DSGVO sei vom Schadensbegriff zwar auch der bloße Kontrollverlust über eigene Daten umfasst, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte, der Begriff „immaterieller Schaden“ weit zu verstehen sei und die DSGVO ein hohes Schutzniveau gewährleisten wolle (siehe dazu die zuvor besprochenen EuGH-Entscheidungen).

Es sei dennoch, wenn sich eine Person, die auf der Grundlage von Art. 82 Abs. 1 DSGVO Schadensersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden könne. Die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen reicht nicht aus, so der BGH. Folglich könne ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten nicht zu einer Entschädigung führen.

Im zugrunde liegenden Fall hatte der Kläger die beklagte Stadt wegen der unverschlüsselten Versendung von verwaltungsgerichtlichen Empfangsbekenntnissen durch Telefax auf Geldentschädigung in Anspruch genommen.

### *2.3.4 Keine zu hohen Anforderungen an Darlegung eines immateriellen Schadens*

In einem weiteren Urteil zum immateriellen Schadensersatz gemäß Art. 82 Abs. 1 DSGVO hat der gleiche Senat ebenfalls am 13. Mai 2025 (Aktenzeichen: VI ZR 67/23) entschieden, dass in diesem Zusammenhang an die Substantiierungspflicht der von einem Datenschutzverstoß betroffenen Person keine überzogenen Anforderungen zu stellen sind.

Im vorliegenden Fall ging es um den Ersatz eines immateriellen Schadens aufgrund einer Negativmeldung des beklagten Inkassounternehmens an die Schufa Holding AG.

### *2.3.5 Verspätete Auskunft begründet keinen immateriellen Schadensersatzanspruch*

Mit immateriellem Schadensersatz hatte sich im Jahr 2025 auch das Bundesarbeitsgericht (BAG, Urteil vom 20. Februar 2025, Aktenzeichen: 8 AZR 61/24) auseinanderzusetzen und zwar im Zusammenhang mit einem Verstoß gegen die Auskunftspflicht nach Art. 15 DSGVO. Der Kläger verlangte – letztlich erfolglos – Schadensersatz, weil eine verspätete Auskunft gegen die Datenschutzgrundverordnung verstoße. Der immaterielle Schaden bestehe in Form eines wochenlangen Kontrollverlusts bezüglich der Datenverarbeitung, der ihm Sorgen bereitet und Angst ausgelöst habe, weil die Beklagte, seine ehemalige Arbeitgeberin, womöglich „Schindluder“ mit seinen Daten treibe.

Für das höchste deutsche Arbeitsgericht fehlt es vorliegend bereits für einen möglichen Schadensersatzanspruch an einem Schaden als eine der drei Voraussetzungen für einen solchen Anspruch nach Art. 82 Abs. 1 DSGVO – ebenso wie das Vorliegen eines DSGVO-Verstoßes sowie einem Kausalzusammenhang zwischen dem erlittenen Schaden und dem Verstoß.

Zwar soll – wie in den vorherigen Urteilsbesprechungen geschildert – ein Kontrollverlust über personenbezogene Daten durchaus einen immateriellen Schaden darstellen können. Aber nur, sofern die betroffene Person nachweise, einen solchen Schaden tatsächlich erlitten zu haben. Eine verspätete Auskunftserteilung stelle jedoch nicht ohne Weiteres einen Schaden im Sinne von Art. 82 DSGVO dar.

Mit Verweis auf den EuGH stellen die Bundesarbeitsrichter dar, dass unter einem Kontrollverlust nur eine Situation zu verstehen sei, in der die betroffene Person eine begründete Befürchtung des Datenmissbrauchs hege. Das bloße Berufen auf eine bestimmte Gefühlslage reiche dabei nicht aus. Anders als etwa bei einer Veröffentlichung von sensiblen Daten im Internet aufgrund eines Datenlecks begründe eine lediglich verspätete Auskunft für sich genommen keinen Kontrollverlust, sondern nur einen Zeitverzug hinsichtlich der Auskunft.

Denn, so das BAG weiter, wäre schon das Berufen auf abstrakte Befürchtungen ausreichend für die Annahme eines (immateriellen) Schadens, könnte jeder Verstoß gegen Art. 15 DSGVO einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO begründen. Die eigenständige Voraussetzung des Schadens würde damit bedeutungslos.

Verspätete Auskünfte können für Verantwortliche dennoch teuer werden – bei entsprechender Ahndung durch die zuständige Datenschutzaufsicht.

### *2.3.6 Verzicht auf Auskunftsrecht in arbeitsgerichtlichem Vergleich möglich*

Ein Beschäftigter kann in einem zur Beendigung eines Arbeitsverhältnisses führenden arbeitsgerichtlichen Vergleich grundsätzlich auf sein Auskunftsrecht nach Art. 15 Abs. 1 DSGVO verzichten. Voraussetzung hierfür ist für das Oberverwaltungsgericht (OVG) Saarlouis (Urteil vom 13. Mai 2025, Aktenzeichen: 2 A 165/24) allerdings, dass die entsprechende Klausel im Vergleich auch weit genug gefasst ist. Diese lautete im vorliegenden Fall: „Mit Erfüllung des Vergleichs sind alle Ansprüche aus dem Arbeitsverhältnis und dessen Beendigung, gleich ob bekannt oder unbekannt, gleich aus welchem Rechtsgrund, abgegolten mit Ausnahme der Arbeitspapiere."

Ausgleichsklauseln in gerichtlichen Vergleichen, die – wie vorliegend – ausdrücklich auch unbekannte Ansprüche unabhängig von ihrem Rechtsgrund erfassen sollen und auf diese Weise zu erkennen geben, dass die Parteien an die Möglichkeit des Bestehens ihnen nicht bewusster Ansprüche gedacht und auch sie in den gewollten Ausgleich einbezogen haben, sind für die Verwaltungsrichter regelmäßig als umfassender Anspruchsausschluss in Form eines konstitutiven negativen Schuldanerkenntnisses zu verstehen. Sie haben keinen Zweifel daran, dass auch der Auskunftsanspruch nach Art. 15 DSGVO hiervon umfasst wird.

Der Kläger hatte in beiden Instanzen damit erfolglos auf Fortführung seines datenschutzrechtlichen Verfahrens gegen die frühere Arbeitgeberin durch die zuständige Datenschutzaufsicht geklagt. Diese hatte das Verwaltungsverfahren gegen die frühere Arbeitgeberin aufgrund des zwischen den Parteien geschlossenen Vergleichs und den damit einhergehenden Verzicht auf das Auskunftsrecht gemäß Art. 15 DSGVO per Bescheid eingestellt.

**Aus der Urteilsbegründung:**
„Dass der Betroffene bei einem Verzicht auf das Auskunftsrecht nicht mehr überprüfen kann, ob gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) verstoßen wurde, und er gleichzeitig sein Recht auf Datenübertragbarkeit (Art. 20 DSGVO) mangels Kenntnis der über ihn gespeicherten Daten faktisch nicht mehr ausüben kann, ist die logische Folge des Verzichts, besagt aber nichts darüber, ob ein solcher rechtlich möglich ist oder nicht."

### *2.3.7 Kirchliche oder staatliche Gerichtsbarkeit – manchmal keine leichte Abgrenzung*

Das Landesarbeitsgericht (LAG) Düsseldorf (Beschluss vom 29. Juni 2025 – 3 Ta 60/25) hatte sich im Berichtsjahr unter anderem mit der Abgrenzung von kirchlicher und staatlicher Gerichtsbarkeit auseinanderzusetzen. Es stellt dabei klar, dass es zur Unzulässigkeit einer Klage führt, wenn im staatlichen Rechtsweg trotz vorrangiger kirchengerichtlicher Zuständigkeit geklagt wird.

Diese Abgrenzung ist aber nicht – wie es die Vorinstanz noch getan hat – im Rechtswegverfahren nach §§ 48 Abs. 1 Arbeitsgerichtsgesetz (ArbGG), 17 ff. Gerichtsverfassungsgesetz (GVG) vorzunehmen, denn dieses Vorabentscheidungsverfahren betreffe, so das LAG, allein die Abgrenzung der staatlichen Gerichtsbarkeiten untereinander. Die Abgrenzung von Kirchengerichtsbarkeit und staatlicher Gerichtsbarkeit sei vielmehr ausschließlich im Hauptsacheverfahren im Rahmen der Frage nach der Zulässigkeit der Klage zu klären.

Der Kläger hatte sich vorliegend bei einer evangelischen Einrichtung beworben, diese Bewerbung später jedoch zurückgezogen und im weiteren Verlauf einen datenschutzrechtlichen Auskunftsanspruch gemäß Art. 15 DSGVO geltend gemacht und verlangte nach Art. 82 Abs. 1 DSGVO immateriellen Schadensersatz.

