KATHOLISCHES DATENSCHUTZZENTRUM BAYERN

6. Tätigkeitsbericht

Berichtsjahr 2025

Bistum Würzburg
Christsein unter den Menschen

BISTUM REGENSBURG

ERZBISTUM BAMBERG

BISTUM EICHSTÄTT

BISTUM PASSAU

BISTUM AUGSBURG

ERZDIÖZESE MÜNCHEN UND FREISING

Vorwort

> Datenschutz schützt die Würde des Menschen. Deshalb ist er für die Kirche nicht nur Recht, sondern Ausdruck ihrer Verantwortung.

Das Jahr 2025 hat einmal mehr verdeutlicht, dass Datenschutz kein Randthema kirchlicher Verwaltung ist, sondern ein wesentlicher Bestandteil glaubwürdigen kirchlichen Handelns. In einer Zeit fortschreitender Digitalisierung, wachsender Datenverarbeitung und zunehmender Sensibilität der Menschen für den Schutz ihrer persönlichen Informationen steht auch die Kirche in der Verantwortung, den Schutz der Privatsphäre als Ausdruck der Achtung der Menschenwürde zu gewährleisten.

Für die katholische Kirche ist Datenschutz dabei nicht allein eine rechtliche Verpflichtung, sondern auch eine ethische und pastorale Aufgabe. Der Schutz personenbezogener Daten berührt unmittelbar das Vertrauen der Gläubigen, der Mitarbeitenden und aller Menschen, die mit kirchlichen Einrichtungen in Kontakt stehen und mit ihren vielfältigen Dienstleistungen im Gesundheits- und Sozialbereich in Berührung kommen. Dieses Vertrauen zu wahren und zu stärken, bleibt ein zentrales Anliegen des Katholischen Datenschutzzentrums (KDSZ) Bayern.

Das Berichtsjahr 2025 war in besonderer Weise durch den Abschluss der umfassenden Überarbeitung des Gesetzes über den Kirchlichen Datenschutz (KDG) sowie der zugehörigen Durchführungsverordnung (KDG-DVO) geprägt. Mit der ersten grundlegenden Reform seit Inkrafttreten des KDG im Jahr 2018 wurde das kirchliche Datenschutzrecht an aktuelle rechtliche, technische und organisatorische Entwicklungen angepasst. Die praktische Umsetzung dieser Neuregelungen wird die Datenschutzpraxis in den kommenden Jahren maßgeblich prägen und bildet einen Schwerpunkt dieses Tätigkeitsberichts.

Neben diesen rechtlichen Entwicklungen veränderten insbesondere die fortschreitende Digitalisierung, der zunehmende Einsatz Künstlicher Intelligenz sowie die

wachsenden Anforderungen an Informationssicherheit und Cyberresilienz die Rahmenbedingungen kirchlicher Datenverarbeitung nachhaltig. Datenschutz lässt sich heute nicht mehr isoliert betrachten. Er steht in engem Zusammenhang mit sicheren technischen und organisatorischen Strukturen sowie einer verantwortungsvollen Gestaltung digitaler Prozesse. Zugleich gewinnt die digitale Souveränität kirchlicher Einrichtungen zunehmend an Bedeutung. Sichere, transparente und möglichst unabhängige digitale Infrastrukturen leisten einen wichtigen Beitrag zum Schutz personenbezogener Daten und stärken zugleich die langfristige Handlungsfähigkeit kirchlicher Organisationen.

Diese Entwicklungen spiegeln sich auch in der Arbeit des KDSZ Bayern wider. Besondere Aufmerksamkeit galt erneut der Beratung kirchlicher Einrichtungen erneut in der Beratung kirchlicher Einrichtungen sowie in der Entwicklung praxisnaher Handreichungen, Schulungsangebote und Informationsmaterialien. Die Erfahrung zeigt, dass frühzeitige Beratung und ein vertrauensvoller Dialog wesentlich dazu beitragen, datenschutzrechtliche Risiken bereits im Vorfeld zu erkennen und zu vermeiden. Gleichzeitig bleibt die unabhängige Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben ein unverzichtbarer Bestandteil unserer gesetzlichen Aufgaben. Beratung und Kontrolle stehen dabei nicht im Widerspruch, sondern ergänzen sich als gleichwertige Elemente einer modernen Datenschutzaufsicht.

Die zunehmende technische Komplexität, neue europäische und kirchliche Rechtsentwicklungen sowie der steigende Bedarf an qualifiziertem Fachwissen stellen kirchliche Einrichtungen und Datenschutzaufsichtsbehörden gleichermaßen vor neue Herausforderungen. Moderne Datenschutzaufsicht geht deshalb heute weit über klassische Kontroll- und Prüftätigkeiten hinaus. Beratung, Schulung, technische Expertise, Öffentlichkeitsarbeit und die Begleitung digitaler Transformationsprozesse sind zu wesentlichen Bestandteilen einer wirksamen Datenschutzaufsicht geworden. Diese Aufgaben werden die Arbeit des KDSZ Bayern auch künftig maßgeblich prägen.

Diese Weiterentwicklung spiegelt sich auch im vorliegenden Tätigkeitsbericht wider. Er erscheint erstmals in einem grundlegend überarbeiteten Layout und folgt einer neu strukturierten inhaltlichen Konzeption. Neben der Darstellung der gesetz-

lichen Aufgaben der Datenschutzaufsicht und der Entwicklungen des Datenschutzrechts geben zahlreiche Praxisbeispiele, Berichte aus der Beratungspraxis, Audits und Beschwerdeverfahren einen vertieften Einblick in die tägliche Arbeit des Katholischen Datenschutzzentrums Bayern. Ziel der Neugestaltung ist es, den Tätigkeitsbericht nicht nur als Rechenschaftsbericht, sondern zugleich als praxisnahe Orientierungshilfe für Verantwortliche, betriebliche Datenschutzbeauftragte und alle am kirchlichen Datenschutz Interessierten weiterzuentwickeln.

Mein besonderer Dank gilt den Mitarbeitenden unserer Behörde sowie allen Verantwortlichen und betrieblichen Datenschutzbeauftragten in den kirchlichen Einrichtungen, die sich mit großem Engagement für die Umsetzung datenschutzrechtlicher Vorgaben einsetzen. Ebenso danke ich allen, die durch Hinweise, Anfragen und konstruktive Kritik zur Weiterentwicklung des Datenschutzes beigetragen haben.

Der vorliegende Tätigkeitsbericht soll nicht nur Rechenschaft über die Arbeit des KDSZ Bayern ablegen, sondern zugleich Orientierung geben und Impulse für eine verantwortungsvolle, rechtssichere und menschenwürdige Gestaltung des Umgangs mit personenbezogenen Daten vermitteln. Ich wünsche Ihnen eine anregende Lektüre.

Dominikus Zettl
Gemeinsamer Diözesandatenschutzbeauftragter
für die bayerischen (Erz-)Diözesen und Leiter des
Katholischen Datenschutzzentrums Bayern (KdöR)

Inhaltsverzeichnis

Impressum

Herausgeber

Gemeinsamen Diözesandatenschutzbeauftragten für die bayerischen (Erz-)Diözesen Augsburg, Bamberg, Eichstätt, München und Freising, Passau, Regensburg, Würzburg

Katholisches Datenschutzzentrum Bayern (KdöR)

Datenschutzaufsicht für die bayerischen (Erz-)Diözesen

Vordere Sterngasse 1

90402 Nürnberg

Telefon
+49 911 4777405-0

E-Mail
post@kdsz.bayern

Internet
www.kdsz.bayern

Das Katholische Datenschutzzentrum Bayern ist eine Körperschaft des öffentlichen Rechts. Es wird durch den Diözesandatenschutzbeauftragten **Dominikus Zettl** vertreten.

Sprachliche Gleichbehandlung

Zur besseren Lesbarkeit wird in diesem Tätigkeitsbericht überwiegend das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter. Die gewählte Sprachform dient ausschließlich der sprachlichen Vereinfachung und enthält keine Wertung.

Veröffentlichung

Vorgelegt im Juli 2026

Der Verwaltungsrat hat beschlossen, aus Gründen der Nachhaltigkeit auf eine gedruckte Ausgabe zu verzichten. Der Tätigkeitsbericht wird ausschließlich in elektronischer Form veröffentlicht.

https://kdsz.bayern
https://datenschutzarchiv.org/zaftda

1 Das Katholische Datenschutzzentrum Bayern

Eine wirksame Datenschutzaufsicht setzt nicht nur rechtliche Expertise voraus. Ebenso entscheidend sind eine leistungsfähige Organisation, qualifizierte Mitarbeitende und eine sichere technische Infrastruktur. Dieses Kapitel gibt einen Überblick über die organisatorischen, personellen und technischen Entwicklungen des Berichtsjahres sowie über Maßnahmen, die die Leistungsfähigkeit des Katholischen Datenschutzzentrums Bayern (KDSZ Bayern) nachhaltig stärken.

1.1 Geschäftsbetrieb und Organisation

Der gesetzliche Auftrag des KDSZ Bayern reicht heute weit über die klassische Kontrolle datenschutzrechtlicher Vorgaben hinaus. Beratung, Prüfung, Schulung, technische Bewertung und Öffentlichkeitsarbeit bilden gemeinsam die Grundlage einer modernen Datenschutzaufsicht. Die organisatorische und technische Weiterentwicklung der Behörde war deshalb auch im Berichtsjahr 2025 ein wesentlicher Schwerpunkt.

Die Aufgaben des KDSZ Bayern entwickeln sich kontinuierlich weiter. Neben der klassischen Bearbeitung von Beschwerden und Datenschutzverletzungen gewinnen insbesondere Beratungsleistungen, technische Fragestellungen, Digitalisierungsprojekte sowie die Begleitung neuer europäischer Rechtsakte zunehmend an Bedeutung.

Gleichzeitig steigen die Anforderungen an Organisation, Personal und technische Infrastruktur. Die folgenden Abschnitte geben einen Überblick über die wichtigsten organisatorischen Entwicklungen des Berichtsjahres sowie über Maßnahmen zur Stärkung der Leistungsfähigkeit und digitalen Souveränität der Behörde.

Die nachfolgenden Abschnitte behandeln Personal • Digitale Souveränität • Diözesennetz • Öffentlichkeitsarbeit • KI-Konsultation • Ausblick

1.1.1 Personelle Situation und Aufgabenwahrnehmung

Im Berichtsjahr 2025 konnte das KDSZ Bayern seine Aufgaben nach dem personellen Aufbau der Vorjahre erstmals durchgängig mit vollständiger Besetzung wahrnehmen. Mit nunmehr fünf Mitarbeitenden war es möglich, die gesetzlichen Aufgaben nach dem Gesetz über den Kirchlichen Datenschutz (KDG) intensiver und zugleich in größerer Breite wahrzunehmen. Insbesondere konnten die Beratungs- und Informationsangebote ausgebaut sowie die Präsenz der Datenschutzaufsicht gegenüber den kirchlichen Einrichtungen weiter gestärkt werden.

Gleichzeitig zeigte sich jedoch deutlich, dass die stetig wachsenden Anforderungen des Datenschutzrechts, die fortschreitende Digitalisierung kirchlicher Arbeitsprozesse sowie die zunehmende Zahl komplexer datenschutzrechtlicher Fragestellungen mit dem bestehenden Personalbestand nur eingeschränkt und vielfach nicht innerhalb des angestrebten beziehungsweise gesetzlich vorgesehenen Zeitrahmens bewältigt werden können. Insbesondere die Begleitung technischer Entwicklungen, die Durchführung von Prüfungen, die Bearbeitung von Beschwerden sowie die steigende Nachfrage nach Beratung und Schulung führen bereits heute zu einer hohen Arbeitsbelastung.

> Eine unabhängige Datenschutzaufsicht benötigt ausreichende personelle Ressourcen, um ihre gesetzlichen Aufgaben wirksam, zeitnah und dauerhaft erfüllen zu können.

Mit Blick auf die weitere Entwicklung wird daher zu beobachten sein, ob die derzeitigen personellen Ressourcen den dauerhaft wachsenden gesetzlichen Anforderungen auch künftig in vollem Umfang gerecht werden können. Die Sicherstellung einer zeitnahen Bearbeitung von Anfragen und Beschwerden sowie die kontinuierliche Wahrnehmung aller gesetzlichen Aufgaben werden maßgeblich davon abhängen, dass die personelle Ausstattung mit der Entwicklung des Aufgabenbestandes Schritt halten kann.

1.1.2 Digitale Souveränität und Open-Source-Strategie

Von besonderer Bedeutung war im Berichtsjahr die strategische Weiterentwicklung der digitalen Souveränität der Behörde. Der bereits in den Vorjahren eingeschlagene Weg hin zu einer konsequenten Nutzung von Open-Source-Software und unabhängigen IT-Strukturen wurde konsequent fortgesetzt und in wesentlichen Bereichen weiter ausgebaut.

Im Zuge dieser Weiterentwicklung erfolgte zunehmend eine Umstellung von europäischen Anbietern auf Anbieter mit Sitz in Deutschland. Ziel war es, neben der Einhaltung der europäischen Datenschutzstandards auch die rechtliche und technische Kontrolle über besonders sensible Kommunikations-, Verwaltungs- und Fachverfahren weiter zu stärken. Das KDSZ Bayern nimmt damit weiterhin eine Vorreiterrolle unter den kirchlichen Datenschutzaufsichten ein.

> Digitale Souveränität bedeutet, selbst über Daten, Infrastruktur und eingesetzte Software entscheiden zu können. Sie ist Voraussetzung für langfristige Unabhängigkeit, Transparenz und Datenschutz.

Die Erfahrungen des Berichtsjahres haben erneut bestätigt, dass digitale Souveränität weit mehr ist als eine technische oder wirtschaftliche Fragestellung. Sie ist eine wesentliche Voraussetzung für vertrauenswürdige, resiliente und langfristig unabhängige Verwaltungsstrukturen. Gerade vor dem Hintergrund zunehmender geopolitischer Unsicherheiten, wachsender Cyberbedrohungen und einer fortschreitenden Konzentration des Marktes für digitale Dienste gewinnen offene, transparente und selbstbestimmte IT-Strukturen weiter an Bedeutung.

Die im Berichtsjahr gewonnenen Erfahrungen wurden darüber hinaus zum Anlass genommen, die Digitalisierungs- und Open-Source-Strategie des KDSZ Bayern grundlegend zu überarbeiten und in einem umfassenden strategischen Konzept zu verschriftlichen. Die hieraus entstandenen Grundsatzdokumente bildeten zugleich die Grundlage für die Bewerbung des KDSZ Bayern beim Open-Source-Wettbewerb. Aufgrund ihres Umfangs und ihrer weiteren Umsetzung werden diese

Dokumente sowie die daraus entwickelte Gesamtstrategie im Tätigkeitsbericht für das Jahr 2026 ausführlich vorgestellt.

1.1.3 Prüfung einer Anbindung an das Diözesennetz

Die Prüfung einer möglichen Anbindung des KDSZ Bayern an die Infrastruktur des „Diözesennetzes" wurde im Jahr 2025 durch eines der bayerischen Bistümer angestoßen. Das Diözesennetz verbindet derzeit elf Diözesen sowie sechs Caritasverbände deutschlandweit und schafft damit einen gemeinsamen digitalen Raum für rund 40.000 Nutzende an etwa 5.000 Standorten. Über die gemeinsame Netzwerkinfrastruktur werden zentrale Dienste für Kommunikation und Datenaustausch bereitgestellt, die eine sichere, leistungsfähige und verlässliche Vernetzung kirchlicher Einrichtungen ermöglichen.

Ein solcher Netzverbund bietet kirchlichen Einrichtungen grundsätzlich erhebliche Vorteile. Durch zentrale Sicherheits- und Kommunikationsdienste können einheitliche technische Standards etabliert, Schutzmaßnahmen gebündelt und die Resilienz gegenüber Cyberangriffen gestärkt werden. Gemeinsame Perimetersicherungen, geschützte interne Kommunikationswege sowie standardisierte Sicherheits- und Administrationsprozesse tragen dazu bei, Risiken frühzeitig zu erkennen und Sicherheitsvorfälle effizient zu bewältigen. Zugleich ermöglicht eine gemeinsame Netzwerkarchitektur einen sicheren und leistungsfähigen Datenaustausch zwischen den beteiligten Einrichtungen und erleichtert die Zusammenarbeit über Diözesan- und Organisationsgrenzen hinweg. Vor dem Hintergrund zunehmender technischer Komplexität sowie stetig wachsender Anforderungen an Informationssicherheit und Datenschutz gewinnen derartige kooperative Infrastrukturmodelle auch im kirchlichen Bereich zunehmend an Bedeutung.

Vor diesem Hintergrund wurde im Berichtsjahr geprüft, ob und unter welchen Voraussetzungen sich das KDSZ Bayern an dieser Netzwerkstruktur beteiligen kann. Gegenstand der Überlegungen war insbesondere eine Umstellung des bisherigen Internetanschlusses auf eine MPLS-basierte Anbindung. Ein wesentlicher Vorteil einer solchen Integration könnte in einer besonders geschützten Kommunikations-

infrastruktur innerhalb des Diözesennetzes liegen. Hierzu zählen insbesondere ein abgesicherter E-Mail-Verkehr zwischen den angeschlossenen Einrichtungen, die Nutzung gemeinsamer Sicherheits- und Perimeterstrukturen für den Internetzugang sowie die Einbindung in eine hochverfügbare und professionell betriebene Netzwerkinfrastruktur.

Eine Beteiligung am Diözesennetz würde zugleich erhebliche Veränderungen des technischen Betriebs der IT-Infrastruktur des KDSZ Bayern erfordern. Die derzeit auf eigenständig angemieteten Servern oder als Software-as-a-Service (SaaS) betriebenen Fachverfahren und Dienste – insbesondere E-Mail, Groupware sowie weitere zentrale Anwendungen – müssten schrittweise in die Infrastruktur des Diözesennetzes überführt werden. Damit ginge zwangsläufig auch eine Verlagerung des technischen Serverbetriebs auf einen der beteiligten diözesanen IT-Dienstleister einher. Eine solche Migration stellt nicht nur aufgrund ihrer technischen Komplexität, sondern auch wegen der hohen Anforderungen an Verfügbarkeit, Informationssicherheit, Datenschutz und Betriebskontinuität eine anspruchsvolle Aufgabe dar. Darüber hinaus wären umfangreiche organisatorische und vertragliche Anpassungen erforderlich, um den dauerhaften und sicheren Betrieb der Fachverfahren sicherzustellen.

Mit einer möglichen Anbindung sind zugleich datenschutzrechtliche und organisationsrechtliche Fragestellungen verbunden, die für eine unabhängige Datenschutzaufsichtsbehörde von besonderer Bedeutung sind. Wird die technische Infrastruktur von einer derjenigen Diözesen betrieben, die gleichzeitig der Datenschutzaufsicht des KDSZ Bayern unterliegt, ergeben sich erhöhte Anforderungen an die organisatorische Trennung von Betrieb und Aufsicht sowie an die transparente Zuordnung von Verantwortlichkeiten. Dies gilt insbesondere für Prüfungen und Audits der jeweiligen IT-Infrastruktur. Das KDSZ Bayern hätte dabei zu berücksichtigen, dass die im Rahmen der Aufsicht zu prüfenden Systeme zugleich die Grundlage der eigenen täglichen Aufgabenerfüllung bilden. Die Wahrung der gesetzlichen Unabhängigkeit der Datenschutzaufsicht und die Vermeidung möglicher

Interessenkonflikte waren daher maßgebliche Kriterien der im Berichtsjahr durchgeführten Bewertung.

> Technische Zusammenarbeit und datenschutzrechtliche Unabhängigkeit müssen auch künftig miteinander vereinbar bleiben.

Zum Ende des Berichtsjahres war die Prüfung noch nicht abgeschlossen. Eine abschließende Entscheidung über eine Beteiligung am Diözesennetz lag daher noch nicht vor.

1.1.4 Öffentlichkeitsarbeit und digitale Kommunikation

Auch die Öffentlichkeitsarbeit des KDSZ Bayern wurde im Berichtsjahr 2025 konsequent weiterentwickelt. Ziel war es, den gesetzlichen Auftrag zur Information, Beratung und Sensibilisierung kirchlicher Stellen sowie der Öffentlichkeit weiter auszubauen und datenschutzrechtliche Fragestellungen verständlich und praxisnah zu vermitteln. Dabei gewannen insbesondere Themen der digitalen Souveränität, des Einsatzes datenschutzfreundlicher Technologien sowie der verantwortungsvollen digitalen Kommunikation zunehmend an Bedeutung.

Ein besonderes Augenmerk lag im Berichtsjahr auf den umfangreichen Vorbereitungen für den gemeinsamen Auftritt der katholischen Datenschutzaufsichten beim 104. Deutschen Katholikentag in Würzburg. Die Planung und Konzeption des gemeinsamen Messestandes erfolgte in enger Zusammenarbeit zwischen dem KDSZ Bayern, dem Katholischen Datenschutzzentrum Frankfurt/Main und der Katholischen Datenschutzaufsicht Nord. Gemeinsam wurden Informations- und Sensibilisierungskonzepte entwickelt sowie Materialien und Veranstaltungsformate vorbereitet, die Besucherinnen und Besuchern einen niedrigschwelligen Zugang zu den Themen Datenschutz, digitale Selbstbestimmung und sichere digitale Kommunikation ermöglichen sollten.

> Öffentlichkeitsarbeit ist Teil des gesetzlichen Auftrags der Datenschutzaufsicht. Information, Beratung und Sensibilisierung stärken den Datenschutz bereits vor dem Entstehen konkreter Datenschutzverstöße.

Gemeinsamer Auftritt der katholischen Datenschutzaufsichten beim Katholikentag

Begleitend hierzu wurde auf der eigenen Mastodon-Instanz des KDSZ Bayern eine Informationskampagne gestartet, die insbesondere die Themen digitale Souveränität, Open-Source-Software und datenschutzfreundliche Kommunikationsplattformen in den Mittelpunkt stellte. Ziel war es, die Öffentlichkeit frühzeitig für alternative, datenschutzfreundliche Formen digitaler Kommunikation zu sensibilisieren und zugleich praktische Einblicke in die Möglichkeiten dezentraler Netzwerke zu vermitteln.

Informationskampagne des KDSZ Bayern auf Mastodon

Darüber hinaus wurde gemeinsam mit dem Organisationsteam des Deutschen Katholikentags eine Kooperation zur Stärkung nicht-kommerzieller digitaler Kommunikationsräume initiiert. Ziel dieser Zusammenarbeit war es, das Fediverse und insbesondere Mastodon als datenschutzfreundliche Alternative zu kommerziellen

sozialen Netzwerken sichtbarer zu machen und interessierten Nutzerinnen und Nutzern den Einstieg in dezentrale Kommunikationsplattformen zu erleichtern. Bereits im Vorfeld des Katholikentags wurden hierzu gemeinsame Informationen veröffentlicht sowie erste Unterstützungsangebote für die Nutzung des Fediverse entwickelt. Die Kooperation verstand sich zugleich als sichtbares Zeichen für digitale Verantwortung und für die Förderung offener und datenschutzfreundlicher Kommunikationsstrukturen innerhalb der Kirche.

Die Erfahrungen des Berichtsjahres haben gezeigt, dass Fragen der digitalen Souveränität, der informationellen Selbstbestimmung und einer verantwortungsvollen digitalen Kommunikation zunehmend Gegenstand kirchlicher und gesellschaftlicher Diskussionen sind. Die im Jahr 2025 entwickelten Konzepte und vorbereitenden Maßnahmen bildeten zugleich die Grundlage für den gemeinsamen Auftritt der katholischen Datenschutzaufsichten beim 104. Deutschen Katholikentag im Jahr 2026.

1.1.5 Beteiligung an der KI-Konsultation der BfDI

Das KDSZ Bayern beteiligte sich im Berichtsjahr unter Federführung des Katholischen Büros Berlin an der öffentlichen Konsultation der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zum datenschutzkonformen Umgang mit personenbezogenen Daten in KI-Modellen. Die Stellungnahme wurde gemeinsam mit dem KDSZ Bayern sowie der betrieblichen Datenschutzbeauftragten des Bistums Würzburg erarbeitet, die ihre praktische Fachkompetenz und langjährige Erfahrung im kirchlichen Datenschutz in die Beantwortung der Konsultationsfragen einbrachte. Ziel des Konsultationsverfahrens war es, praktische Erfahrungen, technische Erkenntnisse und rechtliche Bewertungen aus Wissenschaft, Wirtschaft und Datenschutzaufsicht zusammenzuführen, um datenschutzrechtliche Maßstäbe für den Einsatz Künstlicher Intelligenz weiterzuentwickeln.

Im Rahmen der gemeinsamen Stellungnahme brachte das KDSZ Bayern insbesondere die Erfahrungen und Anforderungen kirchlicher Einrichtungen in die Diskussion ein. Hervorgehoben wurde, dass Datenschutz und Informationssicherheit bereits

bei der Planung und dem Einsatz von KI-Systemen berücksichtigt werden müssen. Dabei wurde zugleich darauf hingewiesen, dass kirchliche Einrichtungen regelmäßig keine eigenen Sprachmodelle entwickeln, sondern überwiegend auf bestehende KI-Dienste zurückgreifen. Datenschutzrechtliche Anforderungen müssen daher vor allem an den Stellen umgesetzt werden, an denen die Einrichtungen tatsächlich Einfluss auf den Einsatz der Systeme nehmen können, etwa durch eine datenschutzgerechte Konfiguration, geeignete organisatorische Rahmenbedingungen und einen verantwortungsvollen Umgang mit eingegebenen Daten.

> Datenschutzaufsicht bedeutet heute auch, neue Technologien frühzeitig rechtlich und praktisch mitzugestalten.

Gerade im kirchlichen Bereich stellt der Einsatz Künstlicher Intelligenz besondere Anforderungen an Datenschutz, Vertraulichkeit und ethische Verantwortung. Kirchliche Einrichtungen verarbeiten in erheblichem Umfang personenbezogene Daten, die häufig einen besonderen Schutz genießen und ein hohes Maß an Vertrauen voraussetzen. Die Entwicklung und Nutzung KI-gestützter Systeme darf sich daher nicht allein an technischen Möglichkeiten oder wirtschaftlicher Effizienz orientieren, sondern muss stets die Grundrechte, die Menschenwürde sowie die berechtigten Interessen der betroffenen Personen in den Mittelpunkt stellen. Ebenso bedarf der Einsatz von KI einer angemessenen Sensibilisierung der Mitarbeitenden, klarer Verantwortlichkeiten und einer kontinuierlichen menschlichen Kontrolle.

Die Beteiligung an der Konsultation unterstreicht zugleich den Anspruch des KDSZ Bayern, die datenschutzrechtliche und rechtspolitische Entwicklung neuer Technologien aktiv zu begleiten und die praktische Erfahrung der kirchlichen Datenschutzaufsicht in bundesweite Diskussions- und Gesetzgebungsprozesse einzubringen.

1.1.6 Perspektiven

Die vielfältigen Aktivitäten des Berichtsjahres 2025 verdeutlichen, dass Datenschutzaufsicht heute weit über klassische Kontroll- und Prüftätigkeiten hinausgeht. Beratung, Schulung, technische Expertise, Öffentlichkeitsarbeit sowie die Begleitung digitaler Transformationsprozesse und die Förderung digitaler Souveränität sind zu wesentlichen Bestandteilen einer modernen und zukunftsorientierten Datenschutzaufsicht geworden. Zugleich gewinnt die Fähigkeit, neue technologische Entwicklungen frühzeitig zu bewerten und datenschutzgerecht zu begleiten, zunehmend an Bedeutung.

Das KDSZ Bayern wird diesen Weg auch in den kommenden Jahren konsequent fortsetzen. Ziel bleibt es, die kirchlichen Einrichtungen als unabhängige Datenschutzaufsicht kompetent zu begleiten, den Schutz der Persönlichkeitsrechte nachhaltig zu stärken und zugleich einen Beitrag zu einer sicheren, verantwortungsvollen und vertrauenswürdigen Digitalisierung innerhalb der Kirche zu leisten.

1.2 Verwaltungsrat

Der Verwaltungsrat begleitet die organisatorische und wirtschaftliche Entwicklung des KDSZ Bayern. Er gewährleistet die institutionellen Rahmenbedingungen für eine leistungsfähige und unabhängige Datenschutzaufsicht.

Im Dezember 2025 trat der Verwaltungsrat des KDSZ Bayern zusammen. Das Gremium setzt sich gemäß der Satzung aus Vertreterinnen und Vertretern der sieben bayerischen (Erz-)Diözesen zusammen. Es ist für die organisatorischen, personellen sowie haushaltsrechtlichen Angelegenheiten des KDSZ Bayern zuständig. Die Wahrnehmung der gesetzlichen Aufgaben der Datenschutzaufsicht erfolgt hiervon unabhängig und weisungsfrei.

Im Mittelpunkt der Beratungen standen die weitere Ausgestaltung der Arbeitsweise des Verwaltungsrates sowie die organisatorische Weiterentwicklung der Behörde. Hierzu gehörten insbesondere der Erlass einer Geschäftsordnung, die Einrichtung einer Geschäftsführung, die Einführung einer gemeinsamen digitalen Austauschplattform sowie Fragen der zukünftigen Personal- und Haushaltsplanung. Darüber hinaus informierte die Behördenleitung über die aktuelle personelle, organisatorische und finanzielle Entwicklung des KDSZ Bayern sowie über den Stand laufender Digitalisierungs- und Organisationsprojekte.

> Der Verwaltungsrat gewährleistet die organisatorischen und finanziellen Voraussetzungen für eine leistungsfähige Datenschutzaufsicht. Die fachliche Aufsichtstätigkeit bleibt hiervon gesetzlich unabhängig.

Ein Hauptanliegen der Sitzung war die langfristige Sicherung einer leistungsfähigen und unabhängigen Datenschutzaufsicht. Vor dem Hintergrund stetig wachsender rechtlicher und technischer Anforderungen befasste sich der Verwaltungsrat insbesondere mit den zukünftigen Herausforderungen im Bereich des Datenschutzrechts, der Informationssicherheit und der Informationstechnik.

Dabei wurden sowohl die Weiterentwicklung der organisatorischen Strukturen als auch der mittel- und langfristige Bedarf an fachlichen und technischen Ressourcen erörtert. Einigkeit bestand darüber, dass eine wirksame Datenschutzaufsicht dauerhaft auf ausreichend qualifiziertes Personal, moderne technische Infrastrukturen und eine organisatorisch unabhängige Behördenstruktur angewiesen ist.

Im Rahmen der Sitzung regte der Verwaltungsrat ferner an, die Transparenz der Tätigkeit des KDSZ Bayern weiter auszubauen. Künftig werden im Tätigkeitsbericht regelmäßig auch statistische Angaben, insbesondere zu Datenschutzverletzungen, Beschwerden und Beratungen, veröffentlicht werden. Dadurch soll die Entwicklung der Aufsichtstätigkeit nachvollziehbar dokumentiert und der Öffentlichkeit ein noch umfassenderer Einblick in die Arbeit der Behörde ermöglicht werden.

1.3 Finanzen

Die finanzielle Unabhängigkeit bildet eine wesentliche Voraussetzung für die unabhängige Wahrnehmung der gesetzlichen Aufgaben des KDSZ Bayern. Der Gesetzgeber trägt diesem Grundsatz durch einen eigenständigen Haushalt und eine gesicherte Finanzierung Rechnung.

Die finanzielle Ausstattung des KDSZ Bayern richtet sich nach § 42 Abs. 5 des Gesetzes über den Kirchlichen Datenschutz (KDG). Danach sind dem Diözesandatenschutzbeauftragten die Personal- und Sachmittel zur Verfügung zu stellen, die für die unabhängige Wahrnehmung seiner gesetzlichen Aufgaben und Befugnisse erforderlich sind. Zur Sicherung dieser Unabhängigkeit verfügt das KDSZ Bayern über einen eigenen Haushalt, der gesondert auszuweisen und zu veröffentlichen ist. Die gesetzlich vorgesehene Rechnungsprüfung erfolgt durch eine von den Diözesen bestimmte unabhängige Stelle, soweit hierdurch die Unabhängigkeit der Datenschutzaufsicht nicht beeinträchtigt wird.

Die Finanzierung des KDSZ Bayern erfolgt über den Überdiözesanen Fonds Bayern (ÜDF). An diesem beteiligen sich die sieben bayerischen (Erz-)Diözesen nach einem vereinbarten Verteilungsschlüssel. Durch diese gemeinsame Finanzierung wird gewährleistet, dass die Datenschutzaufsicht ihre gesetzlichen Aufgaben unabhängig von den einzelnen Diözesen wahrnehmen kann und zugleich über eine verlässliche finanzielle Grundlage verfügt.

> Finanzielle Unabhängigkeit ist keine organisatorische Besonderheit, sondern eine gesetzliche Voraussetzung wirksamer Datenschutzaufsicht.

Grundlage der Finanzierung ist ein jährlich im Voraus aufgestellter Haushaltsplan, der nach Prüfung durch den Überdiözesanen Fonds Bayern beschlossen wird. Die Finanzierung erfolgt in Form von Personal- und Sachkostenzuschüssen. Über die Verwendung der Haushaltsmittel legt das KDSZ Bayern im Rahmen seines Jahresabschlusses Rechenschaft ab.

Als Körperschaft des öffentlichen Rechts ist das KDSZ Bayern verpflichtet, einen Jahresabschluss mit Bilanz zu erstellen. Dieser wird entsprechend den Förderrichtlinien des Überdiözesanen Fonds Bayern jährlich durch ein unabhängiges Wirtschaftsprüfungsunternehmen geprüft. Hierdurch werden eine ordnungsgemäße Haushaltsführung sowie ein hohes Maß an Transparenz, Wirtschaftlichkeit und Nachvollziehbarkeit bei der Verwendung der bereitgestellten Mittel sichergestellt.

Der überwiegende Teil der Haushaltsmittel entfällt auf Personalkosten. Dies entspricht der Aufgabenstruktur einer Datenschutzaufsichtsbehörde, deren Tätigkeit maßgeblich durch hochqualifizierte juristische, technische und organisatorische Facharbeit geprägt ist. Investitionen in Sachmittel dienen insbesondere der Bereitstellung einer sicheren, leistungsfähigen und unabhängigen IT-Infrastruktur sowie der kontinuierlichen Weiterentwicklung der digitalen Arbeitsabläufe.

Auch im Berichtsjahr wurde bei Investitionsentscheidungen darauf geachtet, wirtschaftliche Gesichtspunkte mit den Zielen der digitalen Souveränität, Nachhaltigkeit und langfristigen Unabhängigkeit der IT-Infrastruktur in Einklang zu bringen. Der verstärkte Einsatz von Open-Source-Software sowie die konsequente Weiterentwicklung eigener digitaler Fachverfahren leisten hierzu einen wichtigen Beitrag und ermöglichen zugleich einen wirtschaftlichen und ressourcenschonenden Einsatz der verfügbaren Haushaltsmittel.

> Personalkostenzuschüsse
> **436.564,46 €**
>
> Sachkostenzuschüsse
> **53.000,00 €**
>
> Gesamt
> **489.564,46 €**

1.4 Veröffentlichung von Fallzahlen

Transparenz ist eine wesentliche Voraussetzung für das Vertrauen in die Tätigkeit einer unabhängigen Datenschutzaufsicht. Mit der Veröffentlichung ausgewählter Fallzahlen macht das KDSZ Bayern die Entwicklung seiner Aufsichtstätigkeit künftig besser nachvollziehbar.

Im Rahmen der Beratungen des Verwaltungsrates wurde der Wunsch geäußert, die Transparenz der Tätigkeit des KDSZ Bayern weiter auszubauen und künftig auch statistische Angaben zur Arbeit der Behörde zu veröffentlichen. Diesem Anliegen wird ab dem Tätigkeitsbericht für das Berichtsjahr 2026 entsprochen. Vorgesehen ist insbesondere die Darstellung von Beschwerden, Meldungen von Datenschutzverletzungen, Beratungsanfragen sowie weiterer aufsichtlicher Verfahren in absoluten Zahlen und später dann auch in relativen Zahlen im Vergleich zu den Vorjahren.

Die Fallzahlen dienen nicht dem Vergleich von Behörden, sondern der nachvollziehbaren Darstellung der Entwicklung der Aufsichtstätigkeit und ihrer fachlichen Schwerpunkte.

Mit der Veröffentlichung dieser Angaben soll der Öffentlichkeit ein besseres Verständnis für die Aufgaben, die Arbeitsweise und die Entwicklung der kirchlichen Datenschutzaufsicht vermittelt werden. Vergleichbare statistische Übersichten gehören seit vielen Jahren zu den Tätigkeitsberichten der staatlichen Datenschutzaufsichtsbehörden und haben sich dort als wichtiger Beitrag zu Transparenz und Nachvollziehbarkeit etabliert.

> Fallzahlen allein erlauben keine Bewertung der Qualität einer Datenschutzaufsicht. Sie schaffen jedoch Transparenz über Aufgaben, Entwicklungen und Schwerpunkte der behördlichen Tätigkeit.

Gleichzeitig wurde im Rahmen der Beratungen hervorgehoben, dass statistische Fallzahlen nur eine begrenzte Aussagekraft besitzen. Umfang, Komplexität und

Dauer einzelner Verfahren unterscheiden sich teilweise erheblich. So können wenige technisch oder rechtlich besonders anspruchsvolle Verfahren erhebliche personelle Ressourcen binden, während eine größere Zahl einfacher Beratungsanfragen oder Standardverfahren vergleichsweise schnell bearbeitet werden kann. Ebenso lassen steigende Beschwerdezahlen oder Erhöhungen bei den Datenpannenmeldungen nicht ohne Weiteres den Schluss auf eine Zunahme datenschutzrechtlicher Verstöße zu. Sie können vielmehr auch Ausdruck einer gestiegenen Sensibilisierung für Datenschutzrechte sowie eines wachsenden Vertrauens in die Arbeit der Datenschutzaufsicht sein.

Die künftige Veröffentlichung statistischer Angaben soll daher nicht allein die Entwicklung einzelner Fallzahlen dokumentieren, sondern zugleich zu einer sachgerechten Einordnung der Aufgaben, Herausforderungen und Prioritäten einer modernen Datenschutzaufsicht beitragen. Ziel ist es, die Tätigkeit des KDSZ Bayern für die kirchlichen Einrichtungen, die Öffentlichkeit und die beteiligten Gremien noch transparenter und nachvollziehbarer darzustellen.

2 Entwicklungen des Datenschutz- und Digitalrechts

Das Datenschutzrecht entwickelt sich heute nicht mehr isoliert, sondern als Bestandteil eines umfassenden europäischen Digitalrechts. Neue europäische Verordnungen, die Reform des kirchlichen Datenschutzrechts sowie eine dynamische Rechtsprechung haben den rechtlichen Rahmen im Berichtsjahr 2025 nachhaltig verändert. Dieses Kapitel gibt einen Überblick über die wesentlichen Entwicklungen und ihre Bedeutung für die kirchliche Datenschutzpraxis.

Das Datenschutzrecht war auch im Berichtsjahr 2025 von einer hohen Dynamik geprägt. Während die Datenschutz-Grundverordnung (DSGVO) selbst im Wesentlichen unverändert blieb, entwickelten sich die rechtlichen Rahmenbedingungen auf europäischer, staatlicher und kirchlicher Ebene kontinuierlich weiter. Neue gesetzliche Regelungen, die fortschreitende Digitalisierung sowie zahlreiche gerichtliche Entscheidungen konkretisierten die datenschutzrechtlichen Anforderungen weiter und stellten Verantwortliche ebenso wie Datenschutzaufsichtsbehörden vor neue Herausforderungen.

Auf europäischer Ebene prägten insbesondere die ersten Anwendungsphasen der Verordnung über Künstliche Intelligenz (AI-Act), der Data Act sowie die zunehmende Verzahnung von Datenschutz und Informationssicherheit die rechtspolitische Diskussion. Gleichzeitig konkretisierte die Rechtsprechung des Europäischen Gerichtshofs und der deutschen Gerichte zahlreiche Fragen der Datenschutz-Grundverordnung, insbesondere zu den Betroffenenrechten, zum Schadensersatz sowie zur Verantwortlichkeit bei der Verarbeitung personenbezogener Daten.

Auch das kirchliche Datenschutzrecht wurde im Berichtsjahr umfassend fortentwickelt. Mit der Novellierung des Gesetzes über den Kirchlichen Datenschutz (KDG) und der Neufassung der Durchführungsverordnung zum KDG (KDG-DVO) wurden wesentliche Rechtsgrundlagen an die aktuellen technischen und organisatorischen Entwicklungen angepasst. Darüber hinaus trugen die Entscheidungen der

kirchlichen Datenschutzgerichte zu einer weiteren Konkretisierung und Fortentwicklung des kirchlichen Datenschutzrechts bei.

Schließlich war das Berichtsjahr auch von einem intensiven fachlichen Austausch über den datenschutzgerechten Einsatz neuer Technologien geprägt. Insbesondere die zunehmende Verbreitung Künstlicher Intelligenz verdeutlichte, dass datenschutzrechtliche Fragestellungen zunehmend bereits im Zusammenhang mit der Entwicklung und Einführung neuer Technologien berücksichtigt werden müssen. Datenschutzaufsicht beschränkt sich deshalb nicht mehr auf die Anwendung bestehenden Rechts, sondern begleitet dessen Fortentwicklung in Wissenschaft, Gesetzgebung und Praxis.

Die nachfolgenden Abschnitte geben einen Überblick über die aus Sicht des KDSZ Bayern wesentlichen Entwicklungen des Datenschutz- und Digitalrechts im Berichtsjahr 2025 sowie deren Bedeutung für die kirchliche Datenschutzpraxis.

2.1 Europäische und nationale Gesetzgebung

Das europäische Datenschutzrecht wird zunehmend durch weitere Rechtsakte ergänzt, die den digitalen Binnenmarkt, den Einsatz neuer Technologien sowie die Informationssicherheit betreffen. Datenschutzrechtliche Fragestellungen lassen sich daher immer seltener isoliert betrachten, sondern stehen in engem Zusammenhang mit weiteren Bereichen des europäischen Digitalrechts.

Auch wenn diese Rechtsakte nicht ausschließlich datenschutzrechtliche Regelungen enthalten, wirken sie sich unmittelbar auf die Verarbeitung personenbezogener Daten und die Organisation kirchlicher Einrichtungen aus. Die nachfolgenden Abschnitte geben einen Überblick über die wichtigsten gesetzlichen Entwicklungen des Berichtsjahres und ihre Bedeutung für die kirchliche Datenschutzpraxis.

2.1.1 Digitaler Omnibus

Die Europäische Kommission hat im November 2025 als Bestandteil eines umfassenden Pakets zur Weiterentwicklung des europäischen Digitalrechts ein Gesetz-

gebungsvorhaben vorgestellt, das unter der Bezeichnung ‚Digitaler Omnibus" bekannt geworden ist. Ziel des Vorhabens ist es, bestehende Regelungen des europäischen Digitalrechts besser aufeinander abzustimmen, Überschneidungen zu vermeiden und unnötige bürokratische Belastungen abzubauen.

Der Begriff ‚Omnibus" ist kein offizieller Rechtsbegriff, sondern bezeichnet im europäischen Gesetzgebungsverfahren Vorhaben, mit denen mehrere unterschiedliche Rechtsakte innerhalb eines gemeinsamen Gesetzgebungsverfahrens geändert oder aufeinander abgestimmt werden.

Das Bild ist anschaulich gewählt: Ähnlich wie ein Omnibus zahlreiche Fahrgäste gleichzeitig befördert, werden verschiedene Regelungsbereiche gemeinsam weiterentwickelt. Ziel solcher Omnibus-Verfahren ist es insbesondere, Widersprüche zwischen einzelnen Rechtsakten zu vermeiden, Begriffe und Verfahren zu harmonisieren, Melde- und Dokumentationspflichten besser aufeinander abzustimmen sowie die praktische Anwendung des Rechts insgesamt zu vereinfachen.

Digitaler Omnibus - KDSZ Bayern

Das Vorhaben betrifft zahlreiche europäische Rechtsakte des Digitalrechts. Hierzu zählen insbesondere die DSGVO, der Data Act, der AI Act sowie weitere Regelungen zur Informationssicherheit und zum digitalen Binnenmarkt. Ziel ist eine bessere

Verzahnung dieser Rechtsakte sowie eine kohärentere Ausgestaltung ihrer Anforderungen.

Nach den bislang veröffentlichten Überlegungen sollen auch einzelne Regelungen der DSGVO überprüft werden. In welche Richtung sich mögliche Änderungen tatsächlich entwickeln werden, lässt sich derzeit jedoch noch nicht verlässlich beurteilen.

Diskutiert werden unter anderem eine Konkretisierung des Begriffs der personenbezogenen Daten mit dem Ziel einer klareren Abgrenzung des Anwendungsbereichs der DSGVO, Vereinfachungen bei Informations- und Auskunftspflichten sowie eine stärkere Harmonisierung von Meldeverfahren, etwa durch ein gemeinsames Meldeportal für Datenschutzverletzungen. Darüber hinaus werden Anpassungen der Cookie-Regelungen, eine Überprüfung der Pflicht zur Benennung von Datenschutzbeauftragten sowie eine noch stärker risikoorientierte Ausgestaltung einzelner Pflichten für Verantwortliche erörtert.

Das Vorhaben befindet sich noch in einem frühen Stadium des europäischen Gesetzgebungsverfahrens. Konkrete Formulierungsvorschläge oder belastbare Zeitpläne liegen im Berichtszeitraum nicht vor. Umfang und Inhalt möglicher Änderungen werden sich erst im weiteren Verlauf der Beratungen der europäischen Gesetzgebungsorgane sowie der Stellungnahmen der beteiligten Institutionen und Fachkreise konkretisieren. Eine abschließende Bewertung ist daher im Berichtszeitraum noch nicht möglich.

> Der Digitale Omnibus befindet sich noch im Gesetzgebungsverfahren. Für kirchliche Einrichtungen ergeben sich derzeit keine unmittelbaren Änderungen.

2.1.2 Verordnung über Transparenz und Targeting politischer Werbung

Die Verordnung (EU) 2024/900 über Transparenz und Targeting politischer Werbung (TTPW-VO) schafft erstmals einen einheitlichen europäischen Rechtsrahmen

für politische Werbung. Ziel der Verordnung ist es, Transparenz über politische Werbemaßnahmen herzustellen und die Integrität demokratischer Prozesse innerhalb der Europäischen Union zu stärken. Als Verordnung gilt sie unmittelbar in allen Mitgliedstaaten und ergänzt insbesondere die bestehenden datenschutzrechtlichen Regelungen der Datenschutz-Grundverordnung (DSGVO).

Ein wesentlicher Regelungsgegenstand ist das sogenannte politische Mikrotargeting. Hierunter versteht man die gezielte Ansprache einzelner Personen oder eng abgegrenzter Personengruppen mit individuell zugeschnittenen politischen Botschaften. Grundlage hierfür sind regelmäßig personenbezogene Daten, die beispielsweise aus sozialen Netzwerken oder anderen digitalen Diensten gewonnen werden. Ziel ist es, politische Einstellungen oder Wahlentscheidungen möglichst zielgerichtet zu beeinflussen. Für die betroffenen Personen bleibt dabei häufig nicht erkennbar, dass sie aufgrund eines individuellen Profils ausgewählt wurden.