Die beklagte kirchliche Stelle drang mit ihrer Auffassung, dass der Rechtsweg gemäß § 47 Abs. 1 Nr. 3 Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) zu den Kirchengerichten, nicht aber zu den staatlichen Gerichten eröffnet sei, in beiden Instanzen nicht durch.

Im Übrigen sahen die LAG-Richter – bei unterstellter staatlicher gerichtlicher Zuständigkeit – für Klagen sich erfolglos um eine Anstellung im Arbeitsverhältnis bewerbender Kläger auf datenschutzrechtliche Auskunftserteilung und/oder Schadensersatz nach Art. 82 Abs. 1 DSGVO ausschließlich die Arbeitsgerichte nach § 2 Abs. 1 Nr. 3 lit. c ArbGG zuständig. Der Beschluss ist rechtskräftig.

## 2.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte

### *2.4.1 Meldedaten für die Abo-Gewinnung*

In der einzigen im Berichtsjahr auf der Website des Datenschutzgerichts der Deutschen Bischofskonferenz (DSG-DBK) veröffentlichten, viel diskutierten Entscheidung (Beschluss vom 19. Mai 2025, Aktenzeichen: DSG-DBK 02/2024) hatte sich die 2. Instanz mit Haustürwerbung durch eine kirchliche Zeitung beschäftigt. Wie schon die Vorinstanz, das Interdiözesane Datenschutzgericht, (IDSG, Beschluss vom 22. März 2024, Aktenzeichen: IDSG 13/2023) kam auch das höchste deutsche katholische Datenschutzgericht zu dem Ergebnis, dass die Offenlegung personenbezogener Daten von Kirchengemeindemitgliedern zum Zweck der Haustürwerbung einer rechtlich verselbstständigten Kirchenzeitung rechtmäßig ist. Anders gesehen hatte das die zuständige katholische Datenschutzaufsicht in ihrem angefochtenen Bescheid. Beide Instanzen sahen die Weitergabe der Meldedaten durch das Bistum für die Gewinnung neuer Abonnenten für die Kirchenzeitung durch das kirchliche Interesse gedeckt. Die Offenlegung der personenbezogenen Daten erfolge auf Grundlage von § 9 Abs. 1, § 6 Abs. 1 lit. f) KDG zur Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liege und zugleich zur Erfüllung einer kirchlichen Aufgabe, § 42 Abs. 1 Bundesmeldegesetz (BMG).

Dem Vorliegen eines Erlaubnistatbestands stehe auch nicht entgegen, so das Gericht weiter, „dass im vorliegenden Fall der Abschluss eines Dauerschuldverhältnisses (Abonnement) Gegenstand der Haustürwerbung ist“. Es sei zu der Überzeugung gelangt, „dass die vom Bistum mit dem X beabsichtigte Verkündung durch den X aufgrund wirtschaftlicher Rahmenbedingungen nur weiterhin durchgeführt werden kann, wenn neue Abonnenten gewonnen werden“. Die Haustürwerbung sei dafür ein geeignetes Mittel, mildere, gleich wirksame Maßnahmen seien nicht ersichtlich.

### *2.4.2 Eigen-Verordnung keine Grundlage für Aktenvernichtung*

Bei einer Entscheidung des IDSG (Beschluss vom 26. Mai 2025, Aktenzeichen: IDSG 26/2022) war das Kath. Datenschutzzentrum Frankfurt/M. einmal mehr mittendrin statt nur dabei. Es ging hier um die Vernichtung der bei einem privaten kirchlichen Träger geführten Akte zum begleiteten Umgang.

Bereits bevor das Ganze vor Gericht landete, zog sich die Angelegenheit schon eine ganze Weile hin.

Konkret wendet sich der antragstellende Caritasverband als Träger einer Erziehungsberatung gegen einen Bescheid der Datenschutzaufsicht, mit dem diese die Löschung von Unterlagen zum begleiteten Umgang einer Mutter mit ihren vier Kindern als rechtswidrig eingestuft und beanstandet hat.

Die Kinder der Mutter wurden im Jahr 2013 in staatliche Obhut genommen und in einem Kinderheim untergebracht. Eine familiengerichtliche Vereinbarung regelte den begleiteten Umgang von Mutter und Kindern. Der Antragsteller begleitete den Umgang im Rahmen seiner Erziehungsberatung im Jahr 2014. Die dabei erhobenen Daten beispielsweise in angefertigten Protokollen zu den Umgangstreffen vernichtete der Verband bereits 2017.

Er stützte die Löschung auf eine vom Vorstand des Verbands in Kraft gesetzte und im Verbandshandbuch veröffentlichte „Fristen- und Aufbewahrungsordnung“. Nach dieser Bestimmung sind unter anderem Klientenakten über Beratungen, allgemeine Korrespondenz, Rundschreiben von zeitlicher Bedeutung für die Dauer von drei Jahren aufzubewahren. Die Mutter wandte sich im Jahr 2022 unter anderem mit der Bitte um Prüfung des Vorgangs an die zuständige Frankfurter Datenschutzaufsicht. Diese sah in der Vernichtung der Umgangsakte einen Verstoß gegen das KDG, weil die genannte Ordnung keine ausreichende Grundlage für die Löschung gewesen sei. Es handele sich dabei nicht um eine Ordnungsvorschrift mit Bindungswirkung für Dritte. Es liege vielmehr nahe, so die Aufsicht weiter, eine Pflicht zur Aufbewahrung zumindest bis zur Volljährigkeit der in einer Umgangsakte genannten Kinder anzunehmen. Das IDSG schloss sich diesen Ausführungen in seinem Beschluss ausdrücklich an.

Für den Verband dagegen lag gar keine Löschung vor, weil die Daten eben nur woanders seien, zum Beispiel beim Jugendamt; im Übrigen habe das KDG zu der Zeit noch gar nicht gegolten und Löschen sei sowieso der beste Datenschutz.

Dem Hinweis auf die Nichtgeltung des KDG ist das Gericht mit einem Hinweis darauf, dass die Vernichtung auch nach der damals geltenden Anordnung über den kirchlichen Datenschutz (KDO) unzulässig gewesen wäre, begegnet. Im Übrigen sah es in der Aufbewahrungsordnung des Trägers ebenfalls keine rechtmäßige Grundlage für die Aktenlöschung.

Dem Argument des Antragstellers, nach dem eine Löschung grundsätzlich zu begrüßen und deshalb von einer konkludenten oder zumindest mutmaßlichen Einwilligung des Betroffenen auszugehen sei, tritt das Gericht mit dem Verweis auf Fallkonstellationen wie die vorliegende entgegen, in denen ein berechtigtes Interesse an der weiteren Speicherung besteht: „In dieser Konstellation bedeutet die Löschung ohne Einwilligung des Betroffenen eine Verletzung seiner subjektiven Datenschutzrechte. Das Interesse des Betroffenen kann berechtigt sein, weil nur durch die weitere Speicherung der Daten die Vollständigkeit im Sinn der Richtigkeit der Daten gewährleistet ist und so eine Entscheidung auf der Grundlage eines unrichtigen Sachverhalts vermieden wird (vgl. § 7 Abs. 1 lit. d) und f) KDG, Art. 5 Abs. 1 lit. d) und f) DSGVO).“

Das Interesse der Mutter an der weiteren Aufbewahrung der Akte war für das Gericht somit

berechtigt: „Aus dem ihr grundsätzlich zustehenden Recht der elterlichen Sorge, das verfassungsrechtlich (Art. 6 Abs. 2 GG) und einfachgesetzlich (§ 1626 BGB, § 1 Abs. 2 SGB VIII) gewährleistet ist, folgt das berechtigte Interesse, die Nachprüfbarkeit der jugendhilferechtlichen Unterstützung der Ausübung ihrer elterlichen Sorge auch durch eine Vollständigkeit der einschlägigen Akten zu sicherzustellen."

Die Sache geht aber weiter, denn ein Rechtsmittel ist unter dem Aktenzeichen DSG-DBK 09/2025 anhängig.

**Leitsatz des Gerichts:**
Die Vernichtung der bei einem privaten Träger (hier: Caritas) geführten Akte zum begleiteten Umgang ohne Einwilligung der Betroffenen verstößt gegen ihr Datenschutzrecht, wenn sie nach Maßgabe der datenschutzrechtlichen Vorschriften ein berechtigtes Interesse an der weiteren Speicherung der Daten hat, weil nur durch die weitere Speicherung der Daten die Vollständigkeit im Sinn der Richtigkeit der Daten gewährleistet ist und so für weitere jugendhilferechtliche Bedarfslagen oder zivilrechtliche Streitfälle eine Entscheidung auf der Grundlage eines unrichtigen Sachverhalts vermieden wird (vgl. § 7 Abs. 1 lit. d) und f) KDG, Art. 5 Abs. 1 lit. d) und f) DSGVO).

### *2.4.3 Handschriftliches Spendenverzeichnis unterfällt Datenschutz*

In dem letzten im Berichtsjahr vom IDSG veröffentlichten Beschluss (Beschluss vom 14. Dezember 2025, Aktenzeichen: IDSG 07/2025) hat das Gericht entschieden, dass ein handschriftlich geführtes Spendenverzeichnis einer kirchlichen Kleiderkammer, das eine chronologische Sortierung der für jeden einzelnen Tag erstellten Spendenlisten enthält, durchaus ein Dateisystem im Sinne des § 2 Abs. 1 KDG darstellt. Anders als die Datenschutzaufsicht zuvor sah es damit den sachlichen Anwendungsbereich des KDG gemäß § 2 Abs. 1 KDG eröffnet.

Dem Ganzen zugrunde lag ein Streit um ein Auskunftsersuchen des Vermieters der Kleiderkammer-Räumlichkeiten, der zeitweilig dort auch ehrenamtlich tätig war. Der Antragsteller vermutete in dem Spendenverzeichnis negative Kommentare zu seiner Person und forderte deshalb Einsicht. Die konkrete Einsichtnahme wurde ihm verwehrt und ihm im Übrigen fälschlicherweise mitgeteilt, dass sich keine Aufzeichnungen zu seiner Person darin befänden.

**Fehlerhafte Auskunft ist rechtswidrige Datenverarbeitung**
Die Richter sahen in der Erteilung der inhaltlich fehlerhaften Auskunft nicht nur eine Nichterfüllung des Auskunftsanspruchs aus § 17 KDG, sondern darüber hinaus auch eine rechtswidrige Datenverarbeitung, „die insbesondere gegen die Grundsätze der sachlichen Richtigkeit und Zweckbindung gemäß § 7 Abs. 1 lit. b) und d) KDG (Art. 5 Abs. 1 lit. b) und d) DSGVO) verstößt".

Außerdem sei die korrekte Auskunftserteilung oft eine notwendige Voraussetzung für die Feststellung von Datenschutzverstößen und den daraus eventuell folgenden weiteren Maßnahmen wie das Geltendmachen von Ansprüchen auf Berichtigung, Löschung und Schadenersatz.

**Auskunftsrecht umfasst nicht Einsichtsrecht**
Der Antragsteller habe aber keinen – wie von ihm gewünscht – Anspruch auf Einsichtnahme in das Spendenverzeichnis. Ein solcher ergebe sich nicht aus § 17 KDG. Denn das Recht auf Auskunft und auf Überlassung von Kopien (mit gegebenenfalls geschwärzten Daten Dritter) beinhalte nicht ein Recht auf Akteneinsicht.

Die Akteneinsicht geht, so das IDSG in seiner Begründung, über die in § 17 Abs. 1 und 3 KDG normierten Rechte hinaus, „weil sie die Einsichtnahme in die Originalakte in der vollständigen und unveränderten Fassung bedeutet".

**Leitsätze des Gerichts:**
1. Ein handschriftlich geführtes Spendenverzeichnis, das eine chronologische Sortierung der für jeden einzelnen Tag erstellten Spendenlisten enthält, ist ein Dateisystem im Sinn des § 2 Abs. 1 KDG.
2. Die Erteilung einer inhaltlich fehlerhaften Auskunft stellt sowohl eine Nichterfüllung des Auskunftsanspruchs aus § 17 KDG als auch eine rechtswidrige Datenverarbeitung dar.
3. § 17 KDG umfasst nicht ein Recht auf Akteneinsicht.

### *2.4.4 Einsichtnahme in Mitarbeiter-Account*

Mit einem sehr praxisrelevanten Fall hatte sich das IDSG Mitte des Jahres 2025 zu beschäftigen. Dabei ging es um die Frage der Verletzung von Datenschutzrechten bei der Einsichtnahme eines Verantwortlichen in den Account einer Mitarbeiterin (Beschluss vom 15. Juni 2025, Aktenzeichen: IDSG 19/2023).

Der Dienstgeber war vorliegend auf der Suche nach einer wichtigen Datei, nämlich der Mündelliste. Die Vorgesetzte der Antragstellerin brauchte diese aus Abrechnungsgründen. Da die wichtige Liste nicht an ihrem angestammten Platz war und die Antragstellerin einige Tage abwesend, beauftragte die Vorgesetzte die EDV-Abteilung mit der Suche nach der Datei. Diese fand die Liste auch und teilte dem Dienstgeber den Fundort im Dateisystem mit. Damit

war es jedoch nicht getan, weil sich die betroffene Mitarbeiterin in ihren Datenschutzrechten verletzt fühlte, denn die Datei lag in ihrem passwortgeschützten Bereich.

Die zuständige Datenschutzaufsicht hatte die Beschwerde abgewiesen, weil hier überhaupt keine Daten verarbeitet worden seien. Dies sahen die IDSG-Richter genauso und wiesen den Rechtsbehelf gegen den Bescheid ab. Zur Begründung schlossen sie sich den Ausführungen der Aufsicht an, dass die bloße Suche nach einer Datei noch keine Einsichtnahme im Sinne einer Verarbeitung sei. Lediglich der Speicherort der Datei weise einen Personenbezug auf. Die Verarbeitung dieses Datums sei jedoch durch das Erheben im Rahmen des Beschäftigungsverhältnisses gemäß § 53 Abs. 1 KDG rechtmäßig gewesen.

Das Gericht prüfte auch in aller Kürze einen möglichen Verstoß gegen das Grundrecht aus can. 220 CIC, der das Verbot beinhaltet, den guten Ruf oder die Intimsphäre einer anderen Person widerrechtlich zu verletzen. Eine Rufschädigung habe die Antragstellerin jedoch gar nicht geltend gemacht und eine Entscheidung darüber liege im Übrigen „nicht in der Zuständigkeit des Gerichts“. Des Weiteren sei eine Verletzung der Intimsphäre durch die IT-Maßnahmen nicht gegeben.

Eine gewisse Brisanz hatte der Fall auch, weil die Mitarbeiterin zugleich Vorsitzende der Mitarbeitervertretung war. Darauf ging das Gericht jedoch nicht näher ein. Es verwies in dem Zusammenhang darauf, dass in einem datenschutzrechtlichen Gerichtsverfahren nicht zu prüfen sei, ob hier das Vorgehen auch den Vorschriften der Mitarbeitervertretungsordnung entspreche.

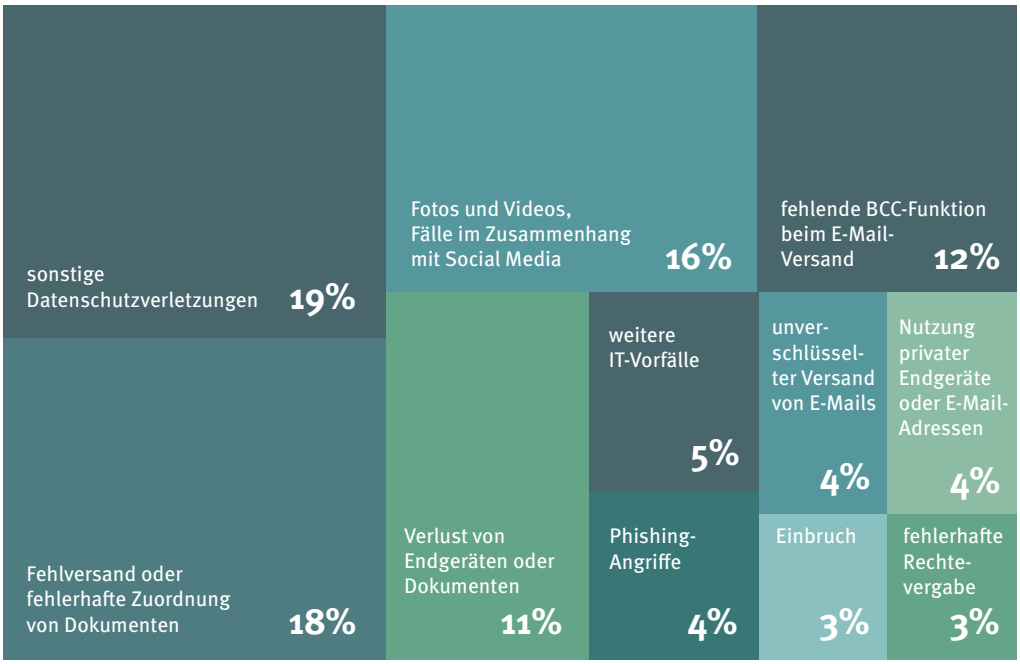
# 3 Schwerpunkte der Tätigkeiten im Berichtszeitraum

## 3.1 Datenschutzverletzungen

Eine Steigerung um knapp 30 % lässt sich bei den im Kath. Datenschutzzentrum Frankfurt/M. im Berichtsjahr eingegangenen Datenschutzverletzungen feststellen. Das ist eine deutliche Erhöhung, im Jahr 2024 war dagegen zum Vorjahr sogar ein leichter Rückgang zu verzeichnen gewesen.