Das politische Mikrotargeting gewann insbesondere im Zusammenhang mit den US-Präsidentschaftswahlen ab 2008 zunehmend an Bedeutung. Internationale Aufmerksamkeit erlangte das Thema spätestens durch den im Jahr 2018 bekannt gewordenen Cambridge-Analytica-Skandal. Dabei wurde deutlich, dass personenbezogene Daten ohne wirksame Einwilligung genutzt worden waren, um detaillierte Persönlichkeitsprofile zu erstellen und hierauf aufbauend gezielte politische Einflussnahme zu betreiben. Gleichzeitig mehrten sich Hinweise darauf, dass digitale Werbekampagnen auch zur Einflussnahme auf demokratische Prozesse anderer Staaten eingesetzt werden können. Diese Entwicklungen führten europaweit zu der Erkenntnis, dass Transparenz und Datenschutz einen wichtigen Beitrag zum Schutz demokratischer Willensbildungsprozesse leisten können und müssen.

Vor diesem Hintergrund sieht die Verordnung umfangreiche Transparenz- und Dokumentationspflichten vor. Bürgerinnen und Bürger sollen künftig leichter erkennen können, dass es sich um politische Werbung handelt, von wem diese finanziert wird und welche Kriterien einer gezielten Ansprache zugrunde liegen. Gleichzeitig werden die Voraussetzungen für den Einsatz personenbezogener Daten zu Tar-

geting-Zwecken erheblich verschärft. Dadurch soll verhindert werden, dass politische Werbung auf der Grundlage sensibler personenbezogener Daten oder ohne ausreichende Transparenz erfolgt. Darüber hinaus enthält die Verordnung besondere Regelungen zum Schutz vor ausländischer Einflussnahme auf demokratische Wahlen innerhalb der Europäischen Union.

> Die TTPW-VO richtet sich in erster Linie an politische Akteure und Anbieter politischer Werbung. Für kirchliche Einrichtungen wird sie nur in besonderen Einzelfällen praktische Bedeutung erlangen.

Die Verordnung gilt seit dem 10. Oktober 2025 vollständig und entfaltet damit unmittelbare Wirkung auch in Deutschland. Einzelne Aufgaben werden nach Art. 22 TTPW-VO den staatlichen Datenschutzaufsichtsbehörden übertragen. Die kirchlichen Datenschutzaufsichtsbehörden sind von diesen Zuständigkeitsregelungen nicht unmittelbar erfasst. Gleichwohl kann die Verordnung mittelbare Auswirkungen auch auf kirchliche Einrichtungen entfalten. Dies gilt insbesondere für Fragen der kirchlichen Öffentlichkeitsarbeit und digitalen Kommunikation, soweit Inhalte einen politischen Bezug aufweisen oder die Abgrenzung zwischen gesellschaftlicher Meinungsäußerung, kirchlicher Interessenvertretung und politischer Werbung zu beurteilen ist. Auch im Rahmen der gesetzlichen Beratungsaufgaben kann sich hieraus künftig ein erhöhter Informations- und Unterstützungsbedarf ergeben.

Für die praktische Umsetzung der Verordnung sind ergänzende nationale Regelungen erforderlich. Diese betreffen insbesondere die Festlegung der zuständigen Behörden, Verfahrensregelungen sowie Sanktionsvorschriften. Ein entsprechender Gesetzentwurf wird im Jahr 2026 vorgelegt.

Die weitere Umsetzung der Verordnung wird zeigen, wie sich die neuen Transparenz- und Datenschutzanforderungen auf die politische Kommunikation in der Europäischen Union auswirken. Die praktische Bedeutung für kirchliche Einrichtungen bleibt derzeit begrenzt. Die Verordnung verdeutlicht jedoch die fortschreitende Ausdifferenzierung des europäischen Digitalrechts.

2.1.3 Data Act

Mit der Verordnung (EU) 2023/2854 (Data Act) hat die Europäische Union einen weiteren wichtigen Baustein ihres digitalen Binnenmarkts geschaffen. Die Verordnung (EU) 2023/2854 verfolgt das Ziel, den Zugang zu und die Nutzung von Daten innerhalb der Europäischen Union zu erleichtern sowie faire Wettbewerbsbedingungen in einer zunehmend datengetriebenen Wirtschaft zu schaffen. Sie ergänzt damit bestehende europäische Rechtsakte im Bereich der Digitalisierung und ist Teil der europäischen Datenstrategie.

Im Mittelpunkt des Data Act stehen insbesondere Daten, die bei der Nutzung vernetzter Produkte und digitaler Dienste entstehen. Nutzerinnen und Nutzer sollen künftig einen besseren Zugang zu diesen Daten erhalten und selbst entscheiden können, ob und mit wem sie diese teilen. Gleichzeitig werden Hersteller und Anbieter verpflichtet, den Zugang zu bestimmten Daten unter fairen, angemessenen und diskriminierungsfreien Bedingungen zu ermöglichen. Darüber hinaus enthält die Verordnung Regelungen, die den Wechsel zwischen Cloud- und Plattformdiensten erleichtern und dadurch Wettbewerb sowie Interoperabilität fördern sollen.

Der Data Act verfolgt damit in erster Linie wirtschafts- und innovationspolitische Ziele. Anders als die DSGVO schützt er nicht unmittelbar die Privatsphäre natürlicher Personen, sondern regelt den Zugang zu, die Nutzung von und den Austausch digitaler Daten. Berührungspunkte zum Datenschutz bestehen jedoch überall dort, wo die betroffenen Datensätze personenbezogene Daten enthalten oder einen Personenbezug aufweisen.

Aus diesem Grund stellt der Data Act ausdrücklich klar, dass die Datenschutz-Grundverordnung durch seine Regelungen weder eingeschränkt noch ersetzt wird. Personenbezogene Daten dürfen weiterhin ausschließlich unter den Voraussetzungen der DSGVO verarbeitet werden. Soweit Daten sowohl dem Anwendungsbereich des Data Act als auch der DSGVO unterfallen, sind die Vorgaben beider Rechtsakte nebeneinander anzuwenden. Der Data Act ergänzt das Datenschutzrecht, ohne dessen Schutzniveau zu verändern.

Obwohl der Data Act als europäische Verordnung unmittelbar in allen Mitgliedstaaten gilt, bedarf es ergänzender nationaler Regelungen für seine praktische Durchsetzung. Hierzu gehören insbesondere die Benennung der zuständigen Behörden, Verfahrensregelungen sowie Vorschriften zur Rechtsdurchsetzung und Sanktionierung. Ein entsprechender deutscher Gesetzentwurf lag im Berichtszeitraum bereits vor, war zum Jahresende jedoch noch nicht verabschiedet.

Für kirchliche Einrichtungen wird der Data Act künftig insbesondere dort an Bedeutung gewinnen, wo vernetzte technische Systeme, intelligente Gebäude- und Haustechnik, medizinische Geräte oder Cloud-Dienste eingesetzt werden und hierbei Daten erzeugt oder verarbeitet werden. Neben den datenschutzrechtlichen Anforderungen der DSGVO sind in diesen Bereichen künftig zunehmend auch die datenwirtschaftlichen Vorgaben des Data Act zu beachten. Dies gilt insbesondere für Fragen des Datenzugangs, der Datenweitergabe sowie des Wechsels zwischen verschiedenen Cloud-Anbietern.

> Der Data Act ergänzt das Datenschutzrecht – er ersetzt es nicht. Für personenbezogene Daten gelten weiterhin uneingeschränkt DSGVO und KDG.

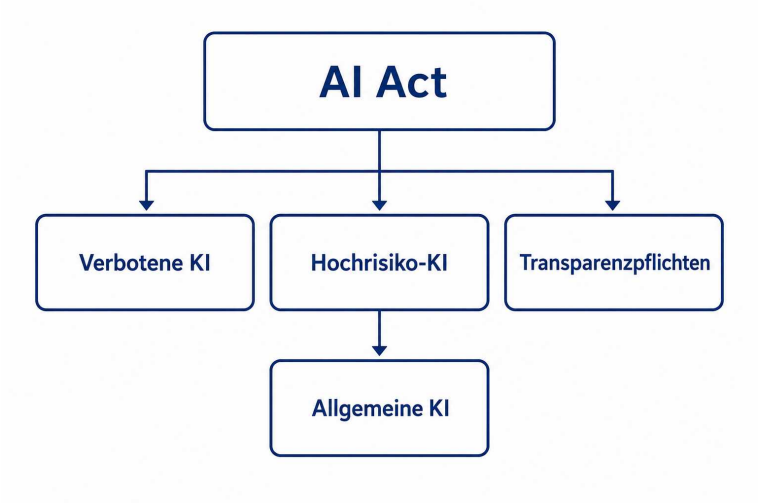
Mit dem Data Act setzt die Europäische Union ihre Strategie fort, einen einheitlichen europäischen Rechtsrahmen für die digitale Wirtschaft zu schaffen. Für Verantwortliche wird damit deutlich, dass Datenschutzrecht und Datenrecht künftig noch stärker zusammenwirken werden. Das KDSZ Bayern wird die weitere Umsetzung des Data Act sowie die sich daraus ergebenden Fragestellungen für kirchliche Einrichtungen aufmerksam begleiten und in seine Beratungs- und Aufsichtstätigkeit einbeziehen.

2.1.4 Verordnung über Künstliche Intelligenz (AI Act)

Mit der Verordnung (EU) 2024/1689 über künstliche Intelligenz (Artificial Intelligence Act – AI Act) hat die Europäische Union erstmals einen umfassenden Rechtsrahmen für die Entwicklung, das Inverkehrbringen und den Einsatz Künstlicher Intelligenz geschaffen. Die bereits im Jahr 2024 verabschiedete Verordnung verfolgt das

Ziel, Innovationen zu fördern und zugleich ein hohes Maß an Sicherheit, Transparenz und Grundrechtsschutz zu gewährleisten. Durch einheitliche europäische Regelungen soll das Vertrauen in den Einsatz von KI-Systemen gestärkt und ein verantwortungsvoller Umgang mit dieser Schlüsseltechnologie sichergestellt werden.

Der AI Act verfolgt dabei einen risikobasierten Ansatz. Je höher das von einem KI-System ausgehende Risiko eingeschätzt wird, desto umfangreicher sind die gesetzlichen Anforderungen. Besonders risikobehaftete Anwendungen unterliegen strengen Vorgaben, während bestimmte KI-Praktiken aufgrund ihres inakzeptablen Risikos vollständig verboten sind. Daneben enthält die Verordnung Transparenz- und Informationspflichten sowie besondere Anforderungen für Hochrisiko-KI-Systeme in sensiblen Bereichen, etwa im Gesundheitswesen, im Finanzsektor oder bei kritischen Infrastrukturen.



Risikobasierter Regelungsansatz des AI Act

Eine der ersten unmittelbar geltenden Verpflichtungen betrifft seit Februar 2025 die Sicherstellung einer angemessenen KI-Kompetenz. Danach müssen Anbieter und Betreiber von KI-Systemen geeignete Maßnahmen treffen, damit die mit Entwicklung, Betrieb oder Nutzung von KI-Systemen befassten Personen über ausreichende Kenntnisse und Fähigkeiten verfügen. Der AI Act schreibt hierbei keine einheitlichen Schulungen oder Zertifizierungen vor. Vielmehr richtet sich der Umfang der erforderlichen Qualifizierungsmaßnahmen nach den jeweiligen Aufgaben der Mit-

arbeitenden, dem eingesetzten KI-System, dessen Risikopotenzial sowie dem vorhandenen Vorwissen.

Für kirchliche Einrichtungen besitzt diese Verpflichtung bereits heute erhebliche praktische Bedeutung. Künstliche Intelligenz kommt inzwischen nicht mehr ausschließlich in spezialisierten Anwendungen zum Einsatz, sondern findet sich zunehmend auch in alltäglichen Arbeitsmitteln. Neben generativen KI-Systemen gehören hierzu beispielsweise intelligente Suchfunktionen, Übersetzungsprogramme, Dokumentenanalyse, Assistenzsysteme, Telefon- und Serviceplattformen oder moderne Office-Anwendungen. Viele Einrichtungen setzen damit bereits KI-Systeme ein, ohne dass dies im Arbeitsalltag stets bewusst wahrgenommen wird. Auch in diesen Fällen ist zu prüfen, welche Anforderungen der AI Act an die Qualifizierung der Mitarbeitenden stellt.

Die Umsetzung dieser Vorgaben stellt insbesondere größere kirchliche Einrichtungen und Träger vor zusätzliche organisatorische Herausforderungen. Gleichzeitig können vorhandene Strukturen für Pflichtschulungen und Fortbildungen genutzt werden. Gerade Einrichtungen im Gesundheits-, Sozial- und Bildungsbereich verfügen bereits über umfangreiche Erfahrungen mit verpflichtenden Qualifizierungsmaßnahmen. Hier bestehen zahlreiche Berührungspunkte zu den Bereichen Datenschutz, Informationssicherheit und Compliance, sodass bestehende Schulungs- und Sensibilisierungskonzepte sinnvoll weiterentwickelt werden können.

Der AI Act ersetzt dabei nicht die DSGVO, sondern ergänzt diese. Werden im Rahmen von KI-Systemen personenbezogene Daten verarbeitet, sind die datenschutzrechtlichen Vorgaben der DSGVO und des KDG uneingeschränkt zu beachten. Im Rahmen der KI-Kompetenz sollten Mitarbeitende daher auch für datenschutzrechtliche Fragestellungen sensibilisiert werden. Hierzu zählen insbesondere der datenschutzgerechte Umgang mit personenbezogenen Daten, mögliche Verzerrungen („Bias“) und Halluzinationen von KI-Systemen, Fragen der Transparenz sowie das Recht betroffener Personen, nicht ausschließlich automatisierten Ent-

scheidungen mit rechtlicher oder ähnlich erheblicher Wirkung unterworfen zu werden.

> Der AI Act ersetzt das Datenschutzrecht nicht. Beim Einsatz Künstlicher Intelligenz sind AI Act, DSGVO und KDG nebeneinander zu beachten.

Für die unmittelbare Überwachung der Vorgaben des AI Act sind nicht die Datenschutzaufsichtsbehörden zuständig. Die Marktüberwachung erfolgt nach der europäischen KI-Verordnung grundsätzlich durch speziell benannte staatliche Marktüberwachungsbehörden. In Deutschland zeichnet sich hierbei insbesondere eine koordinierende Rolle der Bundesnetzagentur ab, ergänzt durch weitere fachlich zuständige Behörden in den jeweiligen Anwendungsbereichen.

Unabhängig hiervon werden sich für Datenschutzaufsichtsbehörden künftig verstärkt Fragestellungen an der Schnittstelle zwischen Künstlicher Intelligenz und Datenschutz ergeben. Hierzu zählen insbesondere die datenschutzkonforme Verarbeitung personenbezogener Daten durch KI-Systeme, Anforderungen an Transparenz und Nachvollziehbarkeit automatisierter Verarbeitungsvorgänge sowie der Umgang mit fehlerhaften oder verzerrten KI-Ausgaben. Mit der zunehmenden Verbreitung von KI-Systemen wird diesen Fragestellungen auch im kirchlichen Bereich eine wachsende praktische Bedeutung zukommen.

Die Pflicht zur Sicherstellung von KI-Kompetenz verdeutlicht zugleich einen grundlegenden Gedanken des europäischen Digitalrechts: Digitale Souveränität entsteht nicht allein durch den Einsatz neuer Technologien. Sie setzt vielmehr voraus, dass die Menschen, die diese Technologien entwickeln, auswählen und einsetzen, deren Funktionsweise, Chancen und Risiken verstehen und verantwortungsvoll mit ihnen umgehen. Der AI Act trägt diesem Gedanken erstmals auf europäischer Ebene ausdrücklich Rechnung. Das KDSZ Bayern wird die weitere Entwicklung des KI-Rechts sowie deren Auswirkungen auf kirchliche Einrichtungen und die Datenschutzpraxis weiterhin aufmerksam begleiten.

2.1.5 Informationssicherheit als Bestandteil des europäischen Digitalrechts

Neben dem Datenschutz gewinnen europäische Regelungen zur Informationssicherheit zunehmend an Bedeutung. Mit der NIS-2-Richtlinie, der DORA-Verordnung und dem Cyber Resilience Act verfolgt die Europäische Union das Ziel, die digitale Resilienz von Einrichtungen und Unternehmen nachhaltig zu stärken. Datenschutz und Informationssicherheit werden dabei zunehmend als komplementäre Elemente einer vertrauenswürdigen Digitalisierung verstanden.

Datenschutz und Informationssicherheit verfolgen unterschiedliche Zielrichtungen, sind in der Praxis jedoch eng miteinander verbunden. Während das Datenschutzrecht die rechtlichen Anforderungen an die Verarbeitung personenbezogener Daten regelt, umfasst die Informationssicherheit die technischen und organisatorischen Maßnahmen zum Schutz sämtlicher Informationen einer Einrichtung. Ihr Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen dauerhaft sicherzustellen. Mit der fortschreitenden Digitalisierung und der zunehmenden Vernetzung steigen zugleich die Anforderungen an die Informationssicherheit. Neben dem Schutz vor Datenverlust gewinnen insbesondere die Abwehr von Cyberangriffen, Sabotage, Erpressung und unbefugten Zugriffen auf IT-Systeme an Bedeutung. Ein wirksamer Schutz personenbezogener Daten setzt deshalb regelmäßig auch ein angemessenes Informationssicherheitsniveau voraus.

Diese Entwicklung zeigt sich auch in der Aufsichtspraxis des KDSZ Bayern. Erfolgreiche Cyberangriffe auf IT-Systeme gehen heute häufig mit einer Gefährdung personenbezogener Daten einher. Im Fokus der Angreifer stehen regelmäßig Kunden-, Klienten- oder Patientendaten, aber auch Beschäftigtendaten sowie Informationen von Geschäftspartnern und anderen Beteiligten. Selbst wenn sich ein tatsächlicher Abfluss personenbezogener Daten nicht nachweisen lässt, besteht häufig zumindest die konkrete Möglichkeit einer Datenschutzverletzung.

Vor diesem Hintergrund gewinnt auch das europäische IT-Sicherheitsrecht für die Datenschutzaufsicht zunehmend an Bedeutung. Die Europäische Union hat in den

vergangenen Jahren mehrere Rechtsakte verabschiedet, mit denen Cybersicherheit und Widerstandsfähigkeit digitaler Infrastrukturen innerhalb Europas nachhaltig gestärkt werden sollen. Hierzu zählen insbesondere die NIS-2-Richtlinie, der Digital Operational Resilience Act (DORA) sowie der Cyber Resilience Act (CRA), deren wesentliche Inhalte nachfolgend dargestellt werden.

> Datenschutz und Informationssicherheit verfolgen unterschiedliche Schutzziele, ergänzen sich jedoch bei der sicheren Gestaltung digitaler Prozesse.

2.1.5.1 NIS-2

Mit der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) hat die Europäische Union den europäischen Rechtsrahmen zur Informationssicherheit grundlegend überarbeitet. Ziel der Richtlinie ist es, die Cybersicherheit kritischer und besonders wichtiger Einrichtungen zu stärken und ein unionsweit einheitliches Sicherheitsniveau zu erreichen.

Die Richtlinie verpflichtet die betroffenen Einrichtungen insbesondere zur Umsetzung angemessener technischer, organisatorischer und personeller Sicherheitsmaßnahmen. Hierzu gehören ein systematisches Risikomanagement, Notfall- und Krisenmanagement, Maßnahmen zur Absicherung von Lieferketten, die Behandlung von Sicherheitsvorfällen sowie regelmäßige Überprüfungen der Wirksamkeit der getroffenen Sicherheitsmaßnahmen. Ergänzend werden umfassende Meldepflichten für erhebliche Sicherheitsvorfälle eingeführt.

Gegenüber der bisherigen NIS-Richtlinie aus dem Jahr 2016 wird der Kreis der betroffenen Einrichtungen erheblich erweitert. Erfasst werden nun deutlich mehr Unternehmen und Einrichtungen, insbesondere aus den Bereichen Gesundheit, Energie, Verkehr, Wasser, digitale Infrastruktur sowie weiteren für das Gemeinwesen bedeutsamen Sektoren.

Die Umsetzung der Richtlinie in deutsches Recht erfolgte durch das Gesetz zur Stärkung der Cybersicherheit in Deutschland, das im Dezember 2025 in Kraft trat.

Gleichzeitig wurde das bestehende IT-Sicherheitsrecht, insbesondere das BSI-Gesetz, umfassend fortentwickelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhält hierdurch zusätzliche Aufgaben und Befugnisse, um die Einhaltung der gesetzlichen Sicherheitsanforderungen zu überwachen und betroffene Einrichtungen im Fall erheblicher Cybervorfälle zu unterstützen.

Einen wesentlichen Schwerpunkt der NIS-2-Richtlinie bildet die ausdrückliche Verantwortung der Geschäftsleitungen. Cybersicherheit wird erstmals als Leitungsaufgabe ausgestaltet. Die Leitungen betroffener Einrichtungen müssen sich aktiv mit den Risiken für ihre Organisation auseinandersetzen und geeignete organisatorische sowie technische Schutzmaßnahmen veranlassen. Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen, sind zudem verpflichtet, sich beim Meldeportal des BSI zu registrieren, um insbesondere im Krisenfall eine wirksame Kommunikation sicherzustellen. Bis Mitte März 2026 hatten sich bereits rund 14.000 Einrichtungen registriert, darunter auch mehrere Einrichtungen beziehungsweise Unternehmen aus dem Aufsichtsbereich des KDSZ Bayern.

Auch wenn die NIS-2-Richtlinie kein Datenschutzrecht darstellt, bestehen erhebliche Berührungspunkte zur Datenschutz-Grundverordnung. Zahlreiche Anforderungen an das Risikomanagement, an technische und organisatorische Maßnahmen sowie an das Management von Sicherheitsvorfällen wirken sich zugleich auf den Schutz personenbezogener Daten aus. Erfolgreiche Cyberangriffe führen heute regelmäßig auch zu datenschutzrechtlichen Fragestellungen und können insbesondere Meldepflichten nach Art. 33 DSGVO beziehungsweise den entsprechenden Vorschriften des KDG auslösen.

Informationssicherheit ist damit nicht nur Voraussetzung für einen wirksamen Datenschutz, sondern zugleich wesentlicher Bestandteil der gesetzlichen Pflicht zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen.

Kirchliche Einrichtungen fallen nicht automatisch in den Anwendungsbereich der NIS-2-Richtlinie. Ob einzelne Einrichtungen oder Träger künftig erfasst werden, hängt insbesondere von ihrer Größe, ihrer Tätigkeit sowie der jeweiligen nationalen

Umsetzung der Richtlinie ab. Unabhängig von einer unmittelbaren rechtlichen Verpflichtung liefert die NIS-2-Richtlinie wichtige Orientierungspunkte dafür, welche Anforderungen heute allgemein an eine zeitgemäße Informationssicherheit gestellt werden.

Auch für die Datenschutzaufsicht gewinnt die NIS-2-Richtlinie an Bedeutung. Technische und organisatorische Maßnahmen nach Datenschutzrecht lassen sich zunehmend nur unter Berücksichtigung moderner Informationssicherheitsstandards bewerten. Datenschutz und Cybersicherheit entwickeln sich damit immer stärker zu komplementären Bestandteilen einer sicheren digitalen Infrastruktur.

Die fortschreitende Verzahnung von Datenschutzrecht und Informationssicherheit wird daher auch künftig einen wesentlichen Schwerpunkt der Aufsichtstätigkeit des KDSZ Bayern bilden.

Die Anforderungen der NIS-2-Richtlinie können zugleich Anhaltspunkte für die Auslegung des Begriffs der ‚geeigneten technischen und organisatorischen Maßnahmen“ im Datenschutzrecht liefern, auch wenn beide Regelungswerke unterschiedliche Schutzziele verfolgen.

> NIS-2 ist keine Datenschutzregelung. Die Richtlinie verdeutlicht jedoch den europäischen Maßstab für eine zeitgemäße Informationssicherheit und gewinnt damit auch für die datenschutzrechtliche Bewertung technischer und organisatorischer Maßnahmen an Bedeutung.