Der Anteil der Meldungen aus dem Gesundheitswesen bleibt weiterhin stabil bei ca. 15 %, der größte Anteil der gemeldeten Datenschutzverletzungen mit 41 % kommt weiterhin aus den Bereichen der Kinder- und Jugend- sowie der Alten- und Behindertenhilfe.

**Gemeldete Datenschutzverletzungen nach Themenbereichen**




Die Zahl der mit IT-Sicherheit zusammenhängenden Datenschutzverletzungen ist geringfügig gestiegen, die fehlende BCC-Funktion beim E-Mail-Versand blieb im Berichtsjahr leider weiterhin konstant bei 12 %. So manches Mal mag es auf die Hektik im Arbeitsalltag zurückzuführen sein, wünschenswert wäre trotzdem eine rückläufige Zahl – allmählich müssten sich die Auswirkungen des „offenen E-Mail-Verteilers“ doch herumgesprochen haben.

Ein nicht zu unterschätzender – aber bei den Meldungen von Datenschutzverletzungen immer wieder zu findender – Fall ist die fehlerhafte Rechtevergabe. Zum einen werden häufig Rechte ohne die Beachtung des Need-to-know-Prinzips vergeben. Jeder Mitarbeitende sollte Zugriff nur zu den Informationen oder personenbezogenen Daten erhalten, die für die Erfüllung der Aufgabe unmittelbar erforderlich sind. Zum anderen fehlen teilweise definierte Prozesse, die dafür sorgen, dass einmal vergebene Zugriffsrechte sowohl regelmäßig auf ihre weiterhin bestehende Notwendigkeit geprüft als auch – sofern erforderlich – unmittelbar gelöscht

werden, zum Beispiel wenn eine Mitarbeiterin oder ein Mitarbeiter das Unternehmen oder die Einrichtung verlässt.

In einem dem Kath. Datenschutzzentrum Frankfurt/M. gemeldeten Fall wurden die Zugriffsrechte eines Praktikanten nach Beendigung des Praktikums nicht gelöscht und dieser konnte – und hat sich auch – noch Wochen später in das System eingeloggt.

Als Datenschutzverletzungen wurden der Datenschutzaufsicht auch Fälle von Verlusten elektronischer Endgeräte gemeldet. In einem Fall tauchte ein Laptop, der an einer Bushaltestelle vergessen worden war, nach Monaten wieder auf, sein zwischenzeitlicher Aufenthaltsort blieb unbekannt. Das Gerät wurde vor seinem Verschwinden von mehreren Personen benutzt und war deshalb „der Einfachheit halber" weder passwortgeschützt noch mit einer Festplattenverschlüsselung versehen. Nach seinem Wiederauftauchen wurden diesbezüglich Änderungen vorgenommen, die mit dem Laptop arbeitenden Personen haben auf Empfehlung der Datenschutzaufsicht an einer Datenschutzschulung teilgenommen.

### *3.1.1 Ist der Mailversand ohne BCC in einer Kita quasi „der Standard"?*

Diese Frage beschäftigte die Datenschutzaufsicht, nachdem bei der Bearbeitung einer eher unspektakulären Datenschutzverletzung, sprich eines Mail-Versands mit offenem Verteiler, auffiel, dass just diese Art von Datenschutzverletzung in ein und derselben Einrichtung in einem relativ kurzen Zeitraum gleich fünfmal passiert war. Und das, obwohl nach jeder einzelnen Meldung erneute Sensibilisierungen stattgefunden hatten.

Die Hinweise des Kath. Datenschutzzentrums Frankfurt/M., dass in der betreffenden Einrichtung sowohl die technischen und organisatorischen Maßnahmen als auch die dem Umgang mit personenbezogenen Daten beim E-Mail-Versand zugrunde liegenden Prozesse dringend geprüft, gegebenenfalls nachgebessert und angepasst werden sollten, wurden vom Verantwortlichen aufgenommen und die entsprechenden Maßnahmen unmittelbar umgesetzt. Die Datenschutzaufsicht konnte aus diesem Grund von weiteren Maßnahmen absehen.

Hier zeigt sich deutlich, dass zum Prozess beim Umgang mit Datenschutzverletzungen nicht nur das Erkennen einer solchen, die Festlegung der einzelnen Prozessschritte und die Einhaltung des gesetzlich definierten Meldewegs gehören. Vielmehr gehört auch die im KDG ebenfalls festgeschriebene Dokumentation der Datenschutzverletzung dazu, die es erst ermöglicht, wiederkehrende Muster zu lokalisieren und adäquate Abhilfe zu schaffen.

### *3.1.2 „Stay Informed", aber nicht alle Informationen sind auch für alle gedacht!*

Um im täglichen Kita-Betrieb Informationen zwischen Eltern, Verantwortlichem und Mitarbeitenden schnell und unkompliziert austauschen zu können, kommen in vielen Einrichtungen mittlerweile entsprechende Apps zum Einsatz, unter anderem auch die Anwendung „Stay Informed".

Allerdings bedeutet das nicht, dass über eine solche Kommunikations-App alle Informationen auch stets an alle weitergegeben werden sollten. Im Fall einer dem Kath. Datenschutzzentrum Frankfurt/M. gemeldeten Datenschutzverletzung wurden die Schwangerschaft einer Mitarbeiterin und das damit einhergehende Beschäftigungsverbot über „Stay Informed“ kommuniziert, und zwar ohne das Einverständnis der betroffenen Beschäftigten.

Auch wenn die Bekanntgabe der Schwangerschaft in guter Absicht geschah, um bei eventuell auftretenden Betreuungsengpässen frühzeitig um Verständnis bei den Eltern zu werben, so handelte es sich hier jedoch eindeutig um die Übermittlung von besonderen Kategorien personenbezogener Daten ohne Rechtsgrundlage. Dies wurde durch die Datenschutzaufsicht festgestellt und es wurde ein Bescheid mit entsprechenden Anordnungen erlassen, die vom Verantwortlichen fristgerecht umgesetzt wurden.

### *3.1.3 Keine Schlüsselrückgabe trotz Beendigung des Beschäftigungsverhältnisses*

Bei der oben beschriebenen, häufig etwas vernachlässigten Rechtevergabe geht es um die Zugriffsrechte auf Daten, wobei im Fokus des Kath. Datenschutzzentrums Frankfurt/M. hier die personenbezogenen Daten stehen. Doch nicht nur Zugriffs- auch Zugangsrechte sollten unter datenschutzrechtlichen Gesichtspunkten betrachtet werden.

Der Datenschutzaufsicht wurde im Jahr 2025 eine Datenschutzverletzung gemeldet, in der es darum ging, dass ein Mitarbeiter einer Kita nach Beendigung seines Beschäftigungsverhältnisses – trotz mehrfacher Aufforderung – nicht bereit war, die ihm für seine Tätigkeit überlassenen Schlüssel zurückzugeben. Für einige Wochen bestand demnach die Möglichkeit, dass er sich Zugang zur Kita und somit auch zu personenbezogenen Daten hätte verschaffen können.

Um die Sicherheit der in der Kita vorhandenen personenbezogenen Daten sicherzustellen, wurde seitens der Einrichtungsleitung geprüft, dass jene sich in einem abschließbaren Schrank und zudem in einem abschließbaren Bereich befinden, zu dem der Schlüssel des ehemaligen Mitarbeiters nicht passt. Als finale Maßnahme wurde der Austausch der gesamten Schließanlage vorgenommen.

Zugangsrechte und deren Dokumentation sind also ebenfalls ein wichtiger Teil der technischen und organisatorischen Maßnahmen, die zum Schutz personenbezogener Daten ergriffen werden sollten. Dazu gehören Schlüssel- und Übergabeprotokolle sowie Dokumentationen darüber, welche Bereiche mit welchen Schlüsseln zugänglich sind.

## 3.2 Beschwerden

Bereits unter Punkt 2 „Entwicklung des Datenschutzes“ wurde die starke Zunahme der Beschwerden im Berichtsjahr thematisiert, die dem Vernehmen nach bei allen Datenschutzaufsichten festzustellen war.

Im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. hat sich die Anzahl der Beschwerden im Jahr 2025 gegenüber dem Vorjahr nahezu verdoppelt. Dabei lohnt sich ein Blick auf die Beschwerden aus dem Krankenhausumfeld: Nach einem Rückgang vom Jahr 2023 auf das Jahr 2024 hat sich deren Anzahl im aktuellen Berichtszeitraum mehr als verdreifacht und macht damit rund 36 % aller Beschwerden aus.

### *3.2.1 TikTok-Challenge führt zu „verschlüsseltem“ Toilettenzugang*

Dass Social Media und Datenschutz nicht immer leicht in Einklang zu bringen sind, wird allerorten deutlich. Manchmal jedoch zeigt TikTok sogar indirekt datenschutzrechtliche Auswirkungen.

Im Rahmen einer beim Kath. Datenschutzzentrum Frankfurt/M. eingereichten Beschwerde, die aufgrund der Sachlage als Hinweis gewertet wurde, wurde bemängelt, dass an einer Schule der Zugang zu den Toiletten nur noch dann möglich sei, wenn im Sekretariat der Schlüssel abgeholt und der Name des oder der Abholenden in eine Liste eingetragen werde. Der Hinweisgeber sah darin einen Datenschutzverstoß, da personenbezogene Daten ohne Rechtsgrundlage erhoben worden seien, zudem eine Art Profiling vorläge und die Liste für Dritte einsehbar aufbewahrt werde.

Im Rahmen der Sachverhaltsaufklärung stellte sich heraus, dass die getroffene Maßnahme zum einen nur für einen sehr kurzen Zeitraum Bestand hatte, zum anderen die Notwendigkeit der Durchführung auf eine TikTok-Challenge zurückzuführen war, die Schülerinnen und Schüler dazu verleiten sollte, ihre Notdurft bewusst neben, statt in Toiletten zu verrichten. Ein Phänomen, das Schulen wohl bundesweit betroffen hat.

Aus Sicht des für die Sauberkeit und Sicherheit der Schülerinnen und Schüler Verantwortlichen ist die ergriffene Maßnahme durchaus nachvollziehbar und aufgrund der Kürze der Durchführungszeit, stellte sich für die Datenschutzaufsicht nach der Stellungnahme des Verantwortlichen der Hinweis als erledigt dar. Grundsätzlich natürlich wünscht sich das Kath. Datenschutzzentrum Frankfurt/M. im Zusammenhang mit Plattformen wie TikTok eine gänzlich andere Art der „Verschlüsselung“.

### *3.2.2 Kein Recht auf Auskunft um jeden Preis*

Den Betroffenenrechten kommt sowohl im staatlichen wie auch im kirchlichen Datenschutz eine zentrale Rolle zu. Informationspflichten und Auskunftserteilungen gewährleisten für die Betroffenen Transparenz, und zwar sowohl zum Zeitpunkt der Datenerhebung als auch für den Zeitraum der Verarbeitung und Speicherung ihrer Daten.

> **„Eine Informationspflicht des Verantwortlichen besteht nicht, wenn „wegen überwiegender berechtigter Interessen Dritter [die Daten] geheim gehalten werden müssen und das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss, …“ (§ 15 Abs. 5 KDG).**

Es finden sich im KDG jedoch auch Regelungen, die festlegen, wann das Recht auf Auskunft nicht mehr besteht. Dies ist zum Beispiel dann der Fall, wenn Daten wegen „überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen“.

Beim Kath. Datenschutzzentrum Frankfurt/M. wurde im Berichtsjahr eine Beschwerde eingereicht, in der ein nicht erfülltes Auskunftsbegehren Gegenstand war. Im Rahmen der Sachverhaltsaufklärung stellte sich heraus, dass bei einer Veranstaltung der Kirchengemeinde Anwesende vom Beschwerdeführer nicht nur mit Wein (der eigentlich zum Genuss gedacht war) überschüttet wurden, sondern auch mit erheblichen unangebrachten verbalen Äußerungen. Diese waren der Bibel entliehen und deuteten drohendes Ungemach für die Anwesenden an.

Vor diesem Hintergrund wurde das Auskunftsersuchen des Beschwerdeführers nicht erfüllt, weil weitere unangemessene Reaktionen seinerseits auf möglicherweise in der zu erteilenden Auskunft namentlich genannte Dritte nicht auszuschließen waren. Die berechtigten Interessen dieser Dritten, die in diesem Fall in deren körperlicher Unversehrtheit liegen, überwiegen das Recht auf Auskunft; die Rechtsgrundlagen dafür finden sich in den §§ 15 und 17 KDG.

## 3.3 Anfragen

Bei den im Berichtszeitraum im Kath. Datenschutzzentrum Frankfurt/M. eingegangenen Anfragen lässt sich thematisch kein Schwerpunkt erkennen, nahezu alle Bereiche der Zuständigkeit waren betroffen: Gesundheitswesen, Kinder- und Jugendhilfe, Kirchengemeinden, Schulen, Altenhilfe.

Während sich die Anzahl der Anfragen vom Jahr 2023 zum Jahr 2024 leicht verringert hatte, ist sie im Jahr 2025 angestiegen – und zwar um ca. 45 %. Dabei erstreckten sich die Themenbereiche von der Frage zur Verwendung von Fotos auf Webseiten über die Verschlüsselung von E-Mails und Hardware bis hin zum Einsatz einer Videoüberwachung. Auch komplexe Zusammenhänge wie geltendes Recht bei ökumenischen Einrichtungen und konkrete Fragestellungen zur Datenschutzfolgenabschätzung (DSFA) waren zu finden.

Wie verzwickt manches Mal die Beantwortung einer bloßen Frage zur zuständigen Aufsicht im kirchlichen Datenschutz sein kann, zeigte eine Beschwerde im Jahr 2025 aus dem Hochschulbereich: Ein Akademiker wollte sich über einen an einer Universität im

südwestlichen Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. tätigen anderen Akademiker beschweren.

Die Hochschule wirkte auf den ersten Blick katholisch, deren Trägerschaft erschloss sich aber anhand der Angaben auf der Website nicht so ohne weiteres. Ein Blick in die Datenschutzerklärung half auch nicht weiter, war diese doch stramm auf DSGVO gebürstet und enthielt noch nicht einmal Spuren des KDG – geschweige denn des eigentlich einschlägigen KDG-OR.

Denn weitere Recherchen ergaben schließlich, dass die Uni dem Ordensdatenschutz unterfällt und die Beschwerde im Hochschulmilieu daher an den entsprechenden Ordensdatenschutzbeauftragten abzugeben ist, der die Angelegenheit dann auch weiter betreute.

Betrachtet man nur den zur Klärung der Zuständigkeit betriebenen Aufwand, ist leicht vorstellbar, vor welchen Herausforderungen staatliche Datenschutzbehörden stehen, wenn diese einen Datenschutzvorfall an die entsprechenden Stellen im kirchlichen Datenschutz abgeben möchten bzw. müssen.

## 3.4 Gerichtsverfahren

Erfreulicherweise war im Berichtsjahr nur ein moderater Anstieg von Klagen gegen Bescheide des Kath. Datenschutzzentrums Frankfurt/M. festzustellen.

Eine davon hat es vom Umfang her allerdings in sich, bewegt dieser sich doch im Gigabyte-Bereich – viel Lesestoff für die ehrenamtlichen Richterinnen und Richter beim IDSG in Bonn. Für die Aufsicht stellen solche Umfänge zwischenzeitlich allerdings keine Ausnahme mehr dar. Das Mitteilungsbedürfnis des einen oder anderen Petenten scheint kaum Grenzen zu kennen. Das Herausarbeiten des eigentlich datenschutzrechtlich Relevanten erinnert dann oftmals an das Suchen der berühmten Nadel im Heuhaufen. Aber bekanntlich braucht man hierzu nur einen entsprechend starken Magneten.

Zwei vor dem IDSG anhängige Verfahren konnten im Sommer 2025 mit Vergleichen der Parteien und jeweils reduzierten Bußgeldern schließlich erledigt werden. In diesen Fällen konnte die Datenschutzaufsicht aufgrund besonderer – oder vielleicht noch treffender – absolut außergewöhnlicher Vorkommnisse in der Rechtsabteilung des Verantwortlichen diesem bei den Höhen der Bußgelder wie vom Gericht angeregt entgegenkommen.

Einige Verfahren verharren in der ersten Instanz, andere sind in die zweite Instanz gegangen bzw. befinden sich dort teils schon seit Längerem.