2.1.5.2 DORA

Mit der Verordnung (EU) 2022/2554 über die digitale operationelle Resilienz des Finanzsektors (Digital Operational Resilience Act – DORA) hat die Europäische Union erstmals einen einheitlichen Rechtsrahmen zur Stärkung der digitalen Widerstandsfähigkeit von Finanzunternehmen geschaffen. Ziel der Verordnung ist es, die Stabilität des europäischen Finanzsystems auch unter den Bedingungen zunehmender Cyberbedrohungen sicherzustellen. Seit dem 17. Januar 2025 ist DORA vollständig anwendbar. DORA ist als Verordnung unmittelbar in allen Mitgliedstaaten

anwendbar und bedurfte daher – anders als die NIS-2-Richtlinie – keiner Umsetzung in nationales Recht.

DORA gilt für eine Vielzahl regulierter Finanzunternehmen, darunter insbesondere Kreditinstitute, Versicherungsunternehmen, Zahlungsdienstleister, Wertpapierfirmen sowie bestimmte IKT-Drittdienstleister. Die Verordnung enthält umfassende Anforderungen an das Management von Informations- und Kommunikationstechnologie- Risiken, die Behandlung und Meldung von Sicherheitsvorfällen, regelmäßige Resilienztests sowie die Steuerung von Risiken bei ausgelagerten IT-Dienstleistungen. Im Mittelpunkt der Verordnung steht die Überwachung kritischer IKT-Drittdienstleister Überwachung kritischer IKT-Drittdienstleister, von deren Verfügbarkeit und Sicherheit zahlreiche Finanzunternehmen abhängig sind.

DORA stellt für den Finanzsektor einen sektorspezifischen Rechtsrahmen (lex specialis) gegenüber der NIS-2-Richtlinie dar. Soweit Finanzunternehmen in den Anwendungsbereich beider Regelungswerke fallen, gehen die spezielleren Anforderungen des DORA den allgemeinen Vorgaben der NIS-2-Richtlinie vor. Auf diese Weise soll ein einheitliches und branchenspezifisch abgestimmtes Cybersicherheitsniveau im europäischen Finanzsektor gewährleistet werden.

> DORA richtet sich unmittelbar an Finanzunternehmen. Die Verordnung verdeutlicht jedoch, welche Anforderungen die Europäische Union künftig an ein professionelles Management digitaler Risiken stellt.

Auch wenn DORA kirchliche Einrichtungen regelmäßig nicht unmittelbar erfasst, verdeutlicht die Verordnung die zunehmende Entwicklung hin zu sektorspezifischen Regelungen der Informationssicherheit. Sie zeigt zugleich, dass Cybersicherheit und digitale Resilienz heute als integraler Bestandteil einer verantwortungsvollen Organisations- und Unternehmensführung verstanden werden. Diese Entwicklung wird auch außerhalb des Finanzsektors Auswirkungen auf die Ausgestaltung technischer und organisatorischer Maßnahmen haben und ist deshalb für die datenschutzrechtliche Aufsicht von Interesse.

Während DORA die organisatorische Widerstandsfähigkeit von Finanzunternehmen stärkt, richtet sich der Cyber Resilience Act unmittelbar an Hersteller und Anbieter digitaler Produkte.

2.1.5.3 Cyber Resilience Act (CRA)

Mit der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act – CRA) hat die Europäische Union erstmals einen einheitlichen Rechtsrahmen für die Cybersicherheit digitaler Produkte geschaffen. Ziel der Verordnung ist es, die Sicherheit von Hard- und Softwareprodukten bereits bei ihrer Entwicklung zu stärken und während ihres gesamten Lebenszyklus sicherzustellen.

Der CRA verpflichtet Hersteller dazu, Produkte mit digitalen Elementen nach dem Grundsatz ‚Security by Design" (Sicherheit durch Technikgestaltung) zu entwickeln. Hersteller müssen geeignete Cybersicherheitsmaßnahmen bereits während der Produktentwicklung berücksichtigen, bekannte Schwachstellen dokumentieren, Sicherheitsupdates bereitstellen sowie erhebliche Sicherheitslücken und schwerwiegende Sicherheitsvorfälle an die zuständigen Behörden melden. Damit wird Cybersicherheit zu einem verbindlichen Qualitätsmerkmal digitaler Produkte und nicht erst zu einer Aufgabe ihrer späteren Betreiber. Die wesentlichen Anforderungen des CRA werden ab dem Jahr 2027 verbindlich anwendbar sein.

Der CRA stellt ausdrücklich klar, dass seine Regelungen die Datenschutz-Grundverordnung unberührt lassen. Zugleich knüpft die Verordnung an die Grundsätze ‚Data Protection by Design" und ‚Data Protection by Default" nach Art. 25 DSGVO an. Damit wird deutlich, dass Datenschutz und Cybersicherheit zunehmend als zusammengehörende Bestandteile einer verantwortungsvollen Entwicklung digitaler Produkte verstanden werden. Während die DSGVO den Schutz personenbezogener Daten in den Mittelpunkt stellt, verfolgt der CRA das Ziel, digitale Produkte selbst widerstandsfähiger gegenüber Cyberangriffen und Sicherheitslücken zu machen.

Gemeinsam mit der NIS-2-Richtlinie ergänzt der Cyber Resilience Act den europäischen Rechtsrahmen zur Informationssicherheit. Während NIS-2 Anforderungen an den sicheren Betrieb von Einrichtungen und Organisationen stellt, richtet sich der CRA an Hersteller und Anbieter digitaler Produkte. Beide Regelungswerke verfolgen unterschiedliche Ansätze, stärken jedoch gemeinsam das Cybersicherheitsniveau innerhalb der Europäischen Union.

Kirchliche Einrichtungen richten sich regelmäßig nicht als Hersteller digitaler Produkte an den Markt und fallen daher nur ausnahmsweise unmittelbar in den Anwendungsbereich des CRA. Gleichwohl profitieren sie mittelbar von den höheren Sicherheitsanforderungen, da digitale Produkte künftig mit einem höheren Sicherheitsniveau entwickelt und über einen längeren Zeitraum mit Sicherheitsupdates versorgt werden müssen.

Der CRA verdeutlicht den grundlegenden Wandel des europäischen Digitalrechts. Informationssicherheit soll bereits bei der Entwicklung digitaler Produkte berücksichtigt werden und nicht erst durch organisatorische Maßnahmen ihrer Betreiber. Das KDSZ Bayern wird die weitere Umsetzung des CRA und seine Auswirkungen auf die Bewertung technischer und organisatorischer Maßnahmen im kirchlichen Bereich weiterhin aufmerksam begleiten.

> Der Cyber Resilience Act richtet sich in erster Linie an Hersteller digitaler Produkte. Kirchliche Einrichtungen profitieren von höheren Sicherheitsstandards, einer besseren Versorgung mit Sicherheitsupdates und damit von einer insgesamt sichereren digitalen Infrastruktur.

Die dargestellten europäischen Rechtsakte zeigen, dass Datenschutz, Informationssicherheit und digitale Resilienz heute zunehmend als zusammenhängende Elemente eines modernen europäischen Digitalrechts verstanden werden. Auch wenn kirchliche Einrichtungen nicht von allen Regelungen unmittelbar betroffen sind, prägen sie die Anforderungen an eine sichere und verantwortungsvolle Digitalisierung nachhaltig.

Während die dargestellten europäischen Rechtsakte den allgemeinen Rahmen des europäischen Digitalrechts fortentwickeln, wurde auch das kirchliche Datenschutzrecht im Berichtsjahr grundlegend überarbeitet.

2.2 Fortentwicklung des kirchlichen Datenschutzrechts

Neben den Entwicklungen des europäischen Digitalrechts wurde auch das kirchliche Datenschutzrecht im Berichtsjahr grundlegend fortentwickelt. Mit der Novellierung des KDG sowie der Neufassung der KDG-DVO wurden zahlreiche Regelungen an die zwischenzeitlichen praktischen Erfahrungen sowie an die europäische Rechtsentwicklung angepasst.

Ziel der Reform war keine grundlegende Neuausrichtung des kirchlichen Datenschutzrechts. Vielmehr dienten die Änderungen der Weiterentwicklung bestehender Regelungen, der Schließung praktischer Regelungslücken sowie einer stärkeren Orientierung an den Anforderungen einer zunehmend digitalisierten Verwaltung und Sozialwirtschaft.

2.2.1 Reform des Gesetzes über den Kirchlichen Datenschutz (KDG) - Weiterentwicklung des kirchlichen Datenschutzrechts

Mit dem Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) im November 2025 wurde die erste umfassende Reform des Gesetzes über den Kirchlichen Datenschutz (KDG) seit seinem Inkrafttreten im Jahr 2018 verabschiedet. Parallel hierzu wurde auch die Durchführungsverordnung zum KDG (KDG-DVO) grundlegend überarbeitet. Beide Regelwerke traten in den jeweiligen Diözesen zum 1. März 2026 in Kraft und bilden seither den maßgeblichen Rechtsrahmen für den Datenschutz in der katholischen Kirche in Deutschland.

Die Novellierung stellt keine grundlegende Neuausrichtung des kirchlichen Datenschutzrechts dar. Vielmehr knüpft sie an die seit 2018 bewährten Strukturen des KDG an und entwickelt diese auf der Grundlage der zwischenzeitlich gewonnenen

praktischen Erfahrungen sowie der rechtlichen und technischen Entwicklungen konsequent weiter. Ziel der Reform ist es, bestehende Regelungen zu präzisieren, ihre praktische Anwendbarkeit zu verbessern und den Herausforderungen einer zunehmend digitalisierten Verwaltung Rechnung zu tragen. Zugleich wird das Datenschutzniveau innerhalb der katholischen Kirche weiter gestärkt.

> Die KDG-Novelle stellt keine grundlegende Neuausrichtung des kirchlichen Datenschutzrechts dar. Sie entwickelt die seit 2018 bewährten Regelungen konsequent weiter und passt sie an die Anforderungen einer zunehmend digitalisierten kirchlichen Praxis an.

Die Reform verfolgt dabei mehrere Zielsetzungen. Neben einer stärkeren Orientierung an der Terminologie und Systematik der DSGVO werden insbesondere die Anforderungen moderner Informations- und Kommunikationstechnologien, neuer Formen digitaler Zusammenarbeit sowie gewachsener organisatorischer Strukturen berücksichtigt. Gleichzeitig wurden zahlreiche Regelungen sprachlich und systematisch weiter an das europäische und staatliche Datenschutzrecht angenähert, kirchenspezifische Besonderheiten ausdrücklich geregelt und bestehende Praxisfragen einer rechtssicheren Lösung zugeführt. Die Novellierung versteht sich damit gleichermaßen als Beitrag zur Rechtssicherheit, zur Praktikabilität des kirchlichen Datenschutzrechts und zur weiteren Professionalisierung der Datenschutzorganisation innerhalb der Kirche.

Bereits die überarbeitete Präambel verdeutlicht diese Weiterentwicklung des kirchlichen Datenschutzrechts. Anders als die bisherige Fassung hebt sie ausdrücklich hervor, dass der Schutz personenbezogener Daten Bestandteil der kirchlichen Grundrechtsordnung ist und sich insbesondere aus can. 220 CIC ableitet. Gleichzeitig wird betont, dass die Verarbeitung personenbezogener Daten zur Erfüllung kirchlicher Aufgaben erforderlich ist und das kirchliche Datenschutzrecht weiterhin im Einklang mit den Vorgaben der Datenschutz-Grundverordnung fortentwickelt wird.

Die Gesetzesbegründung stellt zugleich klar, dass der kirchliche Auftrag keine eigenständige datenschutzrechtliche Rechtsgrundlage für jede Verarbeitung personenbezogener Daten begründet. Vielmehr bedarf auch künftig jede Verarbeitung einer gesetzlichen Erlaubnisnorm oder einer wirksamen Einwilligung.

Damit unterstreicht die Präambel zugleich die Eigenständigkeit des kirchlichen Datenschutzrechts im Rahmen des verfassungs- und europarechtlich gewährleisteten kirchlichen Selbstbestimmungsrechts.

Wesentliche Neuerungen der KDG-Novelle

Die Reform entwickelt das kirchliche Datenschutzrecht behutsam weiter und passt es an die Anforderungen einer zunehmend digitalisierten Verwaltung an. Zu den wichtigsten Änderungen gehören insbesondere:

- ☑ Einwilligung: Wegfall der Schriftform; künftig grundsätzlich formfrei möglich.
- ☑ Auftragsverarbeitung: Vereinbarungen können künftig in Textform abgeschlossen werden.
- ☑ Betriebliche Datenschutzbeauftragte: Anhebung der Benennungsschwelle von zehn auf zwanzig mit der Verarbeitung personenbezogener Daten beschäftigte Personen.
- ☑ § 52a KDG: Neue datenschutzrechtliche Regelungen für Gottesdienste und sonstige kirchliche Veranstaltungen.
- ☑ § 54a KDG: Neuer Rechtsrahmen für Datenverarbeitungen im Zusammenhang mit der institutionellen Aufarbeitung sexualisierter Gewalt.
- ☑ Datenschutzaufsicht: Präzisierung der Aufgaben und Befugnisse sowie stärkere Orientierung an Art. 58 DSGVO.

Modernisierung des materiellen Datenschutzrechts

Ein weiterer Schwerpunkt der Reform liegt in der Fortentwicklung des materiellen Datenschutzrechts. Zahlreiche Vorschriften wurden sprachlich, systematisch und inhaltlich überarbeitet, um sie besser an die Datenschutz-Grundverordnung anzupassen und zugleich den Anforderungen einer zunehmend digitalisierten kirchlichen Verwaltung gerecht zu werden. Dabei handelt es sich überwiegend nicht um grundlegende inhaltliche Neuregelungen, sondern um eine gezielte Weiterentwicklung und Präzisierung bestehender Vorschriften. Ziel ist es, Rechtsunsicherheiten zu beseitigen, die praktische Anwendung des Gesetzes zu erleichtern und bislang ungeklärte Fallgestaltungen ausdrücklich zu regeln.

Hierzu zählen unter anderem Anpassungen der Begriffsbestimmungen, eine stärkere Annäherung an die unionsrechtliche Terminologie sowie Klarstellungen zur gemeinsamen Verantwortlichkeit, zur Auftragsverarbeitung, zur Verarbeitung personenbezogener Daten im Beschäftigungskontext und zur internationalen Datenübermittlung. Darüber hinaus wurde der Beschäftigtenbegriff erweitert und umfasst nun ausdrücklich auch Leiharbeitnehmerinnen und Leiharbeitnehmer, soweit diese bei kirchlichen Stellen eingesetzt werden.

Auch die Vorschriften über betriebliche Datenschutzbeauftragte wurden punktuell weiterentwickelt. In Anlehnung an das staatliche Datenschutzrecht wurde die Schwelle für die verpflichtende Benennung eines Datenschutzbeauftragten von zehn auf zwanzig mit der Verarbeitung personenbezogener Daten beschäftigte Personen angehoben. Zugleich stellt das Gesetz nun ausdrücklich klar, dass auch juristische Personen als betriebliche Datenschutzbeauftragte benannt werden können. Damit trägt die Novelle den inzwischen etablierten Strukturen externer Datenschutzberatung Rechnung und schafft zusätzliche Flexibilität bei der organisatorischen Umsetzung des Datenschutzes.

Von erheblicher praktischer Bedeutung ist darüber hinaus die Neuregelung der datenschutzrechtlichen Einwilligung. Die bislang im KDG vorgesehene Schriftform wurde aufgegeben. Künftig kann eine Einwilligung grundsätzlich formfrei erteilt

werden, soweit das Gesetz keine besondere Form vorschreibt. Hierdurch trägt der Gesetzgeber den Anforderungen moderner digitaler Kommunikations- und Verwaltungsprozesse Rechnung und eröffnet insbesondere den Einsatz elektronischer Verfahren.

Die praktische Erleichterung sollte allerdings nicht überschätzt werden. Verantwortliche bleiben weiterhin verpflichtet, das Vorliegen einer wirksamen Einwilligung nachweisen zu können. Gerade im Streitfall kann eine lediglich mündlich erteilte Einwilligung erhebliche Beweisschwierigkeiten mit sich bringen. Die eigentliche Bedeutung der Neuregelung liegt deshalb weniger im vollständigen Verzicht auf Formerfordernisse als vielmehr in der Möglichkeit, künftig verstärkt die Textform oder andere dokumentierbare elektronische Verfahren zu nutzen. Insbesondere Einwilligungen per E-Mail, über Online-Formulare oder vergleichbare digitale Kommunikationswege können dadurch rechtssicherer und zugleich praxisgerechter eingesetzt werden. Die Änderung verdeutlicht zugleich den grundlegenden Ansatz der KDG-Novelle: Das Datenschutzniveau wird nicht abgesenkt, vielmehr werden bestehende Anforderungen an die Erfordernisse einer zunehmend digitalisierten Verwaltung angepasst und ihre praktische Umsetzung erleichtert.

> Die Abschaffung der Schriftform erleichtert digitale Verfahren. Die Pflicht, eine wirksame Einwilligung nachweisen zu können, bleibt jedoch unverändert bestehen.

Ein ähnlicher Modernisierungsgedanke zeigt sich auch bei den Regelungen zur Auftragsverarbeitung. Vereinbarungen zwischen Verantwortlichen und kirchlichen Auftragsverarbeitern können künftig ebenfalls in Textform abgeschlossen werden. Hierdurch werden digitale Verwaltungs- und Beschaffungsprozesse erleichtert und der Abschluss entsprechender Verträge vereinfacht, ohne die inhaltlichen Anforderungen an die Vereinbarung oder deren Nachweisbarkeit zu verändern. Gleichzeitig entfällt die bisherige Beschränkung, wonach Auftragsverarbeiter ihren Sitz grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums haben mussten. Künftig richtet sich die Zulässigkeit der Einbindung von Auftragsverarbeitern in Drittstaaten nach den allgemeinen Vorschriften über

internationale Datenübermittlungen. Damit orientiert sich das KDG auch in diesem Bereich stärker an der Systematik der DSGVO und trägt der zunehmenden internationalen Ausrichtung moderner IT- und Cloud-Dienste Rechnung. Auch diese Änderungen verdeutlichen, dass die Reform bestehende Datenschutzstandards nicht absenkt, sondern deren praktische Umsetzung an moderne Kommunikations-, Verwaltungs- und IT-Strukturen anpasst.

Neu aufgenommen wurde außerdem eine ausdrückliche Einbeziehung ehrenamtlich tätiger Personen in die Verpflichtung zur Wahrung der Vertraulichkeit personenbezogener Daten. Damit stellt das Gesetz klar, dass auch Ehrenamtliche, soweit sie personenbezogene Daten verarbeiten, den datenschutzrechtlichen Verschwiegenheits- und Vertraulichkeitspflichten unterliegen. Angesichts der herausragenden Bedeutung ehrenamtlichen Engagements innerhalb der katholischen Kirche und Sozialarbeit schafft die Neuregelung mehr Rechtssicherheit für die kirchliche Praxis.

Ebenfalls von systematischer Bedeutung ist die Anpassung einzelner Begriffsbestimmungen an die Terminologie der DSGVO. So wurde insbesondere der bislang eigenständig definierte Begriff der ‚Offenlegung" aus dem KDG gestrichen. Da die Offenlegung bereits als Form der Verarbeitung personenbezogener Daten von den allgemeinen Regelungen des KDG erfasst wird, bedarf es hierfür künftig keiner eigenständigen gesetzlichen Definition mehr. Die bisher darunter erfassten Fallgestaltungen werden nun durch die allgemeinen Vorschriften über die Verarbeitung personenbezogener Daten sowie den unionsrechtlich geprägten Begriff der ‚Übermittlung" abgedeckt. Dadurch werden Doppelregelungen vermieden, die Terminologie weiter an die Datenschutz-Grundverordnung angeglichen und die praktische Anwendung des Gesetzes vereinfacht.

Besondere praktische Bedeutung besitzen die neu geschaffenen Sonderregelungen für spezifische kirchliche Verarbeitungssituationen. Mit § 52a KDG wurde erstmals eine ausdrückliche datenschutzrechtliche Grundlage für Datenverarbeitungen im Zusammenhang mit Gottesdiensten und sonstigen kirchlichen Veranstal-

tungen geschaffen. Die Vorschrift trägt insbesondere den Herausforderungen moderner Kommunikationsformen Rechnung und schafft einen rechtlichen Rahmen für Bild- und Tonaufnahmen, Livestreams sowie Veröffentlichungen im kirchlichen Kontext. Dadurch werden zahlreiche Fragestellungen geregelt, die in den vergangenen Jahren zunehmend an praktischer Bedeutung gewonnen haben.

Von erheblicher Bedeutung ist ferner der neu eingefügte § 54a KDG zur Verarbeitung personenbezogener Daten im Zusammenhang mit der institutionellen Aufarbeitung sexualisierter Gewalt und anderer Formen des Missbrauchs. Die Vorschrift schafft keine eigenständige Rechtsgrundlage im Sinne einer allgemeinen Erlaubnisnorm, sondern regelt die datenschutzrechtlichen Voraussetzungen, unter denen solche besonders sensiblen Verarbeitungsvorgänge im Rahmen kirchlicher Aufarbeitungsprozesse erfolgen können. Sie bringt das berechtigte Interesse an Transparenz, Aufklärung und institutioneller Verantwortung mit den Rechten der betroffenen Personen in einen angemessenen Ausgleich und schafft damit mehr Rechtssicherheit für die praktische Durchführung von Aufarbeitungsvorhaben.

> Mit den neuen §§ 52a und 54a KDG enthält das kirchliche Datenschutzrecht erstmals ausdrückliche Sonderregelungen für spezifische kirchliche Verarbeitungssituationen.

Zu den kirchenspezifischen Besonderheiten der Novelle gehört schließlich auch die Präzisierung der Vorschriften über Kirchenbücher und kirchliche Urkunden. Das Gesetz stellt ausdrücklich klar, dass Einträge in Kirchenbüchern – etwa über die Taufe, Firmung oder den Kirchenaustritt – grundsätzlich nicht gelöscht werden, sondern lediglich durch ergänzende Vermerke fortgeschrieben werden können. Damit trägt das KDG der besonderen Funktion kirchlicher Register als dauerhaft geführte Beweis- und Dokumentationsmittel Rechnung und bringt diese zugleich mit den datenschutzrechtlichen Anforderungen in Einklang. Die Regelung verdeutlicht beispielhaft, dass das kirchliche Datenschutzrecht zwar eng an die Datenschutz-Grundverordnung angelehnt ist, zugleich aber die Besonderheiten kirchlicher Aufgaben und Rechtsverhältnisse berücksichtigt.

Die Änderungen des materiellen Datenschutzrechts verdeutlichen insgesamt den Charakter der Reform. Ziel war nicht eine grundlegende Neuausrichtung des kirchlichen Datenschutzrechts, sondern dessen behutsame Weiterentwicklung. Zahlreiche Regelungen wurden präzisiert, an technische und organisatorische Entwicklungen angepasst und um kirchenspezifische Besonderheiten ergänzt. Dadurch gewinnt das kirchliche Datenschutzrecht sowohl an Rechtssicherheit als auch an praktischer Handhabbarkeit und schafft zugleich verlässliche Rahmenbedingungen für die fortschreitende Digitalisierung kirchlicher Verwaltungs- und Arbeitsprozesse.

Stärkung der Datenschutzaufsicht und Weiterentwicklung des Rechtsschutzes

Einen wesentlichen Schwerpunkt der KDG-Novelle bildet die Fortentwicklung der kirchlichen Datenschutzaufsicht. Zwar sah bereits das bisherige KDG eine unabhängige Datenschutzaufsicht mit eigenen Untersuchungs- und Eingriffsbefugnissen vor. Die Reform präzisiert diese Befugnisse jedoch deutlich, entwickelt sie systematisch weiter und orientiert sich dabei noch stärker an der Struktur der Datenschutz-Grundverordnung. Dadurch werden Aufgaben, Zuständigkeiten und Eingriffsmöglichkeiten der Datenschutzaufsicht klarer gefasst und für die Praxis transparenter ausgestaltet.

Bereits die Gesetzessystematik bringt diese Weiterentwicklung zum Ausdruck. Das bisherige Kapitel ‚Datenschutzaufsicht“ trägt nun die Überschrift ‚Unabhängige Datenschutzaufsicht“. Hierdurch wird die institutionelle Eigenständigkeit der kirchlichen Datenschutzaufsichten ausdrücklich hervorgehoben und ihre Stellung innerhalb des kirchlichen Datenschutzrechts weiter verdeutlicht.

Von besonderer praktischer Bedeutung ist die Neufassung des § 47 KDG. Während das bisherige Recht die Aufgaben und Befugnisse der Datenschutzaufsicht bereits regelte, werden diese nun wesentlich ausführlicher beschrieben und stärker an den Regelungen des Art. 58 DSGVO ausgerichtet. Die Vorschrift unterscheidet nun ausdrücklich zwischen Untersuchungs-, Abhilfe- und weiteren Aufsichtsbefugnissen und schafft dadurch eine klarere gesetzliche Systematik.

Zu den ausdrücklich geregelten Untersuchungsbefugnissen gehören insbesondere das Recht, Auskünfte zu verlangen, Einsicht in Unterlagen zu nehmen, Vor-Ort-Prüfungen durchzuführen sowie Zugang zu personenbezogenen Daten und den hierfür eingesetzten Verarbeitungssystemen zu erhalten. Korrespondierend hierzu werden Verantwortliche und kirchliche Auftragsverarbeiter ausdrücklich verpflichtet, mit der Datenschutzaufsicht zusammenzuarbeiten und die zur Aufgabenerfüllung erforderlichen Informationen bereitzustellen.

Auch die Abhilfebefugnisse werden im Gesetz nun detaillierter beschrieben. Hierzu gehören insbesondere Verwarnungen, Anweisungen zur Herstellung rechtmäßiger Zustände, Einschränkungen oder Verbote von Datenverarbeitungen, Anordnungen zur Löschung personenbezogener Daten, Verpflichtungen zur Umsetzung technischer und organisatorischer Maßnahmen sowie die Aussetzung von Datenübermittlungen. Diese Maßnahmen standen der Datenschutzaufsicht im Kern bereits bislang zur Verfügung; ihre gesetzliche Ausgestaltung wird jedoch präzisiert und systematisch klarer gefasst. Dadurch gewinnen sowohl die Datenschutzaufsicht als auch die kirchlichen Verantwortlichen an Rechtsklarheit und Rechtssicherheit.

> Die Novelle erweitert die Aufgaben der Datenschutzaufsicht nicht grundlegend. Sie präzisiert und systematisiert die bereits bestehenden Befugnisse und schafft dadurch mehr Rechtsklarheit.

Parallel hierzu wurden auch die verfahrensrechtlichen Regelungen weiterentwickelt. Die Novelle enthält zusätzliche Vorschriften zu gerichtlichen Rechtsbehelfen gegen Verantwortliche und kirchliche Auftragsverarbeiter sowie zur gerichtlichen Zuständigkeit. Auch die Vorschriften über Geldbußen und sonstige Sanktionen wurden überarbeitet und weiter an die Systematik der Datenschutz-Grundverordnung angenähert.

Die Reform verdeutlicht insgesamt, dass die kirchliche Datenschutzaufsicht auch künftig ihre Aufgaben gleichermaßen beratend, kontrollierend und erforderlichenfalls durchsetzungsorientiert wahrnimmt. Die Präzisierung der gesetzlichen Befugnisse stärkt dabei weniger den Umfang der Aufsicht als vielmehr deren Rechtsklar-

heit und trägt zu einer einheitlicheren und nachvollziehbareren Anwendung des kirchlichen Datenschutzrechts bei.

> Die Reform verbindet Datenschutz, Digitalisierung und Informationssicherheit zu einem modernen Rechtsrahmen für die kirchliche Verwaltung.

Auswirkungen auf die Praxis und Schlussbetrachtung

Für kirchliche Verantwortliche und kirchliche Auftragsverarbeiter führt die Reform zu einem umfassenden Überprüfungs- und Anpassungsbedarf. Datenschutzkonzepte, Verzeichnisse von Verarbeitungstätigkeiten, technische und organisatorische Maßnahmen sowie interne Richtlinien und Verfahrensabläufe sollten daraufhin überprüft werden, ob sie den neuen gesetzlichen Vorgaben entsprechen. Besonderes Augenmerk ist dabei auf die erweiterten Dokumentations- und Mitwirkungspflichten gegenüber der Datenschutzaufsicht sowie auf die neuen spezialgesetzlichen Regelungen für bestimmte kirchliche Verarbeitungssituationen zu legen.

Gleichzeitig stärkt die Novelle die Rechtssicherheit für kirchliche Einrichtungen. Zahlreiche bislang ungeklärte Praxisfragen werden ausdrücklich geregelt, gesetzliche Begriffe präzisiert und Verfahrensabläufe vereinheitlicht. Dies erleichtert nicht nur die Anwendung des kirchlichen Datenschutzrechts, sondern trägt auch dazu bei, Datenschutzprozesse innerhalb kirchlicher Einrichtungen verlässlicher und nachvollziehbarer zu gestalten.

Die Reform verdeutlicht zugleich, dass Datenschutz heute nicht mehr isoliert betrachtet werden kann. Moderne Datenschutzorganisation umfasst zunehmend auch Informationssicherheit, digitale Verwaltungsprozesse, Dokumentation, Compliance und den verantwortungsvollen Einsatz neuer Technologien. Diese Entwicklung spiegelt sich sowohl in der KDG-Novelle als auch in den zeitgleich auf europäischer Ebene verabschiedeten Rechtsakten wider und stellt kirchliche Einrichtungen vor die Aufgabe, ihre organisatorischen Strukturen kontinuierlich weiterzuentwickeln.

Insgesamt stellt die Novellierung des KDG einen wichtigen Schritt zur Fortentwicklung des kirchlichen Datenschutzrechts dar. Sie stärkt die Rechte betroffener Personen, präzisiert die Aufgaben und Befugnisse der Datenschutzaufsicht und schafft zugleich klarere sowie praxisgerechtere Rahmenbedingungen für die Verarbeitung personenbezogener Daten innerhalb der katholischen Kirche. Die Reform verbindet damit die bewährten Grundstrukturen des kirchlichen Datenschutzrechts mit den Anforderungen einer zunehmend digitalisierten Arbeits- und Verwaltungswelt und leistet einen wesentlichen Beitrag zur weiteren Professionalisierung des Datenschutzes in der katholischen Kirche in Deutschland.

Info-Karte Katholikentag: Top 10 der KDG-/KDG-DVO-Novellierung (KDSZ-FFM)

2.2.2 Novellierung der Durchführungsverordnung zum KDG

Parallel zur Reform des Gesetzes über den Kirchlichen Datenschutz (KDG) wurde im Jahr 2025 auch die Durchführungsverordnung zum KDG (KDG-DVO) umfassend überarbeitet. Während das KDG die grundlegenden datenschutzrechtlichen Anforderungen festlegt, konkretisiert die KDG-DVO deren praktische Umsetzung. Sie enthält insbesondere Vorgaben zu technischen und organisatorischen Maßnahmen, zur Informationssicherheit sowie zur datenschutzgerechten Ausgestaltung kirchli-

cher Verwaltungs- und IT-Prozesse. Beide Regelwerke ergänzen sich damit zu einem einheitlichen Rechtsrahmen für den Datenschutz innerhalb der katholischen Kirche.

Die Neufassung der KDG-DVO stellt keine grundlegende Neuausrichtung des kirchlichen Datenschutzrechts dar. Vielmehr knüpft sie an die bewährten Strukturen der bisherigen Durchführungsverordnung an und entwickelt diese vor dem Hintergrund der fortschreitenden Digitalisierung sowie neuer technischer und organisatorischer Anforderungen konsequent weiter. Die Reform reagiert insbesondere auf veränderte IT-Infrastrukturen, mobile Arbeitsformen, die zunehmende Nutzung cloudbasierter Dienste sowie auf die wachsenden Anforderungen an Informationssicherheit und Cyberresilienz.

Die Novelle verfolgt dabei mehrere Zielsetzungen. Zum einen werden bestehende Regelungen modernisiert, präzisiert und an den aktuellen Stand der Technik angepasst. Zum anderen wird der risikobasierte Ansatz des Datenschutzrechts konsequent weiterentwickelt und stärker mit den Anforderungen moderner Informationssicherheit verzahnt. Gleichzeitig verdeutlicht die Reform, dass Datenschutz heute nicht allein durch einzelne technische Maßnahmen gewährleistet werden kann, sondern als kontinuierlicher Organisationsprozess verstanden werden muss, der Planung, Dokumentation, regelmäßige Überprüfung sowie die Sensibilisierung der Mitarbeitenden gleichermaßen umfasst.

Damit entwickelt sich die KDG-DVO zunehmend von einer klassischen Ausführungsverordnung zu einem modernen Regelwerk für Datenschutzorganisation und Informationssicherheit.

> Die KDG-DVO entwickelt sich von einer klassischen Ausführungsverordnung zu einem Organisationsregelwerk für Datenschutz und Informationssicherheit.

Sie schafft einen praxisorientierten Rahmen für die Umsetzung datenschutzrechtlicher Anforderungen in einer zunehmend digitalisierten Arbeitswelt und trägt zugleich den besonderen Anforderungen kirchlicher Einrichtungen Rechnung.

Wesentliche Neuerungen der KDG-DVO

Die Neufassung der Durchführungsverordnung zum KDG entwickelt die Datenschutzorganisation und Informationssicherheit innerhalb kirchlicher Einrichtungen konsequent weiter. Zu den wichtigsten Neuerungen gehören insbesondere:

- ☑ **Risikoorientierter Ansatz:** Technische und organisatorische Maßnahmen orientieren sich künftig stärker am konkreten Risiko für die Rechte und Freiheiten der betroffenen Personen.
- ☑ **Cloud-Dienste:** Erstmals werden cloudbasierte Dienste ausdrücklich geregelt und datenschutzrechtliche Anforderungen an deren Einsatz konkretisiert.
- ☑ **Mobile und hybride Arbeit:** Die Verordnung berücksichtigt ausdrücklich moderne Arbeitsformen sowie dezentrale IT-Infrastrukturen.
- ☑ **Faxkommunikation:** Die Übermittlung personenbezogener Daten per Telefax ist grundsätzlich nicht mehr vorgesehen und nur noch in begründeten Ausnahmefällen zulässig.
- ☑ **Datenschutz durch Technikgestaltung:** Die Grundsätze ‚Privacy by Design" und ‚Privacy by Default" werden bei der Auswahl und Einführung neuer IT-Systeme stärker hervorgehoben.
- ☑ **Dokumentationspflichten:** Datenschutzmaßnahmen müssen regelmäßig überprüft, aktualisiert und nachvollziehbar dokumentiert werden.
- ☑ **Schulungen und Sensibilisierung:** Die regelmäßige Qualifizierung der Mitarbeitenden wird als wesentlicher Bestandteil eines wirksamen Datenschutz- und Informationssicherheitsmanagements ausdrücklich hervorgehoben.

Datenschutzorganisation und Risikomanagement

Einen wesentlichen Schwerpunkt der Neufassung bildet die Weiterentwicklung der technischen und organisatorischen Maßnahmen (TOM). Während die bisherigen Regelungen bereits Anforderungen an den Schutz personenbezogener Daten enthielten, richtet die novellierte KDG-DVO den Blick stärker auf ein risikoorientiertes Datenschutzmanagement. Technische und organisatorische Maßnahmen werden damit nicht mehr ausschließlich als einzelne Sicherheitsvorkehrungen verstanden, sondern als Bestandteil eines fortlaufenden Organisations- und Steuerungsprozesses.

Bereits die Neustrukturierung der Vorschriften zu Datenschutzklassen und Schutzniveaus verdeutlicht diesen Ansatz. Während die bisherige Fassung zwischen der Einordnung in Datenschutzklassen und dem jeweiligen Schutzniveau unterschied, führt die Neufassung beide Aspekte in § 9 KDG-DVO zusammen und stellt die Risikoanalyse stärker in den Mittelpunkt. Maßgeblich ist künftig nicht mehr allein die Art der verarbeiteten Daten, sondern insbesondere das konkrete Risiko für die Rechte und Freiheiten der betroffenen Personen. Die KDG-DVO folgt damit konsequent dem bereits aus der Datenschutz-Grundverordnung bekannten risikobasierten Ansatz.

> Nicht die Art der Daten allein bestimmt künftig das erforderliche Schutzniveau, sondern das konkrete Risiko für die Rechte und Freiheiten der betroffenen Personen.

Hierdurch wird zugleich deutlich, dass Datenschutz nicht schematisch umgesetzt werden kann. Vielmehr müssen Verantwortliche die konkreten Verarbeitungsprozesse bewerten und auf dieser Grundlage angemessene technische und organisatorische Maßnahmen auswählen. Die Anforderungen an den Datenschutz orientieren sich damit stärker an den tatsächlichen Gefährdungen und den jeweiligen Rahmenbedingungen der Verarbeitung.

Mit dieser Entwicklung gewinnen auch Dokumentation und Nachweisführung weiter an Bedeutung. Die KDG-DVO verdeutlicht, dass Datenschutzmaßnahmen nicht

nur einmalig festgelegt, sondern regelmäßig überprüft, fortgeschrieben und nachvollziehbar dokumentiert werden müssen. Dies betrifft sowohl die Überprüfung von Verarbeitungstätigkeiten als auch die Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen. Datenschutz wird damit ausdrücklich als kontinuierlicher Verbesserungsprozess verstanden.

Die Dokumentationspflichten beziehen sich dabei künftig ausdrücklich nicht nur auf die erstmalige Erstellung der erforderlichen Unterlagen, sondern auch auf deren regelmäßige Überprüfung, Aktualisierung und Fortschreibung. Hierdurch wird verdeutlicht, dass Datenschutzdokumentationen keine statischen Verzeichnisse darstellen, sondern fortlaufend an technische, organisatorische und rechtliche Veränderungen angepasst werden müssen. Die Nachweisbarkeit datenschutzrechtlicher Maßnahmen gewinnt dadurch weiter an Bedeutung.

> Datenschutzdokumentationen sind keine statischen Verzeichnisse. Sie müssen regelmäßig überprüft, aktualisiert und fortgeschrieben werden.

Besonders hervorgehoben wird in diesem Zusammenhang die Orientierung an anerkannten technischen und organisatorischen Standards. Die regelmäßige Überprüfung der Sicherheitsmaßnahmen soll sich insbesondere an den Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie an vergleichbaren anerkannten Standards, etwa der Normenreihe ISO/IEC 27001, orientieren. Dadurch wird deutlich, dass Datenschutz und Informationssicherheit zunehmend nach objektivierbaren und allgemein anerkannten Maßstäben bewertet werden.

Die Neufassung der KDG-DVO verdeutlicht damit einen grundlegenden Wandel der Datenschutzorganisation. Datenschutz erschöpft sich nicht mehr in der Einhaltung einzelner gesetzlicher Vorgaben oder technischer Schutzmaßnahmen. Vielmehr wird ein systematischer Managementansatz verfolgt, bei dem Risiken fortlaufend bewertet, Schutzmaßnahmen regelmäßig angepasst und deren Wirksamkeit kontinuierlich überprüft werden. Die KDG-DVO trägt damit den Anforderungen einer

zunehmend digitalisierten und vernetzten Arbeitswelt Rechnung und stärkt zugleich die organisatorische Verantwortung kirchlicher Einrichtungen für den Schutz personenbezogener Daten.

Informationssicherheit und moderne IT-Infrastrukturen

Ein weiterer Schwerpunkt der Novellierung liegt in der Anpassung der KDG-DVO an moderne IT-Infrastrukturen und digitale Arbeitsformen. Während sich die bisherige Fassung noch weitgehend an klassischen lokalen IT-Systemen orientierte, berücksichtigt die Neufassung ausdrücklich die technische Entwicklung der vergangenen Jahre und trägt den veränderten Rahmenbedingungen kirchlicher Einrichtungen, aber auch neuen Formen der Kommunikation Rechnung.

Dies zeigt sich bereits bei den Begriffsbestimmungen. Die KDG-DVO bezieht nun ausdrücklich moderne Formen der Datenverarbeitung ein und berücksichtigt insbesondere mobile Endgeräte, eingebettete Systeme (Embedded Systems), Komponenten des ‚Internet of Things" (IoT), netzwerkgestützte Anwendungen sowie unterschiedliche Modelle cloudbasierter Dienste. Erfasst werden damit sowohl Software-as-a-Service (SaaS) als auch Plattform- (PaaS) und Infrastrukturangebote (IaaS). Die Verordnung trägt damit der Tatsache Rechnung, dass Datenverarbeitung heute vielfach dezentral erfolgt und sich nicht mehr auf lokale Server und abgeschlossene Netzwerke beschränkt.

Die Verordnung berücksichtigt darüber hinaus ausdrücklich unterschiedliche Nutzungsszenarien dienstlicher und privater IT-Systeme. Damit trägt sie den inzwischen weit verbreiteten mobilen und hybriden Arbeitsformen Rechnung, bei denen personenbezogene Daten häufig außerhalb klassischer Büroarbeitsplätze verarbeitet werden. Verantwortliche sind deshalb gehalten, auch für diese Einsatzbereiche angemessene technische und organisatorische Schutzmaßnahmen vorzusehen und deren Einhaltung sicherzustellen.

Besondere praktische Bedeutung kommt dabei der erstmaligen ausdrücklichen Regelung der Nutzung von Cloud-Diensten zu. Erstmals widmet die KDG-DVO die-

sem Themenbereich einen eigenen Paragraphen und schafft damit einen spezifischen Rechtsrahmen für eine Technologie, die inzwischen auch im kirchlichen Bereich zum Arbeitsalltag gehört. Cloudbasierte Anwendungen werden heute unter anderem für Kommunikation, Zusammenarbeit, Videokonferenzen, Dokumentenmanagement und Fachverfahren eingesetzt. Die Novelle macht zugleich deutlich, dass sich durch die Auslagerung von IT-Diensten die datenschutzrechtliche Verantwortung nicht auf den jeweiligen Dienstleister verlagert. Verantwortliche bleiben vielmehr verpflichtet, die eingesetzten Cloud-Dienste sorgfältig auszuwählen und fortlaufend zu überwachen. Hierzu gehören insbesondere die Prüfung der Datenverarbeitungsorte, der eingesetzten Unterauftragnehmer, der technischen und organisatorischen Sicherheitsmaßnahmen sowie des insgesamt gewährleisteten Datenschutzniveaus.

> Die Nutzung von Cloud-Diensten entbindet Verantwortliche nicht von ihrer datenschutzrechtlichen Verantwortung.

Ein anschauliches Beispiel für die stärkere Orientierung am Stand der Technik ist die Neuregelung der Faxkommunikation. Die novellierte KDG-DVO untersagt die Übermittlung personenbezogener Daten mittels Telefax grundsätzlich. Ausnahmen sind nur zulässig, wenn sie durch den Verantwortlichen unter Berücksichtigung geeigneter technischer und organisatorischer Maßnahmen festgelegt werden und dadurch ein angemessenes Schutzniveau gewährleistet werden kann. Hintergrund dieser Regelung ist die datenschutzrechtliche Bewertung, dass herkömmliche Faxübertragungen den heutigen Anforderungen an Vertraulichkeit und Integrität personenbezogener Daten regelmäßig nicht mehr genügen. Insbesondere bei der inzwischen weit verbreiteten IP-basierten Faxübertragung bestehen vergleichbare Risiken wie bei einer unverschlüsselten elektronischen Kommunikation.

Die Neuregelung bedeutet jedoch kein pauschales Verbot des Faxgeräts als technischer Einrichtung. Maßgeblich ist vielmehr, ob der Verantwortliche im konkreten Einzelfall durch geeignete technische und organisatorische Maßnahmen ein dem Stand der Technik entsprechendes Sicherheitsniveau gewährleisten kann. Die Vor-

schrift verdeutlicht damit exemplarisch den risikobasierten Ansatz der KDG-DVO: Nicht einzelne Technologien stehen im Mittelpunkt der Bewertung, sondern die Frage, ob sie den heutigen Anforderungen an eine sichere und datenschutzgerechte Verarbeitung personenbezogener Daten gerecht werden. Zugleich fördert die Regelung den Einsatz moderner, verschlüsselter und nachvollziehbarer elektronischer Kommunikationswege.

> Die KDG-DVO verbietet nicht das Faxgerät, sondern verlangt ein dem Stand der Technik entsprechendes Sicherheitsniveau für die Übermittlung personenbezogener Daten.

Parallel hierzu werden auch die Anforderungen an die technische Absicherung von IT-Systemen weiter konkretisiert. Die KDG-DVO hebt insbesondere die Bedeutung zeitgemäßer Verschlüsselungsverfahren, wirksamer Authentifizierungs- und Berechtigungskonzepte sowie eines angemessenen Zugangsschutzes hervor. Die eingesetzten Schutzmaßnahmen sollen sich dabei am jeweiligen Stand der Technik orientieren und dem konkreten Schutzbedarf der verarbeiteten personenbezogenen Daten entsprechen. Gerade bei mobilen Arbeitsformen und der Nutzung externer Netze kommt der Verschlüsselung personenbezogener Daten eine zentrale Bedeutung zu.

Neu aufgenommen wurde darüber hinaus die ausdrückliche Verpflichtung, geeignete Maßnahmen gegen Identitätsdiebstahl zu treffen. Angesichts der zunehmenden Zahl von Phishing-Angriffen, kompromittierten Benutzerkonten und missbräuchlichen Zugriffsversuchen gewinnt dieser Aspekt der Informationssicherheit erheblich an Bedeutung. Die KDG-DVO trägt damit aktuellen Bedrohungsszenarien Rechnung und verdeutlicht, dass Datenschutz heute untrennbar mit einer wirksamen Cyberabwehr verbunden ist.

Ergänzend stärkt die Novelle den Grundsatz ‚Datenschutz durch Technikgestaltung“ und ‚Datenschutz durch datenschutzfreundliche Voreinstellungen“. Bereits bei der Auswahl, Beschaffung und Einführung neuer IT-Systeme sollen datenschutzfreundliche Lösungen bevorzugt und datenschutzrechtliche Anforderungen frühzeitig

berücksichtigt werden. Datenschutz wird damit nicht erst zu einer Frage des späteren Betriebs, sondern bereits zu einem wesentlichen Kriterium bei der Planung und Einführung neuer digitaler Verfahren.

> Datenschutz beginnt bereits bei der Auswahl und Einführung neuer IT-Systeme – nicht erst mit deren Betrieb.

Die Neufassung der KDG-DVO macht damit deutlich, dass sich Datenschutz und Informationssicherheit zunehmend gegenseitig ergänzen. Moderne IT-Infrastrukturen erfordern nicht nur leistungsfähige technische Lösungen, sondern zugleich ein hohes Maß an organisatorischer Verantwortung und kontinuierlicher Sicherheitsvorsorge. Die Verordnung trägt dieser Entwicklung Rechnung und schafft einen zeitgemäßen Rahmen für den datenschutzgerechten Einsatz moderner Informationstechnologien innerhalb kirchlicher Einrichtungen.

Mensch und Organisation als zentrale Erfolgsfaktoren

Die Novellierung der KDG-DVO verdeutlicht zugleich, dass ein wirksamer Datenschutz nicht allein durch technische Schutzmaßnahmen erreicht werden kann. Moderne Informationssicherheit setzt vielmehr voraus, dass auch die organisatorischen Rahmenbedingungen stimmen und die mit der Datenverarbeitung befassten Personen ihre Aufgaben verantwortungsbewusst wahrnehmen können. Die Reform trägt diesem Gedanken Rechnung, indem sie den Menschen als wesentlichen Bestandteil einer wirksamen Datenschutzorganisation stärker in den Mittelpunkt rückt.

Von besonderer praktischer Bedeutung ist hierbei die ausdrückliche Verpflichtung zur regelmäßigen Schulung der Mitarbeitenden. Während die bisherige Fassung der KDG-DVO den Schwerpunkt vor allem auf die Verpflichtung zur Wahrung des Datengeheimnisses legte, verlangt die Neufassung darüber hinaus eine kontinuierliche Sensibilisierung für Datenschutz und Informationssicherheit. Damit trägt der kirchliche Gesetzgeber der Erkenntnis Rechnung, dass technische Schutzmaßnahmen allein keinen ausreichenden Schutz gewährleisten können.