Ein Verfahren, in dem ein Verband nicht mit einem Bescheid und vor allem nicht mit den darin enthaltenen Anordnungen einverstanden war, konnte vor dem IDSG im Berichtszeit-

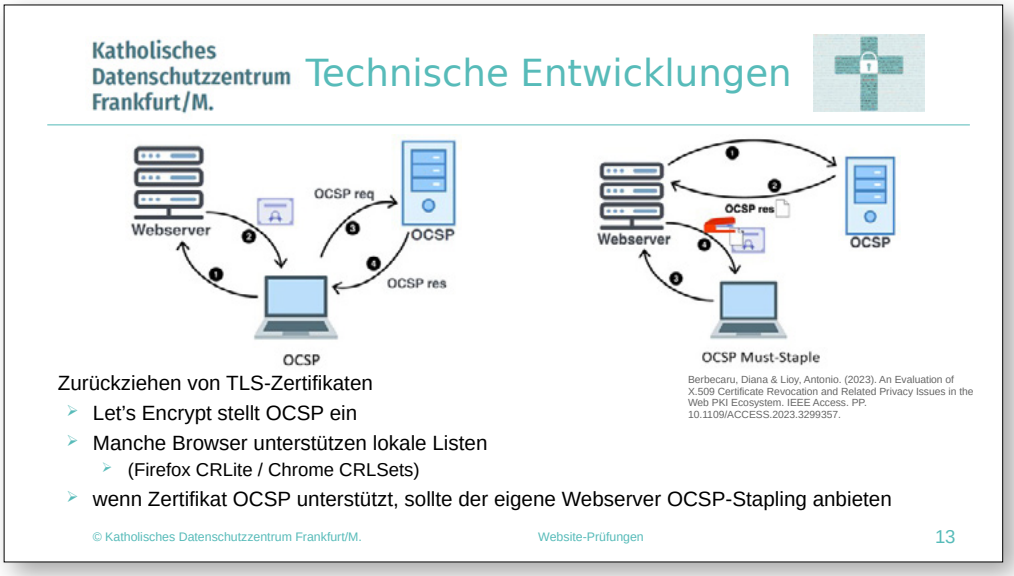
raum aus Sicht der Datenschutzaufsicht erfolgreich abgeschlossen werden, ist aber wie so viele zwischenzeitlich umgehend eine Instanz höher zur Überprüfung gewandert.

Ein Uralt-Verfahren konnte im Berichtszeitraum endlich zu einem zumindest aus Sicht der Aufsicht guten Ende gebracht werden. Die zweite Instanz hatte noch einmal genau nachgerechnet und festgestellt, dass der Antragsteller einen Tag zu früh sein Rechtsmittel gegen eine angebliche Untätigkeit der Datenschutzaufsichtsbehörde eingelegt hat – und deshalb die Klage nach Jahren nunmehr kurz und knackig als unzulässig zurückgewiesen. Wie bereits dazu im letzten Tätigkeitsbericht für das Jahr 2024 berichtet wurde, war in diesem Verfahren von den ursprünglichen Beteiligten nur noch die Datenschutzaufsicht übrig, weil sowohl die damalige Einrichtungsleitung, der zuständige betriebliche Datenschutzbeauftragte als auch der früher dort beschäftigte Petent nicht mehr in dem Betrieb tätig sind.

## 3.5 Prüfungen

Neben Vor-Ort-Prüfungen von katholischen Hochschulen im Zuständigkeitsbereich setzte das Kath. Datenschutzzentrum Frankfurt/M. seine Prüfungen von Schul-Websites fort. Die bereits im Jahr 2024 vorgenommenen technischen Prüfungen von über 240 Internetseiten zeigten teils erhebliche datenschutzrechtliche Mängel auf. Deshalb wurde im Frühjahr 2025 eine erneute großflächige Prüfung der Websites katholischer Schulen durchgeführt. Hierbei konnten jedoch keine wesentlichen Veränderungen im Vergleich zu den zuvor erfolgten Prüfungen festgestellt werden – mit anderen Worten: Die seinerzeit festgestellten datenschutzrechtlich problematischen Auffälligkeiten im überwiegenden Teil der Schul-Websites waren nach wie vor vorhanden.

**Kriterien bei der Prüfung von Schul-Websites**




Aus diesem Grunde schließen sich an diese Querschnittsprüfungen nunmehr Tiefenprüfungen einzelner Internetauftritte von Schulen an, die Sensibilisierung der Verantwortlichen wird ebenfalls fortgesetzt.

Das Kath. Datenschutzzentrum Frankfurt/M. kommt mit diesen Prüfungen seinen gesetzlichen Verpflichtungen als Datenschutzaufsicht, insbesondere seiner in § 44 Abs. 2 lit. a) KDG beschriebenen Beratungsfunktion, nach.

Als datenschutzrechtliche Aufsichtsbehörde führt die katholische Datenschutzaufsicht in unregelmäßigen Abständen bei den im Zuständigkeitsbereich befindlichen Einrichtungen anlasslose Prüfungen durch, die sowohl technische als auch organisatorische Aspekte des Datenschutzes betreffen. Dabei werden wie bei den Website-Prüfungen Datenschutzmaßnahmen gleichartiger Einrichtungen untersucht, um die gesetzeskonforme Umsetzung des Datenschutzes festzustellen und auf verbesserungswürdige oder gegebenenfalls sogar fehlerhafte Aspekte hinweisen zu können.

## 3.6 Umfrage zum Umgang mit Datenschutzverletzungen

Bereits im letztjährigen Tätigkeitsbericht war über eine Sensibilisierungsmaßnahme des Kath. Datenschutzzentrums Frankfurt/M. zu lesen, die gemeinsam mit der Katholischen Datenschutzaufsicht Nord durchgeführt wurde. Gestartet wurde diese Maßnahme, die in Form einer Umfrage stattfand, bereits im Jahr 2024.

Im Rahmen der allgemeinen Zusammenarbeit mit der Katholischen Datenschutzaufsicht Nord wurde festgestellt, dass beide Datenschutzaufsichten in ihren jeweiligen Zuständigkeitsgebieten bei der regelmäßigen Auswertung und Clusterung von gemeldeten Datenschutzverletzungen die gleichen Auffälligkeiten wahrgenommen hatten: Art, Menge und Güte der Meldungen zeigten eine erhebliche Bandbreite. Darüber hinaus wurde auch im Zusammenhang mit Beschwerdeverfahren festgestellt, dass einige Einrichtungen noch immer kein geregeltes Verfahren zum Umgang mit Datenschutzverletzungen haben.

Es entstand die Idee, auf der Grundlage von § 44 KDG, in dem die Aufgaben der Datenschutzaufsicht festgeschrieben sind, eine gemeinsame Kampagne durchzuführen, um die Verantwortlichen und die handelnden Personen in den Einrichtungen zum Umgang mit Datenschutzverletzungen zu sensibilisieren. Dabei standen drei Fragestellungen im Vordergrund:

- Wird als Datenschutzverletzung gemeldet, was gemeldet werden muss?
- Wird korrekt benachrichtigt?
- Werden Datenschutzverletzungen wie erforderlich dokumentiert?

Abseits des primären Ziels, der Sensibilisierung der handelnden Personen, sollte die Umfrage noch weitere Ergebnisse liefern: Das Erkennen von Verbesserungsmöglichkeiten, die Mitteilung der gewonnen Erkenntnisse an und den Austausch darüber mit den betrieblichen Datenschutzbeauftragten und nicht zuletzt die Erfüllung der im KDG festgeschriebenen Aufgaben sowohl der Datenschutzaufsicht als auch der betrieblichen Datenschutzbeauftragten.

Der wichtigste Punkt des Konzepts war von Beginn an, dass es nicht um die Aufarbeitung vergangener Meldungen gehen sollte, sondern um das Erkennen von Verbesserungspotenzialen für die Bearbeitung zukünftiger Datenschutzverletzungen.

Interessant erschien im Kontext der gemeinsamen Durchführung auch eine erweiterte Frage: Im Vorfeld wurden die gleichen Auffälligkeiten konstatiert – werden sich bei paralleler Durchführung der Umfrage ähnliche oder unterschiedliche Ergebnisse für die beiden Datenschutzaufsichten zeigen?

Insgesamt wurden in den beiden Behörden jeweils mehr als 100 Einrichtungen aus deren Zuständigkeitsgebieten angeschrieben und zur Teilnahme an der verpflichtenden Umfrage aufgefordert. Dabei wurden verschiedene Einrichtungsarten einbezogen, um einen Querschnitt abzubilden, und es wurde eine gleichmäßige Verteilung der teilnehmenden Einrichtungen auf die (Erz-)Bistümer der Zuständigkeitsbereiche angestrebt. Zur Teilnahme wurden die Verantwortlichen der Einrichtungen aufgefordert, nicht die betrieblichen Datenschutzbeauftragten oder übergeordnete Organisationen.