> Technische Schutzmaßnahmen allein gewährleisten keinen wirksamen Datenschutz. Entscheidend bleibt das datenschutzbewusste Handeln der Mitarbeitenden.

Die praktische Erfahrung zeigt vielmehr, dass Datenschutzverletzungen nicht nur auf technische Defizite, sondern auch auf menschliche Fehlhandlungen zurückzuführen sind. Phishing-Angriffe, Social-Engineering-Methoden, Fehlkonfigurationen oder unbedachte Weitergaben personenbezogener Daten zählen inzwischen zu den häufigsten Ursachen sicherheitsrelevanter Vorfälle. Regelmäßige Schulungen und Sensibilisierungsmaßnahmen werden deshalb zu einem unverzichtbaren Bestandteil eines wirksamen Datenschutz- und Informationssicherheitsmanagements.

Die Reform verdeutlicht zugleich, dass datenschutzrechtliche Verantwortung nicht auf hauptamtlich Beschäftigte beschränkt ist. Wie bereits im novellierten KDG werden auch ehrenamtlich tätige Personen ausdrücklich in die datenschutzrechtlichen Verpflichtungen einbezogen. Damit trägt der Gesetzgeber der besonderen Bedeutung des ehrenamtlichen Engagements innerhalb der katholischen Kirche Rechnung und stellt zugleich klar, dass die Verarbeitung personenbezogener Daten unabhängig von der Art der Tätigkeit die Einhaltung datenschutzrechtlicher Anforderungen voraussetzt. Für kirchliche Einrichtungen bedeutet dies, dass auch Ehrenamtliche angemessen informiert, sensibilisiert und in bestehende Datenschutzkonzepte einbezogen werden müssen.

Darüber hinaus macht die KDG-DVO deutlich, dass Datenschutz und Informationssicherheit zunehmend als Leitungsaufgabe zu verstehen sind. Die Auswahl angemessener technischer und organisatorischer Maßnahmen, die Durchführung von Risikoanalysen, die Organisation von Schulungen sowie die regelmäßige Überprüfung der Wirksamkeit bestehender Schutzmaßnahmen erfordern strategische Entscheidungen und eine kontinuierliche Steuerung innerhalb der Organisation. Datenschutz wird damit zu einer dauerhaften Führungs- und Organisationsaufgabe, die nicht allein auf Datenschutzbeauftragte oder IT-Abteilungen übertragen werden kann.

Die Neufassung der KDG-DVO unterstreicht damit einen grundlegenden Wandel des Datenschutzverständnisses. Neben technischen Lösungen und rechtlichen Vorgaben gewinnen organisatorische Verantwortung, Sicherheitskultur und die kontinuierliche Qualifizierung der Mitarbeitenden zunehmend an Bedeutung. Erst das Zusammenwirken dieser Faktoren ermöglicht einen wirksamen und nachhaltigen Schutz personenbezogener Daten in einer zunehmend digitalisierten Arbeitswelt.

Auswirkungen auf die Praxis und Schlussbetrachtung

Die Novellierung der KDG-DVO führt für kirchliche Stellen zu einem erheblichen Überprüfungs- und Anpassungsbedarf. Bestehende Datenschutz- und Informationssicherheitskonzepte sollten daraufhin überprüft werden, ob sie den weiterentwickelten Anforderungen der Verordnung entsprechen. Dies betrifft insbesondere die Nutzung cloudbasierter Dienste, mobile und hybride Arbeitsformen, Zugriffs- und Berechtigungskonzepte, Verschlüsselungsstrategien, Schulungs- und Sensibilisierungskonzepte sowie die Dokumentation und regelmäßige Überprüfung technischer und organisatorischer Maßnahmen.

Gerade kleinere kirchliche Einrichtungen stehen hierbei vor der Herausforderung, die gestiegenen technischen und organisatorischen Anforderungen mit begrenzten personellen und finanziellen Ressourcen umzusetzen. Gleichzeitig schafft die Neufassung jedoch mehr Orientierung und Rechtssicherheit. Zahlreiche bislang

eher allgemein formulierte Anforderungen werden konkretisiert und an den heutigen Stand der Technik angepasst. Dadurch erhalten Verantwortliche eine verlässlichere Grundlage für die datenschutzgerechte Gestaltung ihrer organisatorischen und technischen Prozesse.

Auch für die kirchliche Datenschutzaufsicht gewinnt die Bewertung technischer und organisatorischer Maßnahmen weiter an Bedeutung. Die novellierte KDG-DVO schafft hierfür präzisere Maßstäbe und erleichtert eine nachvollziehbare und einheitliche Beurteilung des erreichten Datenschutzniveaus. Gleichzeitig stärkt sie die Erwartung an Verantwortliche, Datenschutz und Informationssicherheit dauerhaft als Bestandteil einer verantwortungsvollen Organisations- und Leitungsaufgabe zu verstehen.

> Datenschutz ist Führungsaufgabe. Datenschutzbeauftragte beraten – die Verantwortung verbleibt bei der Leitung.

Die Reform verdeutlicht darüber hinaus eine Entwicklung, die sich inzwischen in zahlreichen europäischen und kirchlichen Rechtsakten wiederfindet. Datenschutz wird zunehmend mit Informationssicherheit, Risikomanagement und organisatorischer Compliance verzahnt. Der Schutz personenbezogener Daten wird nicht mehr allein durch einzelne technische Maßnahmen gewährleistet, sondern durch ein systematisches Zusammenspiel von Risikoanalyse, geeigneten Sicherheitsmaßnahmen, nachvollziehbarer Dokumentation und kontinuierlicher Sensibilisierung der Mitarbeitenden.

> Die KDG-DVO verbindet Datenschutz, Informationssicherheit und Organisationsentwicklung zu einem modernen Managementsystem für kirchliche Einrichtungen.

Insgesamt markiert die Novellierung der KDG-DVO einen wichtigen Schritt hin zu einem modernen und praxisorientierten Datenschutzrecht innerhalb der katholischen Kirche. Sie verbindet die Anforderungen des Datenschutzes mit den Herausforderungen einer zunehmend digitalisierten Arbeits- und Verwaltungswelt und

stärkt zugleich die Informationssicherheit als unverzichtbaren Bestandteil eines wirksamen Datenschutzmanagements. Die KDG-DVO entwickelt sich damit zu einem zentralen Organisationsregelwerk für die datenschutzgerechte Gestaltung kirchlicher Verwaltungs- und IT-Prozesse und leistet einen wesentlichen Beitrag zur weiteren Professionalisierung des Datenschutzes in der katholischen Kirche in Deutschland.

Die Reform des kirchlichen Datenschutzrechts beschränkte sich jedoch nicht auf das KDG und die KDG-DVO. Auch die diözesanen Ausführungsgesetze wurden an die neuen bundesrechtlichen Vorgaben angepasst und fortentwickelt. Die nachfolgende Übersicht zeigt den Stand der Umsetzung in den sieben bayerischen (Erz-)Diözesen.

Diözesane Rechtsentwicklungen 2025 – Überblick

Im Berichtsjahr wurden in mehreren bayerischen (Erz-)Diözesen neue kirchliche Regelungen mit datenschutzrechtlichem Bezug erlassen oder bestehende Vorschriften fortentwickelt. Die Themen lassen sich wie folgt zusammenfassen:

- ☑ **Augsburg:** Bestätigung der betrieblichen Datenschutzbeauftragten sowie Einführung einer Clean-Desk-Policy.
- ☑ **Bamberg:** Neue Geschäftsordnung, Aktenordnung und Vertragsmanagementrichtlinie zur Stärkung von Datenschutz und Informationssicherheit.
- ☑ **Eichstätt:** Gesetzliche Regelung der Akteneinsicht für Ansprechpersonen im Bereich der Aufarbeitung sexualisierter Gewalt.
- ☑ **Regensburg:** Neue Ordnung zu Einsichts- und Auskunftsrechten im Rahmen von Aufarbeitungsprojekten.
- ☑ **Würzburg:** Ordnung zur Führung von Personalakten sowie neues Aufsichtsdekret für private kirchliche Vereine.

2.2.3 Augsburg: Erneute Benennung der bDSB

Mit Dekret vom 1. Januar 2025 (Amtsblatt Nr. 1, 15.01.2025 Seite 21 ff.) wurden für die Diözese Augsburg die drei betrieblichen Datenschutzbeauftragten in ihrem Amt bestätigt und gemäß § 36 KDG für die Dauer von weiteren vier Jahren benannt. Das Dekret konkretisiert ihre unabhängige Stellung, die unmittelbare Berichtslinie an den Generalvikar sowie die Verpflichtung der Dienstgeberin, die Datenschutzbeauftragten umfassend zu unterstützen und frühzeitig in datenschutzrelevante Fragestellungen einzubinden.

2.2.4 Augsburg: Clean-Desk-Policy

Mit Wirkung zum 1. Juni 2025 (Amtsblatt Nr. 12, 09.07.2025 Seite 304 ff.) trat im Bistum Augsburg eine Richtlinie zum Umgang mit personenbezogenen und betrieblichen Daten am Arbeitsplatz („Clean-Desk-Policy“) in Kraft. Ziel der Regelung ist es, insbesondere im Zusammenhang mit Desk-Sharing, Home-Office und mobilem Arbeiten den Schutz sensibler Daten zu stärken und Sicherheitsrisiken durch organisatorische und technische Maßnahmen zu reduzieren. Die Richtlinie enthält verbindliche Vorgaben zur sicheren Aufbewahrung von Unterlagen, zur Absicherung von IT-Arbeitsplätzen sowie zur datenschutzgerechten Gestaltung gemeinschaftlich genutzter Arbeitsplätze.

> Datenschutz beginnt nicht erst in der IT. Auch organisatorische Maßnahmen wie eine Clean-Desk-Policy leisten einen wichtigen Beitrag zum Schutz personenbezogener Daten.

2.2.5 Bamberg: Geschäftsordnung, Aktenordnung und Vertragsmanagementrichtlinie

Das Erzbischöfliches Ordinariat Bamberg hat im Jahr 2025 mit der Einführung einer Geschäftsordnung, einer Aktenordnung sowie einer Vertragsmanagementrichtlinie (Amtsblatt Nr. 11/2025, 02.12.2025, Seite 355 ff.) wichtige Grundlagen für ein moder-

nes, transparentes und rechtskonformes Verwaltungshandeln geschaffen. Solche Regelwerke dienen der klaren Strukturierung von Zuständigkeiten, der Nachvollziehbarkeit von Entscheidungen und der Vereinheitlichung administrativer Abläufe. Gleichzeitig leisten sie einen wesentlichen Beitrag zur Umsetzung von Datenschutz und Informationssicherheit in der kirchlichen Verwaltung.

Die neue Geschäftsordnung regelt insbesondere Aufbauorganisation, Zuständigkeiten, Dienstwege, Schriftgutverwaltung und Archivierung innerhalb des Ordinariats. Hervorgehoben werden dabei Transparenz, nachhaltiges Verwaltungshandeln sowie die Verpflichtung zur Einhaltung rechtlicher Vorgaben. Datenschutz- und informationssicherheitsrelevante Aspekte zeigen sich insbesondere in den Regelungen zur Aktenführung, Nachvollziehbarkeit von Vorgängen, sicheren Verwahrung von Dienstsiegeln sowie zur elektronischen Kommunikation und Archivierung.

Mit der Aktenordnung wurde ein umfassendes Regelwerk für ein strukturiertes analoges und elektronisches Records-Management geschaffen. Die Ordnung definiert Anforderungen an Aktenführung, Dokumentation, Aufbewahrung, Löschung und Archivierung und enthält detaillierte Vorgaben zur Nachvollziehbarkeit von Verwaltungsvorgängen. Besonders hervorzuheben sind die ausdrücklichen Regelungen zur revisionssicheren Speicherung elektronischer Aufzeichnungen, zum Schutz vor unberechtigten Zugriffen sowie zur datenschutzgerechten Löschung personenbezogener Daten nach den Vorgaben des Gesetze über den Kirchlichen Datenschutz (KDG).

Die Vertragsmanagementrichtlinie etabliert schließlich einheitliche Standards für den gesamten Lebenszyklus von Verträgen – von der Vertragsverhandlung bis zur Archivierung. Ziel ist ein rechtskonformes, transparentes und revisionssicheres Vertragswesen. Die Richtlinie sieht zudem die Einführung eines digitalen Vertragsmanagementsystems vor, das die Nachvollziehbarkeit und Kontrolle von Verträgen verbessern soll. Damit einher geht auch ein besserer Überblick über die Vertragverhältnisse mit Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten und mit denen Verträge zur Auftragsverarbeitung abgeschlossen werden

müssen. Datenschutz- und informationssicherheitsrelevante Bezüge ergeben sich insbesondere aus den definierten Rollen- und Berechtigungskonzepten, Dokumentationspflichten sowie den vorgesehenen Compliance- und Prüfmechanismen.

> Geschäftsordnungen, Aktenordnungen und Vertragsmanagement schaffen nicht nur organisatorische Klarheit, sondern bilden zugleich eine wesentliche Grundlage für Datenschutz und Informationssicherheit.

2.2.6 Eichstätt: Gesetz über die Akteneinsicht für die Ansprechpersonen

Zur besseren Unterstützung der Aufarbeitung sexuellen Missbrauchs hat die Diözese Eichstätt ein Gesetz zur Akteneinsicht für die beauftragten Ansprechpersonen erlassen (Pastoralblatt Nr. 4/2025, 07.05.2025, Seite 120 ff.). Die Regelung ermöglicht es den Ansprechpersonen, auf Antrag Einsicht in Personalakten beschuldigter Kleriker oder sonstiger Beschäftigter sowie Zugang zu einschlägigem personenbezogenem Archivgut zu erhalten. Ziel ist eine verbesserte Plausibilitätsprüfung und Aufklärung von Missbrauchsfällen unter Berücksichtigung der datenschutzrechtlichen Rahmenbedingungen durch eine ausdrücklich geregelte Ausnahme von bestehenden Beschränkungen der Personalaktenordnung.

> Eine klare Regelung für die Einsicht in Akten schafft Transparenz und fördert Vertrauen.

2.2.7 Regensburg: Ordnung zur Regelung von Einsichts- und Auskunftsrechten

Mit einer eigenen Ordnung zu Einsichts- und Auskunftsrechten Dritter in Bezug auf Personalaktendaten hat das Bistum Regensburg die rechtlichen Rahmenbedingungen für die Aufarbeitung sexuellen Missbrauchs weiter konkretisiert (Amtsblatt Nr. 5/2025, 16.05.2025, S. 49 ff). Die Regelung ermöglicht unter bestimmten Voraussetzungen die Offenlegung von Personalaktendaten von Klerikern und Kirchenbeamten für Aufarbeitungsprojekte und wissenschaftliche Forschung, wobei zugleich die Vorgaben des Gesetze über den Kirchlichen Datenschutz (KDG), der Kirchlichen

Archivordnung (KAO) sowie der Personalaktenordnung ausdrücklich gewahrt bleiben. Hervorgehoben werden insbesondere Transparenz, unabhängige Aufarbeitung und der Schutz der Persönlichkeitsrechte betroffener Personen.

> Die Aufarbeitung sexualisierter Gewalt erfordert einen sorgfältigen Ausgleich zwischen Transparenz, berechtigtem Informationsinteresse und dem Schutz personenbezogener Daten.

2.2.8 Würzburg: Ordnung über die Führung von Personalakten

Mit der ‚Ordnung über die Führung von Personalakten und den Einsatz automatisierter Verfahren bei der Verarbeitung personenbezogener Daten“ (Diözesanblatt Nr. 3/2025, 25.03.2025, S. 63 ff.) hat das Bistum Würzburg verbindliche Regelungen für den datenschutzkonformen Umgang mit Personalaktendaten geschaffen. Die Ordnung konkretisiert insbesondere Anforderungen an Vertraulichkeit, Zugriffsberechtigungen, Akteneinsicht, Aufbewahrungsfristen sowie den Einsatz elektronischer und hybrider Personalakten unter Beachtung des KDG und der KAO. Hervorgehoben werden zudem technische und organisatorische Schutzmaßnahmen, klare Zuständigkeiten bei der Personalaktenführung sowie die Rechte der Beschäftigten auf Einsicht, Auskunft und datenschutzgerechte Löschung bzw. Archivierung personenbezogener Daten.

> Eine strukturierte Personalaktenführung ist wesentliche Voraussetzung für Vertraulichkeit, Nachvollziehbarkeit und die Wahrung der Rechte der Beschäftigten.

2.2.9 Würzburg: Allgemeines Dekret zur Wahrnehmung der Aufsicht

Mit dem ‚Allgemeinen Dekret zur Wahrnehmung der Aufsicht über die privaten kirchlichen Vereine“ (Diözesanblatt Nr. 12/2025, 19.12.2025, S. 402 ff.) hat das Bistum Würzburg die kirchliche Aufsicht über private kirchliche Vereinigungen neu geregelt und strukturiert. Ziel des Dekrets ist insbesondere die Sicherstellung einer geordneten Vermögensverwaltung, rechtmäßigen Geschäftsführung und transparenten Organisation kirchlicher Vereine innerhalb der Diözese. Aus Sicht des Datenschutzes und der Informationssicherheit sind dabei insbesondere die vorgesehenen Anforderungen an Dokumentation, Nachweisführung, geordnete Verwaltungsprozesse und die Wahrnehmung kirchlicher Aufsichtspflichten von Bedeutung, da diese zugleich die Nachvollziehbarkeit und Kontrolle personenbezogener Datenverarbeitungen in Vereinsstrukturen stärken.

> Auch kirchliche Vereine profitieren von klaren Regelung und der Verpflichtung zum Nachweis im Datenschutz.

Die dargestellten Rechtsentwicklungen verdeutlichen, dass Datenschutz und Informationssicherheit zunehmend auch auf diözesaner Ebene in organisatorische Regelwerke integriert werden. Neben klassischen Datenschutzvorschriften gewinnen insbesondere Regelungen zu Verwaltungsorganisation, Dokumentation, Aktenführung und digitaler Zusammenarbeit an Bedeutung. Die diözesanen Rechtsentwicklungen ergänzen damit das kirchliche Datenschutzrecht um praxisnahe Vorgaben für eine moderne und rechtskonforme Verwaltung.

2.3 Aktuelle Rechtsprechung zum Datenschutzrecht

Im Berichtszeitraum wurde das Datenschutzrecht nicht nur durch gesetzgeberische Maßnahmen und politische Initiativen weiterentwickelt, sondern auch durch die Rechtsprechung der staatlichen und kirchlichen Gerichte maßgeblich konkretisiert. Zahlreiche Entscheidungen haben zur Auslegung zentraler datenschutzrechtlicher Vorschriften beigetragen und wichtige Leitlinien für deren praktische Anwendung entwickelt. Ohne Anspruch auf Vollständigkeit werden nachfolgend ausgewählte Entscheidungen vorgestellt, die aus Sicht des KDSZ Bayern für kirchliche Einrichtungen und deren Datenschutzpraxis von besonderer Bedeutung sind.

Ausgewählte Entscheidungen im Überblick

Die nachfolgenden Entscheidungen verdeutlichen, welche datenschutzrechtlichen Fragestellungen die Gerichte im Berichtszeitraum besonders beschäftigt haben. Schwerpunkte waren insbesondere:

- ☑ **Datenminimierung:** Pflichtangaben in Formularen und digitalen Anwendungen.
- ☑ **Löschung und Aufbewahrung:** Grenzen datenschutzrechtlicher Löschansprüche.
- ☑ **Betroffenenrechte:** Umfang von Auskunfts- und Einsichtsrechten.
- ☑ **Kirchliches Datenschutzrecht:** Anwendungsbereich des KDG und kirchliche Öffentlichkeitsarbeit.
- ☑ **Beschäftigtendatenschutz:** Zulässigkeit technischer Maßnahmen im Arbeitsverhältnis.

2.3.1 Anredeabfrage bei Bahnticketbuchung nicht datenschutzkonform

EuGH | 9. Januar 2025 | Rs. C-394/23

Der Gerichtshof der Europäischen Union hatte über die Frage zu entscheiden, ob die französische Bahngesellschaft SNCF ihre Kunden bei der Buchung von Bahnfahrkarten verpflichtend nach der Anrede („Herr" oder „Frau") fragen darf. Nach Auffassung des EuGH ist die Verarbeitung dieser Information für die Erfüllung des Beförderungsvertrages grundsätzlich nicht erforderlich und kann daher nicht auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO gestützt werden.

Der Gerichtshof betont, dass der Begriff der Erforderlichkeit im Rahmen der Vertragserfüllung eng auszulegen ist. Personenbezogene Daten dürfen auf dieser Rechtsgrundlage nur verarbeitet werden, wenn sie objektiv notwendig sind, um den jeweiligen Vertrag ordnungsgemäß durchführen zu können. Die bloße Ermöglichung einer personalisierten oder höflicheren Kommunikation genügt hierfür nicht.

Darüber hinaus sieht der EuGH einen Verstoß gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO. Verantwortliche dürfen nur diejenigen personenbezogenen Daten erheben, die für den jeweiligen Zweck tatsächlich erforderlich sind.

Die Entscheidung verdeutlicht, dass Verantwortliche die Erforderlichkeit einzelner Datenfelder in Formularen und digitalen Anwendungen kritisch überprüfen sollten. Insbesondere standardmäßig abgefragte personenbezogene Angaben dürfen nicht allein aus Gewohnheit oder zur Verbesserung der Kundenkommunikation erhoben werden, sondern bedürfen einer tragfähigen datenschutzrechtlichen Grundlage.

> **Merksatz:** Nur personenbezogene Daten erheben, die für den jeweiligen Zweck tatsächlich erforderlich sind.

2.3.2 Löschpflicht trotz möglicher Rechtsstreitigkeiten

OLG Karlsruhe | 15. Januar 2025 | 14 U 150/23

Das Oberlandesgericht Karlsruhe hatte sich mit der Frage zu befassen, unter welchen Voraussetzungen personenbezogene Daten trotz eines bestehenden Löschungsanspruchs weiter gespeichert werden dürfen, um sich gegen mögliche zukünftige Rechtsansprüche verteidigen zu können.

Das Gericht stellt klar, dass die Ausnahme vom Löschungsanspruch nach Art. 17 Abs. 3 Buchst. e DSGVO eng auszulegen ist. Eine weitere Speicherung personenbezogener Daten ist nur zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung konkreter Rechtsansprüche erforderlich ist. Die bloß abstrakte Möglichkeit eines zukünftigen Rechtsstreits oder der Umstand, dass Verjährungsfristen noch nicht abgelaufen sind, genügt hierfür grundsätzlich nicht.

Nach Auffassung des OLG Karlsruhe sind personenbezogene Daten daher zu löschen, sobald der ursprüngliche Verarbeitungszweck entfallen ist und keine hinreichend konkrete Wahrscheinlichkeit einer rechtlichen Auseinandersetzung besteht. Verantwortliche müssen im Einzelfall nachvollziehbar begründen können, weshalb eine weitere Speicherung tatsächlich erforderlich ist.

Die Entscheidung verdeutlicht, dass Aufbewahrungsfristen und Löschkonzepte sorgfältig voneinander zu unterscheiden sind. Personenbezogene Daten dürfen nicht vorsorglich über den eigentlichen Verarbeitungszweck hinaus gespeichert werden, nur weil ein späterer Rechtsstreit theoretisch denkbar erscheint. Für kirchliche Einrichtungen unterstreicht das Urteil die Bedeutung eines strukturierten Löschmanagements und einer nachvollziehbaren Dokumentation der jeweiligen Speichergründe.

> **Merksatz:** Die bloße Möglichkeit eines späteren Rechtsstreits rechtfertigt keine längere Speicherung personenbezogener Daten.