Zunächst wurden in der Umfrage rein quantitative Fragen zu festgestellten und gemeldeten Datenschutzverletzungen und zu daraus resultierenden Benachrichtigungen betroffener Personen gestellt. Dabei wurde auch die Zusendung von entsprechenden Dokumentationen erbeten, um nachvollziehen zu können, ob die Einordnung der Datenschutzverletzungen als meldepflichtig bzw. nicht meldepflichtig korrekt war. Anschließend stand im Fokus der Umfrage vor allem der Prozess zum Umgang mit Datenschutzverletzungen: Liegt er definiert und idealerweise in verschriftlichter Form vor und wird er in der Einrichtung auch gelebt? Wie wird den Mitarbeitenden dieser Prozess vermittelt und wird er einer regelmäßigen Evaluation unterzogen? Darüber hinaus schlossen sich Fragen zu Vertretungsregelungen für die zuständigen Personen, zur Art und Weise und zu den Aufbewahrungsorten der Dokumentationen festgestellter Datenpannen an. Auch der Regelmäßigkeit und der Art der Sensibilisierung der mit der Verarbeitung von personenbezogenen Daten betrauten Mitarbeitenden waren Fragen gewidmet.

Die teilnehmenden Einrichtungen kamen aus ganz unterschiedlichen Bereichen und es wurden Einrichtungen jeder Größe befragt, dabei handelte es sich um Gesundheitseinrichtungen, Beratungsstellen, Vereine und Verbände, Einrichtungen der Altenhilfe, Kindertagesstätten und Kirchengemeinden. Dass die von den Einrichtungen in der Umfrage mitgeteilten Informationen deshalb sehr unterschiedlich ausfallen würden, war beinahe erwartbar. Es zeigten sich jedoch auch innerhalb der befragten Gruppen deutliche Unterschiede beim Umgang mit Datenschutzverletzungen.

Zusammenfassend lässt sich sagen: Es war alles dabei. Die Bandbreite reichte vom versierten und verantwortungsvollen Umgang mit personenbezogenen Daten bis hin zur Aussage „personenbezogene Daten haben wir nicht“ (die übrigens von einer Kirchengemeinde kam).

Katholisches Datenschutzzentrum Frankfurt/M.

## 1. Idee und Zielsetzung (4)

**Zielsetzung:**

- Erkennen von Verbesserungsmöglichkeiten
- Mitteilung der gewonnen Erkenntnisse an und Austausch darüber mit den bDSBs
- Erfüllung der im KDG festgeschriebenen Aufgaben sowohl der Datenschutzaufsicht als auch der bDSBs
- Sensibilisierung der handelnden Personen

7

Katholisches Datenschutzzentrum Frankfurt/M.

## 7. Erkenntnisse und Perspektiven (1)

**ES WAR ALLES DABEI:**

| | VON | BIS |
|---|---|---|
| Personenbezogene Daten | „versierter und verantwortungsvoller Umgang damit“ | „personenbezogene Daten haben wir nicht“ |
| Datenschutzverletzungen | „eindeutiges Erkennen von Datenschutzverletzungen“ | „kommen bei uns nicht vor“ |
| Verfahren zum Umgang mit Datenschutzverletzungen | „ausführlich beschrieben und im QM-Handbuch enthalten“ | „gibt‘s bei uns nicht“ |

© Kath

**Auszüge aus dem Vortrag: Umfrage zum Umgang mit Datenschutzverletzungen**

Katholisches Datenschutzzentrum Frankfurt/M.

## 7. Erkenntnisse und Perspektiven (3)

**Verbesserungspotenziale Vereine/Verbände**


- **Ehrenamtsbereich** benötigt grundsätzlich **mehr Aufmerksamkeit** hinsichtlich der datenschutzrechtlichen Sensibilisierung
- mehr **aktive** Hilfestellung
- Verbreitung des Themas **„in die Tiefe“** (nicht nur auf Vorstandsebene)
- **Bewusstsein** schaffen, dass das KDG auch im Ehrenamtsbereich Anwendung findet
- Rolle der **bDSBs** der Ordinariate **kommunizieren** – Dort sind Expertise und Hilfestellungen vorhanden.
- **Klarstellung:** Ja, das Kath. Datenschutzzentrum Frankfurt/M. gibt es wirklich!

© Katholisches Datenschutzzentrum Frankfurt/M. Austauschtreffen bDSB Ordinariate – 04.11.2025 23

Selbst in großen Einrichtungen, die in der Regel über ausreichende Ressourcen und damit auch meist über entsprechend gut implementierte Datenschutzprozesse verfügen, zeigten sich Verbesserungspotenziale in den Bereichen der Feststellung der Meldepflicht und der Dokumentation von Datenschutzverletzungen. Und obwohl bei vielen Einrichtungen mittlerer Größe eine übergeordnete, deutlich größere Organisation dahintersteht, hat der – möglicherweise in der übergeordneten Organisationseinheit schriftlich vorliegende Prozess zum Umgang mit Datenschutzverstößen – nicht immer den Weg bis in jede einzelne untergeordnete Einrichtung geschafft.

Ein Großteil der an der Umfrage beteiligten Vereine und Verbände gehört dem Ehrenamtsbereich an. Die Umfrage hat in diesem Sektor deutliche Verbesserungspotenziale beim Umgang mit Datenschutzverletzungen offenbart, vor allem hinsichtlich der festgelegten bzw. möglichst verschriftlichten Prozesse und der Sensibilisierungsmaßnahmen für die handelnden Personen. Zusätzlich hat sich aber auch gezeigt, dass diesem Bereich grundsätzlich mehr Aufmerksamkeit zum Thema Datenschutz zukommen sollte. Das Bewusstsein für personenbezogene Daten und deren Verarbeitung im Allgemeinen, die Anwendung des KDG auch im Ehrenamtsbereich, die Verbreitung des Themas in die Tiefe (und nicht nur auf Vorstandsebene), die Bekanntmachung bereits vorhandener Hilfestellungen – all dies sind Punkte, die die ehrenamtlich Tätigen in ihren datenschutzrechtlichen Bemühungen unterstützen können.

Die nach Abschluss der Umfrage angekündigte Hilfestellung zum Umgang mit Datenschutzverletzungen war bis zum Redaktionsschluss für den vorliegenden Tätigkeitsbericht noch nicht fertiggestellt, sodass darüber im kommenden Jahr zu berichten sein wird.

# 4 Veranstaltungen und Öffentlichkeitsarbeit

Das Kath. Datenschutzzentrum Frankfurt/M. bot natürlich auch im Jahr 2025 wieder Schulungs- und Fortbildungsveranstaltungen an, die aufgrund großer Nachfrage teils in externen Räumlichkeiten stattfanden. Bei den schon traditionellen Austauschtreffen mit den betrieblichen Datenschutzbeauftragten der Bischöflichen Ordinariate als auch mit den betrieblichen Datenschutzbeauftragten und -koordinatoren aus dem Caritas-, Kita- und Heimbereich ging es thematisch schwerpunktmäßig um die durchgeführten Schul-Websiteprüfungen und die großflächige Umfrage zum Umgang mit Datenschutzverletzungen bei den Verantwortlichen vor Ort. Die vorgestellten Ergebnisse wurden im Anschluss in konstruktiver Atmosphäre diskutiert. Aufgrund zahlreicher Anfragen im Vorfeld der Veranstaltungen wurde das im Sommer 2025 aufgekommene komplexe Thema der neuen teils 100-jährigen Aufbewahrungsfristen für Kinder- und Jugendhilfeakten nach § 9b SGB VIII und dem Umgang damit in der Praxis mitaufgenommen und eingehend behandelt. Der intensive fachliche Austausch der Teilnehmerinnen und Teilnehmer und der Mitarbeiterinnen und Mitarbeiter der Datenschutzaufsicht zeigte wieder einmal die aktuellen datenschutzrechtlichen Herausforderungen in der täglichen Praxis.