2.3.3 Kein Anspruch auf Einsicht in Auftrags-Verarbeitungsverträge

VGH Bayern | 21. Feburar 2025 |, 7 ZB 24.651

Der Bayerische Verwaltungsgerichtshof hatte zu entscheiden, ob eine betroffene Person Einsicht in einen zwischen einem Verantwortlichen und einem Auftragsverarbeiter (AV) geschlossenen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO verlangen kann. Anlass des Verfahrens war das Begehren eines Rundfunkteilnehmers, den zwischen einer Rundfunkanstalt und einem Dienstleister geschlossenen Vertrag einzusehen, um dessen datenschutzrechtliche Wirksamkeit selbst überprüfen zu können.

Der VGH verneinte einen solchen Anspruch. Nach seiner Auffassung begründet Art. 28 DSGVO kein subjektives Recht betroffener Personen auf Einsicht in AVV. Die Vorschrift regelt ausschließlich die datenschutzrechtlichen Anforderungen an das Verhältnis zwischen Verantwortlichem und AV. Die Kontrolle, ob diese Anforderungen eingehalten werden, obliegt den zuständigen Datenschutzaufsichtsbehörden.

Auch aus dem Auskunftsanspruch nach Art. 15 DSGVO ergibt sich kein weitergehendes Einsichtsrecht. Betroffene haben Anspruch auf Auskunft über die Verarbeitung ihrer eigenen personenbezogenen Daten, nicht jedoch auf Offenlegung von Verträgen oder sonstigen Unterlagen, die ihnen eine eigenständige rechtliche Überprüfung der Datenverarbeitung ermöglichen sollen.

> **Merksatz:** Auftragsverarbeitungsverträge unterliegen grundsätzlich nicht dem Auskunftsanspruch betroffener Personen.

Die Entscheidung verdeutlicht die unterschiedliche Aufgabenverteilung innerhalb des Datenschutzrechts. Während betroffene Personen ihre Rechte insbesondere durch Auskunfts-, Berichtigungs-, Löschungs- oder Beschwerderechte wahrnehmen können, ist die Überprüfung der Rechtmäßigkeit von AVV Aufgabe der Datenschutzaufsichtsbehörden. Für Verantwortliche schafft das Urteil Klarheit, dass AVV grundsätzlich nicht gegenüber betroffenen Personen offengelegt werden müssen, sofern hierfür keine andere rechtliche Verpflichtung besteht.

2.3.4 Anwendungsbereich des KDG bei kirchennahen Organisationen

IDSG | 17. September 2025 | 10/2023, Rechtsmittel DSG-DBK | 11/2025

Das Interdiözesane Datenschutzgericht hatte über die Frage zu entscheiden, ob das Kolpingwerk Deutschland dem Anwendungsbereich des Gesetzes über den Kirchlichen Datenschutz (KDG) unterliegt und damit der Aufsicht der kirchlichen Datenschutzaufsicht untersteht. Anlass des Verfahrens war ein Feststellungsbescheid der Datenschutzaufsicht, mit dem die Anwendbarkeit des KDG festgestellt worden war.

Das Gericht bestätigte die Zuständigkeit der kirchlichen Datenschutzaufsicht. Es stellte fest, dass der Antragsteller als ‚sonstiger kirchlicher Rechtsträger" im Sinne des § 3 Abs. 1 Buchst. c KDG einzuordnen ist. Maßgeblich hierfür seien insbesondere die enge organisatorische und institutionelle Verbindung zur Katholischen Kirche, die kirchliche Zielsetzung des Verbandes sowie dessen Einbindung in kirchliche Aufsichts- und Organisationsstrukturen. Hierzu zählen unter anderem die kirchliche Aufsicht über den Verband, die Genehmigung der Satzung und ihrer Änderungen durch die Deutsche Bischofskonferenz sowie die Anwendung der Grundordnung des kirchlichen Dienstes in den Arbeitsverhältnissen.

Besondere Bedeutung kommt der Feststellung des Gerichts zu, dass die Anwendung des KDG nicht davon abhängt, ob sich eine kirchennahe Organisation diesem ausdrücklich unterworfen hat. Nach Auffassung des Gerichts enthält § 3 Abs. 1 Buchst. c KDG keinen Übernahmevorbehalt. Entscheidend sind vielmehr die objektiven Voraussetzungen der organisatorischen Einbindung in die katholische Kirche. Diese Auslegung entspricht nach Auffassung des Gerichts den verfassungs- und unionsrechtlichen Grundlagen des kirchlichen Selbstbestimmungsrechts sowie Art. 91 DSGVO.

Die Entscheidung besitzt über den Einzelfall hinaus erhebliche Bedeutung für die Auslegung des organisatorischen Anwendungsbereichs des KDG. Sie verdeutlicht, dass für die Anwendbarkeit des kirchlichen Datenschutzrechts nicht allein die zivilrechtliche Rechtsform oder eine ausdrückliche Unterwerfungserklärung maßgeb-

lich sind. Entscheidend ist vielmehr, ob eine Organisation nach ihrer Aufgabenstellung und ihrer tatsächlichen organisatorischen Einbindung als kirchlicher Rechtsträger im Sinne des KDG anzusehen ist.

> **Merksatz:** Für die Anwendbarkeit des KDG ist die tatsächliche organisatorische Einbindung in die Kirche entscheidend.

2.3.5 Löschung personenbezogener Daten – Vernichtung einer Caritas-Akte

IDSG | 26. Mai 2025 | 26/2022

Das Interdiözesane Datenschutzgericht hatte über die Frage zu entscheiden, unter welchen Voraussetzungen personenbezogene Daten gelöscht werden müssen und ob die Vernichtung einer Akte trotz eines entsprechenden Löschungsbegehrens datenschutzrechtlich unzulässig sein kann. Gegenstand des Verfahrens war die Aufbewahrung einer Jugendhilfeakte durch einen Caritas-Träger.

Das Gericht stellte klar, dass der Löschungsanspruch nach Art. 17 DSGVO beziehungsweise den entsprechenden Vorschriften des KDG nicht uneingeschränkt besteht. Eine Löschung darf insbesondere dann unterbleiben, wenn die weitere Speicherung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist oder andere gesetzliche Aufbewahrungspflichten entgegenstehen. Im konkreten Fall kam das Gericht zu dem Ergebnis, dass die weitere Aufbewahrung der Unterlagen zulässig war, um die Vollständigkeit und Nachvollziehbarkeit der dokumentierten Vorgänge sicherzustellen und gegebenenfalls spätere rechtliche Auseinandersetzungen auf einer verlässlichen Tatsachengrundlage führen zu können.

Die Entscheidung verdeutlicht, dass datenschutzrechtliche Löschpflichten stets im Zusammenhang mit den jeweiligen Speicherzwecken und gesetzlichen Aufbewahrungspflichten zu beurteilen sind. Datenschutz verlangt nicht nur die rechtzeitige Löschung personenbezogener Daten, sondern ebenso deren rechtmäßige Aufbewahrung, sofern hierfür eine tragfähige Rechtsgrundlage besteht. Für kirchliche

Einrichtungen unterstreicht das Urteil die Bedeutung sorgfältig abgestimmter Lösch- und Aufbewahrungskonzepte sowie einer nachvollziehbaren Dokumentation der jeweiligen Speichergründe.

> **Merksatz:** Datenschutz verlangt nicht nur die Löschung, sondern auch die rechtmäßige Aufbewahrung personenbezogener Daten.

2.3.6 Suche nach Dateien auf einem Dateiserver und Beschäftigtendatenschutz

IDSG | 15. Juni 2025 | 19/2023, Rechtsmittel: DSG-DBK | 10/2025

Das Interdiözesane Datenschutzgericht hatte über die Frage zu entscheiden, ob die Suche einer IT-Abteilung nach einer dienstlich benötigten Datei auf einem Dateiserver eine unzulässige Verarbeitung personenbezogener Daten einer Beschäftigten darstellt. Anlass des Verfahrens war die Beschwerde einer Mitarbeiterin eines kirchlichen Trägers, deren Vorgesetzte die IT-Abteilung beauftragt hatte, eine für den Dienstbetrieb erforderliche Datei zu lokalisieren.

Das Gericht stellte zunächst fest, dass nicht nachgewiesen werden konnte, dass tatsächlich eine Einsichtnahme in den persönlichen Benutzer-Account der Mitarbeiterin erfolgt war. Nach den Feststellungen des Gerichts beschränkte sich die IT-Maßnahme auf eine Suche innerhalb des Dateiservers, um den Speicherort der gesuchten Datei festzustellen. Allein die Information, dass sich die Datei in einem der Mitarbeiterin zugeordneten Ordner befand, stellt zwar eine Verarbeitung personenbezogener Daten dar, diese war jedoch nach § 53 Abs. 1 KDG für Zwecke des Beschäftigungsverhältnisses gerechtfertigt.

Das Gericht betont, dass auch Maßnahmen im Beschäftigungskontext dem Grundsatz der Verhältnismäßigkeit unterliegen. Im konkreten Fall überwog jedoch das berechtigte Interesse des kirchlichen Arbeitgebers, eine für den laufenden Geschäftsbetrieb erforderliche Datei kurzfristig aufzufinden und zu sichern. Demgegenüber war der Eingriff in das Recht auf informationelle Selbstbestimmung der

Beschäftigten lediglich geringfügig, da weder eine inhaltliche Einsichtnahme in die Datei noch eine Durchsuchung ihres Benutzerkontos nachgewiesen werden konnte.

Die Entscheidung verdeutlicht, dass datenschutzrechtlich zwischen einer technischen Suche nach dienstlich erforderlichen Dateien und einer Einsichtnahme in persönliche Benutzerkonten oder deren Inhalte zu unterscheiden ist. Zugleich bestätigt das Gericht, dass personenbezogene Daten von Beschäftigten nach § 53 KDG verarbeitet werden dürfen, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich und verhältnismäßig ist. Für kirchliche Einrichtungen unterstreicht das Urteil die Bedeutung klarer organisatorischer Regelungen für den Umgang mit Dateiservern, Benutzerkonten und IT-Administrationsrechten sowie einer sorgfältigen Dokumentation entsprechender Maßnahmen.

> **Merksatz:** Zwischen der technischen Suche nach einer Datei und der Einsichtnahme in Benutzerinhalte ist datenschutzrechtlich zu unterscheiden.

2.3.7 Kirchliche Öffentlichkeitsarbeit und Datenschutz

DSG-DBK | 19. Mai 2025 | 02/2024

Das Datenschutzgericht der Deutschen Bischofskonferenz hatte über die datenschutzrechtliche Zulässigkeit der Offenlegung personenbezogener Daten von Gemeindemitgliedern an eine rechtlich selbständige Kirchenzeitung zum Zweck der Mitgliederwerbung zu entscheiden. Im Mittelpunkt des Verfahrens stand die Frage, ob eine solche Datenverarbeitung noch der Erfüllung kirchlicher Aufgaben dient und auf eine entsprechende datenschutzrechtliche Rechtsgrundlage gestützt werden kann.

Das Gericht stellt zunächst klar, dass die Herausgabe und Verbreitung einer Kirchenzeitung grundsätzlich Teil des kirchlichen Verkündigungs- und Informationsauftrags sein kann. Auch Maßnahmen der kirchlichen Öffentlichkeitsarbeit können daher datenschutzrechtlich von der Wahrnehmung kirchlicher Aufgaben umfasst sein. Daraus folgt jedoch nicht, dass personenbezogene Daten ohne weitere Prüfung für entsprechende Zwecke verarbeitet werden dürfen.

Vielmehr betont das Gericht, dass die Rechtmäßigkeit der Datenverarbeitung stets anhand der konkreten Umstände des Einzelfalls zu beurteilen ist. Insbesondere sind die jeweils einschlägige Rechtsgrundlage, die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit sowie die schutzwürdigen Interessen der betroffenen Personen zu berücksichtigen. Eine allgemeine Aussage über die Zulässigkeit vergleichbarer Datenverarbeitungen lässt sich daher nicht treffen.

Die Entscheidung verdeutlicht, dass kirchliche Öffentlichkeitsarbeit und Datenschutz keinen Gegensatz darstellen. Auch wenn kirchliche Kommunikations- und Informationsangebote Teil des kirchlichen Sendungsauftrags sein können, bedarf jede Verarbeitung personenbezogener Daten einer eigenständigen datenschutzrechtlichen Prüfung. Für kirchliche Einrichtungen bestätigt das Urteil damit den Grundsatz, dass auch bei der Wahrnehmung originär kirchlicher Aufgaben die Anforderungen des KDG uneingeschränkt zu beachten sind.

> Merksatz: Auch kirchliche Öffentlichkeitsarbeit bedarf stets einer eigenständigen datenschutzrechtlichen Rechtsgrundlage.

Die dargestellten Entscheidungen zeigen, dass sich die datenschutzrechtliche Rechtsprechung zunehmend auf die praktische Anwendung bestehender Regelungen konzentriert. Im Mittelpunkt stehen weniger grundlegend neue Rechtsfragen als vielmehr die Konkretisierung datenschutzrechtlicher Grundprinzipien wie Erforderlichkeit, Verhältnismäßigkeit, Datenminimierung und Rechenschaftspflicht. Für kirchliche Einrichtungen verdeutlichen die Entscheidungen zugleich, dass sowohl die staatliche als auch die kirchliche Rechtsprechung zunehmend vergleichbare Maßstäbe an eine datenschutzkonforme Verarbeitung personenbezogener Daten anlegen.

3 Grundlagen der Datenschutzaufsicht

Mit der Novellierung des Gesetzes über den Kirchlichen Datenschutz (KDG) und dem Inkrafttreten der Neuregelungen zum 1. März 2026 wurden die Aufgaben und Befugnisse der kirchlichen Datenschutzaufsicht weiter präzisiert und teilweise erweitert. Zugleich wurden die Verantwortlichkeiten der Verantwortlichen und der betrieblichen Datenschutzbeauftragten im kirchlichen Datenschutzsystem nochmals deutlicher herausgearbeitet. Die gesetzlichen Änderungen geben daher Anlass, den Schwerpunkt dieses Kapitels gegenüber früheren Tätigkeitsberichten leicht zu verlagern.

Während Tätigkeitsberichte häufig vor allem statistische Angaben oder besonders interessante Einzelfälle aus der Praxis enthalten, verfolgt dieses Kapitel einen weitergehenden Ansatz. Es erläutert die gesetzlichen Aufgaben der Datenschutzaufsicht, die Verantwortung der Verantwortlichen kirchlicher Einrichtungen sowie die Rolle der betrieblichen Datenschutzbeauftragten innerhalb des kirchlichen Datenschutzsystems.

Diese Abgrenzung ist von erheblicher praktischer Bedeutung. In der täglichen Arbeit zeigt sich immer wieder, dass die unterschiedlichen Rollen zwar eng miteinander verbunden sind, ihre jeweiligen Aufgaben jedoch nicht selten miteinander vermischt werden. Datenschutzaufsicht ersetzt weder das Datenschutzmanagement der kirchlichen Einrichtungen noch die Tätigkeit der betrieblichen Datenschutzbeauftragten. Umgekehrt endet die Verantwortung der Verantwortlichen nicht mit der Benennung eines betrieblichen Datenschutzbeauftragten oder der Einbindung der Datenschutzaufsicht. Datenschutz ist und bleibt eine originäre Leitungsaufgabe der Verantwortlichen.

Die Datenschutzaufsicht versteht sich dabei als unabhängige Kontroll- und Beratungsinstanz. Sie überwacht die Einhaltung des kirchlichen Datenschutzrechts und unterstützt kirchliche Einrichtungen durch Beratung, Information und Sensibilisierung bei der datenschutzkonformen Gestaltung ihrer Verfahren. Ihre Aufgabe beschränkt sich dabei nicht auf die nachträgliche Kontrolle einzelner Datenschutzverstöße. Vielmehr trägt sie dazu bei, ein wirksames Datenschutzmanagement zu

fördern, ein einheitliches Verständnis des kirchlichen Datenschutzrechts zu entwickeln und datenschutzrechtliche Risiken möglichst bereits im Vorfeld zu vermeiden.

Das KDSZ Bayern versteht Datenschutzaufsicht daher nicht ausschließlich als klassische Eingriffsverwaltung. Wo immer möglich, setzt es auf Prävention in Form einer frühzeitigen Beratung, vertrauensvolle Zusammenarbeit und einen offenen Dialog mit den Verantwortlichen und den betrieblichen Datenschutzbeauftragten. Eine funktionierende Datenschutzaufsicht misst sich nicht allein an der Zahl ausgesprochener Beanstandungen oder aufsichtsrechtlicher Maßnahmen, sondern ebenso daran, in welchem Umfang sie dazu beiträgt, datenschutzrechtliche Anforderungen verständlich zu vermitteln, Verantwortliche zu unterstützen und dadurch Datenschutzverletzungen bereits im Vorfeld zu verhindern. Beratung und Kontrolle stehen deshalb nicht im Widerspruch, sondern ergänzen sich als gleichwertige Bestandteile einer modernen, risikoorientierten Datenschutzaufsicht.

Die nachfolgenden Abschnitte erläutern die unterschiedlichen Verantwortlichkeiten der am kirchlichen Datenschutz beteiligten Akteure und zeigen auf, wie deren Zusammenwirken einen wirksamen, praxisgerechten und nachhaltig verankerten Datenschutz in den kirchlichen Einrichtungen gewährleistet.

Datenschutz ist ein Zusammenspiel verschiedener Rollen

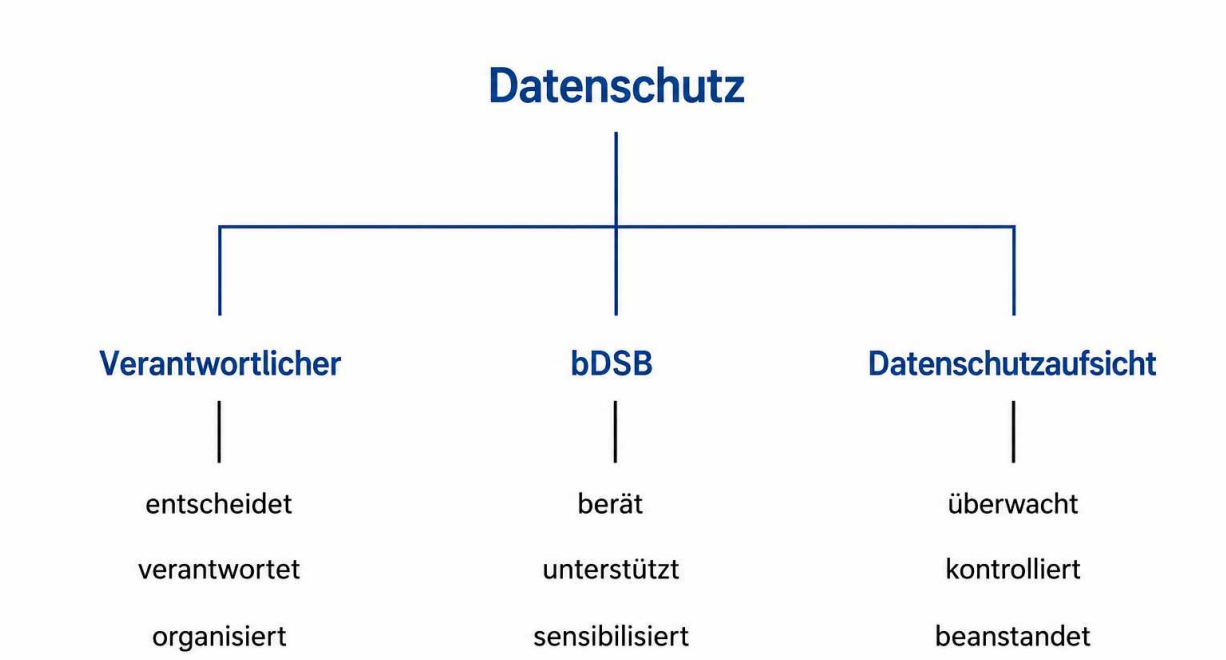
Ein wirksamer Datenschutz setzt das Zusammenwirken mehrerer Akteure voraus. Das KDG weist dabei jedem Beteiligten eine klar definierte Aufgabe zu:

- ☑ Verantwortliche: tragen die Gesamtverantwortung für die Datenschutz-Compliance.
- ☑ Betriebliche Datenschutzbeauftragte: beraten, unterstützen und überwachen innerhalb der Einrichtung.
- ☑ Datenschutzaufsicht: kontrolliert unabhängig die Einhaltung des Datenschutzrechts und unterstützt durch Beratung und Information.

Datenschutz ist eine gemeinsame Aufgabe. Die datenschutzrechtliche Verantwortung verbleibt jedoch stets beim Verantwortlichen.

3.1 Datenschutz ist Führungsaufgabe

Die unterschiedlichen Rollen innerhalb des kirchlichen Datenschutzsystems lassen sich wie folgt darstellen:



Rollen und Verantwortlichkeiten im kirchlichen Datenschutzsystem

3.1.1 Der Verantwortliche als Träger der Datenschutz-Compliance

Das Gesetz über den Kirchlichen Datenschutz weist die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften eindeutig dem Verantwortlichen zu. Verantwortlicher ist die kirchliche Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Mit dieser Entscheidungsbefugnis geht zugleich die Pflicht einher, sämtliche Datenverarbeitungen rechtskonform zu gestalten und die Einhaltung der datenschutzrechtlichen Anforderungen dauerhaft sicherzustellen.

Datenschutz ist deshalb keine isolierte Fachaufgabe einzelner Beschäftigter oder Organisationseinheiten, sondern Bestandteil der Gesamtverantwortung der Leitung einer Einrichtung. Die Verantwortung umfasst sämtliche Bereiche der Datenverarbeitung – von der Einführung neuer IT-Systeme über den Umgang mit Personal- und Patientendaten bis hin zur Veröffentlichung personenbezogener Informationen im Internet oder in sozialen Medien.

Die Einhaltung des Datenschutzrechts ist damit Ausdruck einer wirksamen Datenschutz-Compliance. Sie setzt voraus, dass datenschutzrechtliche Anforderungen frühzeitig in organisatorische Entscheidungen einbezogen und dauerhaft berücksichtigt werden.

> Datenschutz-Compliance ist Aufgabe der Leitung. Verantwortlicher bleibt stets die kirchliche Einrichtung.

3.1.2 Datenschutz ist eine Leitungsaufgabe

Ein wirksamer Datenschutz lässt sich nur verwirklichen, wenn die Leitung einer Einrichtung die hierfür notwendigen organisatorischen, personellen und finanziellen Rahmenbedingungen schafft. Hierzu gehören insbesondere klare Verantwortlichkeiten, geeignete technische und organisatorische Maßnahmen, die Bereitstellung ausreichender Ressourcen und einer direkten Berichts- und Kommunikationslinie, sowie eine kontinuierliche Sensibilisierung der Beschäftigten.

Datenschutz ist daher weder ausschließlich Aufgabe der IT-Abteilung noch der Personalverwaltung oder einzelner Fachbereiche. Vielmehr betrifft er nahezu alle Arbeitsabläufe einer Einrichtung und muss als Bestandteil guter Organisationsführung verstanden werden. Entscheidungen über neue Verfahren, Softwarelösungen oder Digitalisierungsprojekte sind regelmäßig auch Entscheidungen über die Verarbeitung personenbezogener Daten und bedürfen daher einer datenschutzrechtlichen Bewertung.

Gerade im Zuge der fortschreitenden Digitalisierung, der zunehmenden Nutzung cloudbasierter Dienste und des Einsatzes künstlicher Intelligenz gewinnt diese Leitungsverantwortung weiter an Bedeutung. Datenschutz muss bereits bei der Planung neuer Prozesse mitgedacht werden und darf nicht erst nach deren Einführung berücksichtigt werden. In der Praxis haben sich hierfür schriftlich fixierte, schlanke Prozesse beispielsweise für die Beschaffung von Software als besonders hilfreich erwiesen. Hier werden idealerweise alle Stellen benannt, die möglichst früh in einen solchen Prozess eingebunden werden sollten.

> Datenschutz muss bereits bei organisatorischen Entscheidungen berücksichtigt werden – nicht erst nach Einführung neuer Verfahren.