**Auf den Veranstaltungen des Kath. Datenschutzzentrums Frankfurt/M. wurde auch über aktuelle Herausforderungen im Datenschutz referiert und ausgiebig diskutiert.**


Die Belegschaft des Kath. Datenschutzzentrums Frankfurt/M. nutzte im Jahr 2025 auch wieder zahlreiche Fortbildungsmöglichkeiten, so zum Beispiel den alljährlichen Europäischen Datenschutztag in Berlin oder den 4. Datenschutztag Hessen & Rheinland-Pfalz bei tropischen Außentemperaturen. Die letztgenannte Veranstaltung zeigte anschaulich auf, wie menschenzentrierte Digitalisierung gelingen kann und bot auch wieder reichlich Möglichkeiten zum fachlichen Austausch zu aktuellen datenschutzrechtlichen Themen. Die gemeinsame Veranstaltung von Hessen und Rheinland-Pfalz fand in Frankfurt am Main unter dem Motto „Information Overload? Über- und Durchblick für Datenschutzbeauftragte“ statt.


**Die Landesdatenschutzbeauftragten der beiden Bundesländer, Prof. Alexander Roßnagel und Prof. Dieter Kugelmann, diskutierten mit der rheinland-pfälzischen Digitalministerin Dörte Schall auf dem 4. Datenschutztag über die Stärkung der digitalen Selbstbestimmung der Bürgerinnen und Bürger.**

Des Weiteren lud der rheinland-pfälzische Landesdatenschutzbeauftragte Herr Prof. Dieter Kugelmann anlässlich seines zehnjährigen Amtsjubiläums im Oktober 2025 zu einem wissenschaftlichen Symposium („Zehn Jahre Datenschutz im Wandel“) ins Landesmuseum Mainz und knapp einen Monat später in den Plenarsaal des rheinland-pfälzischen Landtags zu einer gemeinsamen Veranstaltung mit der Verbraucherzentrale mit dem Titel: „ePA für alle – Daten für alle?“.

Um „Bürokratieabbau im Datenschutz“ ging es schließlich in einem vom hessischen Landesdatenschutzbeauftragten Herrn Prof. Alexander Roßnagel zusammen mit der Präsidentin des Hessischen Landtages, Frau Astrid Wallmann, veranstalteten Forum, das im Frühjahr 2025 von einigen Mitarbeitenden der Frankfurter Datenschutzaufsicht erkenntnisreich besucht wurde.

# 5 Vernetzung mit anderen Datenschutzaufsichten

Der 10. Ökumenische Datenschutztag hat im Frühjahr 2025 in Frankfurt/M. stattgefunden. Das Kath. Datenschutzzentrum Frankfurt/M. hatte dieses Mal die evangelischen und katholischen Kolleginnen und Kollegen aus den verschiedenen Datenschutzaufsichten zu dem jährlichen Treffen eingeladen. Thematisiert und diskutiert wurden bei diesem anregenden und intensiven Austausch unter anderem die Novellierungen der Datenschutzgesetze, das Kirchliche Datenschutzmodell (KDM) sowie der Datenschutz im Kontext von Missbrauch und Unabhängigen Aufarbeitungskommissionen – und hier vor allem die datenschutzrechtliche Verantwortlichkeit der Akteure.

Abgerundet wurde die Konferenz bei bestem Wetter mit einem aufschlussreichen und kurzweiligen Besuch der Frankfurter Börse und später ausklingen lassen bei typisch Frankfurter Küche und „Ebbelwoi“.

**Der Ökumenische Datenschutztag fand im Jahr 2025 in Frankfurt am Main statt. Einem intensiven Austausch über aktuelle datenschutzrechtliche Themen schloss sich ein abwechslungsreicher Besuch der Frankfurter Börse an.**

Die fünf katholischen Datenschutzaufsichten haben ihren engen und regelmäßigen Austausch auch im Berichtszeitraum fortgesetzt. Sprecher der Konferenz der Diözesandatenschutzbeauftragten war im Jahr 2025 Herr Dominikus Zettl vom Katholischen Datenschutzzentrum Bayern, das seinen Sitz in Nürnberg hat.

Der regelmäßige Austausch mit den staatlichen Datenschutzaufsichten der Bundesländer Baden-Württemberg, Hessen, Rheinland-Pfalz und Saarland, in denen die sieben vom Frankfurter Datenschutzzentrum beaufsichtigten (Erz-)Bistümer oft länderübergreifend beheimatet sind, wurde auch im Jahr 2025 fortgesetzt. Anwesend bei den verschiedenen informativen Treffen waren auch dieses Mal wieder neben Frau Monika Grethel, Herrn Prof. Dieter Kugelmann und Herrn Prof. Alexander Roßnagel jeweils einzelne Fachreferenten aus den Landesdatenschutzaufsichten zu speziellen Fragestellungen.

Die IT’lerinnen und IT’ler der katholischen Datenschutzaufsichten tauschten sich auch im Berichtsjahr wieder mit ihren Kolleginnen und Kollegen bei den staatlichen Datenschutzbehörden aus. Mitarbeiterinnen und Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. stellten unter anderem beispielsweise bei einem der Treffen die Methodik und die technische Umsetzung der durchgeführten flächendeckenden Website-Prüfungen vor.

Mitarbeiterinnen und Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. nehmen neben den Arbeitskreisen (AK) Gesundheit und Soziales sowie Schule und Bildung nunmehr auch an den regelmäßigen Sitzungen des AK KI der Datenschutzkonferenz teil.

# 6 Ausblick

Digitalisierung zu intensivieren heißt auch immer, innovativ zu denken und zu handeln. Oftmals wird in diesem Zusammenhang der Datenschutz als Bremser oder gar Verhinderer der Innovation gesehen. Dies zu widerlegen und diesem Denken vorzubeugen ist auch Aufgabe der Datenschutzaufsichten, denn indem durch die Zusammenarbeit von Gesetzgebung und Datenschutzaufsicht rechtssichere Räume entstehen, können Innovation und Datenschutz Hand in Hand gehen.

Ausgestaltung der Digitalisierung zum Wohle der Menschen und der Gesellschaft bei gleichzeitiger Beachtung der datenschutzrechtlichen Vorgaben – dies ist eine große Aufgabe, die unmittelbare Auswirkungen auch auf die Datenschutzaufsichten hat.

Digitalisierung wird fortschreiten, dies ist wohl allgemeiner Konsens. Doch je nachdem, wie die Gestaltung der Digitalisierung ausfällt, kann dies auch fortschreitende Abhängigkeit bedeuten, und zwar in zweierlei Hinsicht.

Steht die Digitalisierung im Mittelpunkt und der Mensch und sein Leben müssen sich nach ihr richten? Wer ist für wen da? Gibt es ein Recht auf ein analoges Leben? Und was bedeutet das vor allem für nicht-technikaffine Menschen, die sicherlich in besonderem Maß unter den Älteren zu finden sind? Ist eine uneingeschränkte Teilnahme am sozialen Leben ohne permanente Unterstützung überhaupt noch möglich? Hier sind in einigen Bereichen des täglichen Lebens bereits jetzt Abhängigkeiten zu erkennen, denn manche Dienste oder Anwendungen werden nur noch digital angeboten oder die analoge Durchführung ist zumindest nur unter erschwerten Bedingungen zu erreichen.

Abhängigkeit zeigt sich darüber hinaus auch in der immer noch mangelnden digitalen Souveränität in Europa: Der Einsatz von Hard- und Softwareprodukten großer (zumeist US-amerikanischer) Tech-Konzerne wird in zu vielen Bereichen als gegeben und einzige Möglichkeit wahr- und hingenommen, eine Suche nach europäischen, eigenständigeren und datenschutzfreundlicheren Alternativen findet in der Praxis durchaus statt, jedoch noch nicht in ausreichendem Maß.

Datensouveränität vorantreiben und damit den Schutz personenbezogener Daten stärken – dies ist eine der großen Herausforderungen für die kommenden Jahre.

# 7 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland

**Der Diözesandatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.**

**Unser Lieben Frauen Kirchhof 20**
**28195 Bremen**
**Diözesandatenschutzbeauftragter:**
**Andreas Bloms**

**Katholisches Datenschutzzentrum (KdöR)**

**Brackeler Hellweg 144**
**44309 Dortmund**
**Diözesandatenschutzbeauftragter:**
**Steffen Pau**

**Kath. Datenschutzzentrum Frankfurt/M. KdöR**

**Roßmarkt 23**
**60311 Frankfurt/M.**
**Diözesandatenschutzbeauftragte:**
**Ursula Becker-Rathmair**

**Diözesandatenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs**

**Im Badepark 4**
**39218 Schönebeck**
**Diözesandatenschutzbeauftragter:**
**Matthias Ullrich**

**Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen**

**Vordere Sterngasse 1**
**90402 Nürnberg**
**Diözesandatenschutzbeauftragter:**
**Dominikus Zettl**


Quelle: https://www.katholisches-datenschutzzentrum.de

**Kath. Datenschutzzentrum Frankfurt/M.**

Tätigkeitsbericht 2025