3.1.3 Delegation von Aufgaben bedeutet keine Delegation der Verantwortung

Die praktische Umsetzung datenschutzrechtlicher Anforderungen erfolgt regelmäßig arbeitsteilig. Verantwortliche können Beschäftigte mit einzelnen Aufgaben betrauen, Datenschutzkoordinatoren benennen oder einen internen beziehungsweise externen betrieblichen Datenschutzbeauftragten bestellen. Ebenso werden technische Dienstleistungen häufig auf externe Auftragsverarbeiter übertragen.

Diese organisatorische Arbeitsteilung führt jedoch nicht zu einer Übertragung der datenschutzrechtlichen Gesamtverantwortung. Der Verantwortliche bleibt auch dann dafür verantwortlich, dass die Verarbeitung personenbezogener Daten den gesetzlichen Anforderungen entspricht.

In der Praxis besteht bisweilen die Fehlvorstellung, mit der Bestellung eines betrieblichen Datenschutzbeauftragten gehe zugleich die datenschutzrechtliche Verantwortung auf diesen über. Dies ist nicht der Fall. Der betriebliche Datenschutzbeauftragte berät, unterstützt und überwacht die Einhaltung der datenschutzrechtlichen Vorgaben innerhalb der Einrichtung. Die Entscheidung über die datenschutzkonforme Gestaltung von Verfahren sowie deren Umsetzung verbleibt hingegen bei der Leitung der kirchlichen Stelle.

> Aufgaben können delegiert werden – Verantwortung nicht.

3.1.4 Datenschutzmanagement als dauerhafte Compliance-Aufgabe

Datenschutz erschöpft sich nicht in der Erstellung einzelner Dokumente oder der Erfüllung formaler Nachweispflichten. Vielmehr handelt es sich um einen kontinuierlichen Prozess, der dauerhaft gepflegt und weiterentwickelt werden muss.

Zu einem funktionierenden Datenschutzmanagement gehören unter anderem die Führung des Verzeichnisses von Verarbeitungstätigkeiten, die regelmäßige Überprüfung technischer und organisatorischer Maßnahmen, die Durchführung von Datenschutz-Folgenabschätzungen, die Schulung der Beschäftigten sowie die Einführung von Prozessen zum Umgang mit Betroffenenrechten und Datenschutzverletzungen. Ebenso erforderlich ist eine regelmäßige Überprüfung bestehender Prozesse, um sie an technische, organisatorische und rechtliche Entwicklungen anzupassen. Nicht zuletzt gehören auch die Themen der Gestaltung von Vorgaben für die Aufbewahrung und Löschung, sowie die regelmäßige Kontrolle der datenschutzrechtlichen Vorgaben zum Datenschutzmanagement dazu.

Datenschutz und Informationssicherheit stehen dabei in einem engen Zusammenhang. Während die Informationssicherheit die technischen und organisatorischen Voraussetzungen für einen sicheren Betrieb von IT-Systemen und Datenverarbeitungen schafft, sorgt der Datenschutz dafür, dass personenbezogene Daten rechtmäßig verarbeitet und die Rechte der betroffenen Personen gewahrt werden. Bei-

de Bereiche ergänzen sich und bilden gemeinsam einen wesentlichen Bestandteil einer verantwortungsvollen digitalen Organisationskultur.

Viele Maßnahmen der Informationssicherheit stellen zugleich technische und organisatorische Maßnahmen im Sinne des Datenschutzrechts dar. Hierzu gehören beispielsweise die Absicherung von Benutzerkonten durch eine verpflichtende Mehrfaktor-Authentifizierung, wirksame Berechtigungskonzepte, die Verschlüsselung personenbezogener Daten oder Maßnahmen zur Protokollierung und Zugriffskontrolle. Eine enge Verzahnung von Datenschutz und Informationssicherheit trägt daher wesentlich dazu bei, Risiken für personenbezogene Daten zu minimieren und den gesetzlichen Anforderungen des KDG dauerhaft gerecht zu werden.

> Datenschutz ist kein Projekt, sondern ein kontinuierlicher Organisationsprozess.

3.1.5 Die Rolle der Datenschutzaufsicht

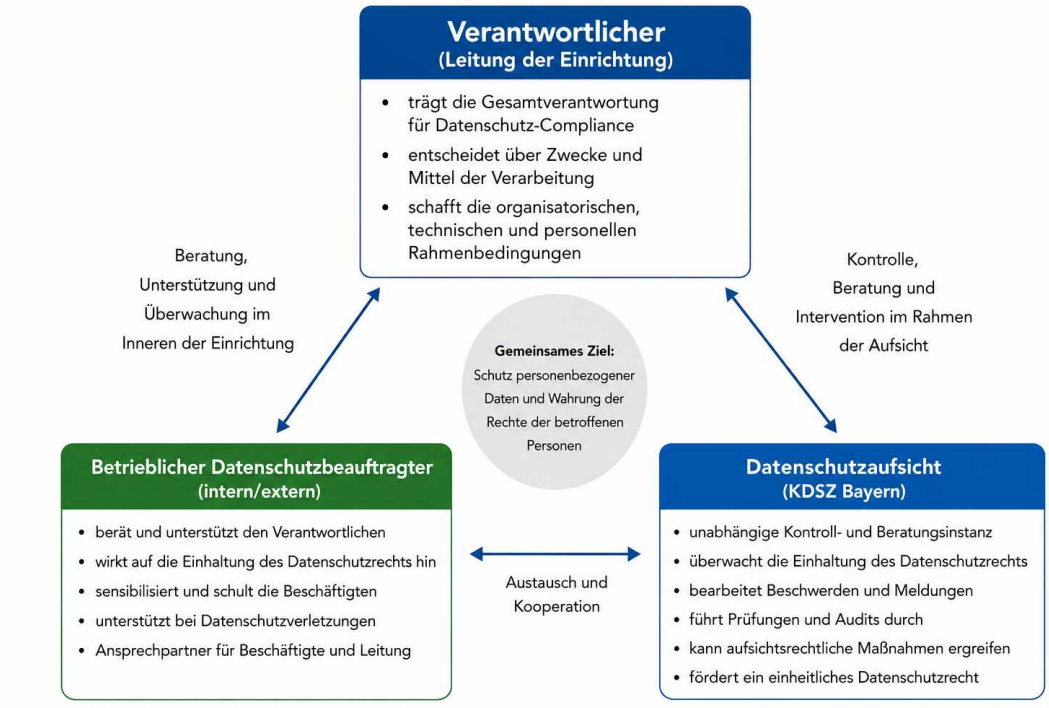
Die gesetzliche Verantwortung der Verantwortlichen bildet zugleich den Ausgangspunkt für die Tätigkeit der Datenschutzaufsicht. Diese übernimmt weder die Aufgaben des Verantwortlichen noch ersetzt sie das interne Datenschutzmanagement oder den betrieblichen Datenschutzbeauftragten.

Ihre Aufgabe besteht vielmehr darin, die Einhaltung des Datenschutzrechts unabhängig zu überwachen und dort beratend oder aufsichtlich tätig zu werden, wo dies gesetzlich vorgesehen ist. Die Datenschutzaufsicht ist deshalb Teil des datenschutzrechtlichen Kontrollsystems, nicht jedoch Teil der Organisationsstruktur der jeweiligen Einrichtung.

Die klare Trennung dieser Verantwortungsbereiche ist Voraussetzung für ein funktionierendes Datenschutzsystem. Verantwortliche, betriebliche Datenschutzbeauftragte und Datenschutzaufsicht verfolgen dasselbe Ziel – den Schutz personenbezogener Daten –, nehmen dabei jedoch unterschiedliche gesetzliche Aufgaben wahr. Erst das Zusammenspiel dieser verschiedenen Rollen gewährleistet einen wirksamen und nachhaltigen Datenschutz in den kirchlichen Einrichtungen.

> Datenschutzaufsicht kontrolliert und berät – sie übernimmt nicht die Verantwortung der Einrichtung.

Die klare Zuordnung der Verantwortlichkeiten bildet die Grundlage für ein wirksames Datenschutzmanagement und zugleich den Ausgangspunkt für die praktische Tätigkeit der Datenschutzaufsicht, die in den folgenden Abschnitten anhand ausgewählter Beispiele dargestellt wird.



Zusammenspiel der Aufgaben und Rollen

3.2 Der betriebliche Datenschutzbeauftragte

3.2.1 Beratung innerhalb der Einrichtung

Der betriebliche Datenschutzbeauftragte nimmt innerhalb der kirchlichen Einrichtung eine zentrale Beratungsfunktion wahr. Er unterstützt den Verantwortlichen sowie die einzelnen Fachbereiche bei allen datenschutzrechtlichen Fragestellungen und begleitet die Einrichtung bei der Umsetzung der gesetzlichen Anforderungen des KDG.

Bereits bei der Planung neuer Verfahren, der Einführung neuer Software oder organisatorischer Veränderungen sollte der betriebliche Datenschutzbeauftragte frühzeitig eingebunden werden. Seine Aufgabe besteht darin, datenschutzrechtliche Risiken zu erkennen, Lösungsmöglichkeiten aufzuzeigen und den Verantwortlichen bei datenschutzkonformen Entscheidungen zu unterstützen.

Der betriebliche Datenschutzbeauftragte kann sowohl aus dem Kreis der Beschäftigten der Einrichtung als auch als externer Dienstleister bestellt werden. Unabhängig von der gewählten Organisationsform begleitet er die Einrichtung kontinuierlich bei der Umsetzung des Datenschutzrechts. Er verschafft sich einen Überblick über die internen Abläufe, die Organisationsstruktur sowie die jeweiligen Verarbeitungsvorgänge und kann dadurch datenschutzrechtliche Fragestellungen frühzeitig erkennen und praxisgerechte Lösungen entwickeln.

> Der betriebliche Datenschutzbeauftragte ist der erste datenschutzrechtliche Ansprechpartner innerhalb der Einrichtung. Seine frühzeitige Einbindung hilft, datenschutzrechtliche Risiken bereits bei der Planung neuer Verfahren zu erkennen und geeignete Lösungen zu entwickeln.

3.2.2 Begleitung des Datenschutzmanagements

Zu den gesetzlichen Aufgaben des betrieblichen Datenschutzbeauftragten gehört es, den Verantwortlichen beim Aufbau und der Weiterentwicklung eines wirksamen Datenschutzmanagements zu unterstützen. Hierzu zählen unter anderem die Mitwirkung bei der Erstellung und Pflege von Verzeichnissen von Verarbeitungstätigkeiten, die Begleitung neuer Verarbeitungsvorgänge sowie die Beratung bei Datenschutz-Folgenabschätzungen und technischen oder organisatorischen Maßnahmen.

Der betriebliche Datenschutzbeauftragte wirkt darauf hin, dass datenschutzrechtliche Anforderungen nicht isoliert betrachtet, sondern als Bestandteil der täglichen Arbeitsabläufe verstanden werden. Datenschutz wird dadurch zu einem kontinuierlichen Prozess innerhalb der Organisation und nicht erst dann relevant, wenn Beschwerden oder Datenschutzverletzungen auftreten.

> Datenschutzmanagement ist eine Daueraufgabe. Der betriebliche Datenschutzbeauftragte begleitet diesen Prozess kontinuierlich und unterstützt den Verantwortlichen bei seiner Weiterentwicklung.

3.2.3 Sensibilisierung und Hinwirken auf die Einhaltung des Datenschutzrechts

Ein wesentlicher Bestandteil der Tätigkeit des betrieblichen Datenschutzbeauftragten ist die Sensibilisierung der Beschäftigten. Datenschutz kann dauerhaft nur gelingen, wenn die Mitarbeitenden die rechtlichen Anforderungen kennen und diese im Arbeitsalltag berücksichtigen. Regelmäßige Schulungen, Informationsangebote und individuelle Beratung tragen wesentlich dazu bei, Datenschutzverletzungen bereits im Vorfeld zu vermeiden, oder diese im Fall der Fälle zuverlässig zu erkennen und Risiken zu begrenzen.

Darüber hinaus wirkt der betriebliche Datenschutzbeauftragte entsprechend seinem gesetzlichen Auftrag auf die Einhaltung der datenschutzrechtlichen Vorschriften innerhalb der Einrichtung hin. Er überprüft bestehende Prozesse, weist auf Ver-

besserungsmöglichkeiten hin und begleitet die Umsetzung datenschutzrechtlicher Anforderungen. Seine Tätigkeit ist dabei beratend und unterstützend ausgestaltet; die Verantwortung für die Umsetzung verbleibt beim Verantwortlichen.

Ebenso unterstützt der betriebliche Datenschutzbeauftragte die Einrichtung bei der Erkennung und Bearbeitung von Datenschutzverletzungen, etwa durch die datenschutzrechtliche Bewertung des Vorfalls oder die Vorbereitung erforderlicher Maßnahmen und Meldungen.

> Wirksamer Datenschutz entsteht nicht allein durch technische Maßnahmen, sondern vor allem durch gut informierte und sensibilisierte Beschäftigte.

3.2.4 Ansprechpartner innerhalb der Einrichtung

Der betriebliche Datenschutzbeauftragte ist regelmäßig die erste Anlaufstelle für datenschutzrechtliche Fragen innerhalb der Einrichtung. Beschäftigte, Führungskräfte und Verantwortliche können sich mit datenschutzrechtlichen Anliegen unmittelbar an ihn wenden. Durch seine unabhängige fachliche Stellung innerhalb der Organisation trägt er dazu bei, datenschutzrechtliche Fragestellungen frühzeitig zu erkennen und einer sachgerechten Lösung zuzuführen.

Zugleich bildet er eine wichtige Schnittstelle zwischen den verschiedenen Fachbereichen und der Leitung. Er vermittelt datenschutzrechtliche Anforderungen in einer für die Praxis verständlichen Weise und unterstützt dabei, rechtliche Vorgaben mit den organisatorischen Bedürfnissen der Einrichtung in Einklang zu bringen.

> Kurze Kommunikationswege fördern einen wirksamen Datenschutz. Der betriebliche Datenschutzbeauftragte verbindet rechtliche Anforderungen mit den praktischen Abläufen der Einrichtung.

3.2.5 Abgrenzung zur Datenschutzaufsicht

Die Aufgaben des betrieblichen Datenschutzbeauftragten unterscheiden sich grundlegend von denen der Datenschutzaufsicht. Während der betriebliche Datenschutzbeauftragte innerhalb der Einrichtung tätig wird und den Verantwortlichen bei der Erfüllung seiner gesetzlichen Pflichten unterstützt, nimmt die Datenschutzaufsicht ihre Aufgaben unabhängig von der jeweiligen Organisation wahr.

Der betriebliche Datenschutzbeauftragte berät, begleitet und unterstützt. Er trifft jedoch keine Entscheidungen anstelle des Verantwortlichen und übt keine hoheitliche Aufsicht über die Einrichtung aus. Zu seinen Aufgaben gehört es jedoch, sich regelmäßig ein Bild vom Stand des Datenschutzmanagements zu verschaffen und auf die Einhaltung der datenschutzrechtlichen Vorgaben hinzuwirken. Hierzu kann und soll er interne Bestandsaufnahmen, Kontrollen oder Audits durchführen sowie die Umsetzung seiner Empfehlungen überprüfen. Diese Prüfungen dienen der kontinuierlichen Verbesserung der Datenschutzorganisation und sind Ausdruck seiner beratenden und überwachenden Funktion innerhalb der Einrichtung.

Ebenso wenig übernimmt die Datenschutzaufsicht die Aufgaben des betrieblichen Datenschutzbeauftragten oder das interne Datenschutzmanagement einer Einrichtung. Gleichwohl stehen betrieblicher Datenschutzbeauftragter und Datenschutzaufsicht in einem engen fachlichen Austausch. Nach § 38 Buchst. e KDG ist der betriebliche Datenschutzbeauftragte verpflichtet, mit der Datenschutzaufsicht zusammenzuarbeiten. Umgekehrt gehört es zu den gesetzlichen Aufgaben der Datenschutzaufsicht, Verantwortliche und betriebliche Datenschutzbeauftragte zu beraten (§ 44 KDG). Der betriebliche Datenschutzbeauftragte kann sich daher bei grundsätzlichen oder besonders komplexen datenschutzrechtlichen Fragestellungen jederzeit an die Datenschutzaufsicht wenden und deren fachliche Einschätzung einholen.

Beide Funktionen ergänzen sich vielmehr in einem abgestimmten Datenschutzsystem. Der betriebliche Datenschutzbeauftragte trägt dazu bei, Datenschutz innerhalb der Organisation wirksam umzusetzen und fortzuentwickeln.

Die Datenschutzaufsicht überprüft demgegenüber unabhängig, ob die gesetzlichen Anforderungen eingehalten werden, und wird insbesondere im Rahmen von Beschwerden, Meldungen von Datenschutzverletzungen, Prüfungen oder sonstigen aufsichtsrechtlichen Verfahren tätig.

Gerade dieses Zusammenspiel von Verantwortlichem, betrieblichem Datenschutzbeauftragtem und unabhängiger Datenschutzaufsicht gewährleistet einen wirksamen Schutz personenbezogener Daten und bildet das Fundament eines funktionierenden kirchlichen Datenschutzsystems.

> Der betriebliche Datenschutzbeauftragte berät und unterstützt die Einrichtung und begleitet deren Datenschutzmanagement durch regelmäßige interne Prüfungen. Die Datenschutzaufsicht überwacht unabhängig die Einhaltung des Datenschutzrechts. Beide Funktionen ergänzen sich, ersetzen sich jedoch nicht.

Während der betriebliche Datenschutzbeauftragte innerhalb der Einrichtung tätig wird und den Verantwortlichen unterstützt, nimmt die Datenschutzaufsicht ihre Aufgaben unabhängig von der jeweiligen Organisation wahr. Deren Aufgaben und Befugnisse werden im folgenden Abschnitt dargestellt.

3.3 Die Datenschutzaufsicht – unabhängige Kontroll- und Beratungsinstanz

3.3.1 Die Datenschutzaufsicht als unabhängige Behörde

Mit dem sechsten Kapitel des Gesetzes über den Kirchlichen Datenschutz (KDG) hat der kirchliche Gesetzgeber die Stellung, Aufgaben und Befugnisse der Datenschutzaufsicht umfassend geregelt und durch die Novellierung zum 1. März 2026 weiter präzisiert. Die Datenschutzaufsicht ist danach eine unabhängige kirchliche Behörde, deren Aufgabe es ist, die Einhaltung des kirchlichen Datenschutzrechts zu überwachen und dessen wirksame Anwendung sicherzustellen.

Die gesetzlich garantierte Unabhängigkeit bildet dabei die wesentliche Voraussetzung für eine wirksame Datenschutzaufsicht.

Diese Unabhängigkeit ist nicht nur eine organisationsrechtliche Entscheidung des kirchlichen Gesetzgebers. Sie ist zugleich Voraussetzung dafür, dass das kirchliche Datenschutzrecht den Anforderungen des Art. 91 Abs. 2 DSGVO entspricht. Danach dürfen Kirchen und Religionsgemeinschaften eigene Datenschutzvorschriften anwenden, sofern deren Einhaltung durch eine unabhängige Datenschutzaufsichtsbehörde überwacht wird. Mit den §§ 42 ff. KDG setzt die katholische Kirche diese unionsrechtliche Vorgabe um und gewährleistet eine von den beaufsichtigten Einrichtungen unabhängige Datenschutzaufsicht.

Sie gewährleistet, dass Entscheidungen ausschließlich auf Grundlage des geltenden Rechts getroffen werden und frei von fachlichen oder organisatorischen Weisungen der beaufsichtigten Einrichtungen erfolgen. Datenschutzaufsicht ist daher weder Teil der Leitung einer kirchlichen Einrichtung noch Bestandteil ihrer Verwaltungsorganisation. Sie übt ihre Aufgaben eigenständig und ausschließlich im Interesse der rechtmäßigen Verarbeitung personenbezogener Daten sowie des Schutzes der Rechte der betroffenen Personen aus.

Das KDSZ Bayern nimmt diese Aufgabe als spezifische Datenschutzaufsicht für die sieben bayerischen (Erz-)Diözesen wahr. Es ist damit keine interne Beratungsstelle, sondern eine unabhängige kirchliche Aufsichtsbehörde im Sinne des Art. 91 Abs. 2 DSGVO. Seine Stellung wird zusätzlich dadurch unterstrichen, dass ihm der Rechtsstatus einer Körperschaft des öffentlichen Rechts verliehen wurde. Als eigenständige juristische Person des öffentlichen Rechts arbeitet das KDSZ Bayern im Rahmen seiner gesetzlichen Aufgaben auch mit den staatlichen Datenschutzaufsichtsbehörden sowie den Gerichten zusammen.

Gerade hierin unterscheidet sich die Datenschutzaufsicht grundlegend vom betrieblichen Datenschutzbeauftragten. Während dieser innerhalb der Einrichtung tätig wird und den Verantwortlichen bei der Erfüllung seiner gesetzlichen Pflichten berät und unterstützt, handelt die Datenschutzaufsicht außerhalb der Organisation. Sie begleitet nicht die laufenden Entscheidungen des Verantwortlichen, son-

dern überprüft unabhängig, ob die gesetzlichen Anforderungen eingehalten werden und ob die Rechte der betroffenen Personen wirksam gewahrt sind.

In der Praxis begegnet der Datenschutzaufsicht dennoch häufig die Vorstellung, sie sei gewissermaßen der ‚Datenschutzbeauftragte aller kirchlichen Einrichtungen". Dieses Verständnis greift zu kurz und entspricht weder der gesetzlichen Systematik noch dem Zweck der Datenschutzaufsicht. Die Verantwortung für die datenschutzkonforme Gestaltung der Datenverarbeitung verbleibt stets beim Verantwortlichen. Der betriebliche Datenschutzbeauftragte unterstützt ihn hierbei innerhalb der Organisation. Die Datenschutzaufsicht übernimmt demgegenüber weder operative Aufgaben des Datenschutzmanagements noch trifft sie Entscheidungen anstelle der Verantwortlichen. So wird das KDSZ Bayern beispielsweise auch keine bestimmte Software ‚freigeben", da eine Entscheidung für oder gegen einen Einsatz immer beim Verantwortlichen liegt. Es ist vielmehr unabhängige Kontroll- und Beratungsinstanz und damit wesentlicher Bestandteil des kirchlichen Datenschutzsystems.

Gerade diese klare Trennung der Verantwortlichkeiten gewährleistet ein ausgewogenes System gegenseitiger Ergänzung und Kontrolle. Verantwortliche, betriebliche Datenschutzbeauftragte und Datenschutzaufsicht verfolgen dasselbe Ziel – den wirksamen Schutz personenbezogener Daten –, erfüllen dieses Ziel jedoch mit unterschiedlichen gesetzlichen Aufgaben und Verantwortlichkeiten.

> Die Unabhängigkeit der Datenschutzaufsicht ist keine organisatorische Besonderheit, sondern gesetzliche Voraussetzung für die Anwendung des kirchlichen Datenschutzrechts nach Art. 91 Abs. 2 DSGVO.

3.3.2 Gesetzlicher Auftrag der Datenschutzaufsicht

Der gesetzliche Auftrag der Datenschutzaufsicht ergibt sich unmittelbar aus § 44 KDG. Danach beschränkt sich ihre Tätigkeit nicht auf die Bearbeitung von Beschwerden oder die Durchführung von Prüfungen. Vielmehr weist das Gesetz der Datenschutzaufsicht ein breites Spektrum an Aufgaben zu, das von Beratung und

Information bis hin zur unabhängigen Kontrolle und Durchsetzung des Datenschutzrechts reicht.

Zu den Kernaufgaben gehört zunächst die Überwachung und Durchsetzung des kirchlichen Datenschutzrechts. Die Datenschutzaufsicht prüft, ob Verantwortliche und Auftragsverarbeiter die gesetzlichen Anforderungen des KDG einhalten, bewertet datenschutzrechtliche Risiken und wirkt darauf hin, festgestellte Defizite zu beseitigen. Dabei steht nicht allein die Reaktion auf Datenschutzverstöße im Mittelpunkt. Ebenso wichtig ist es, datenschutzrechtliche Risiken frühzeitig zu erkennen und gemeinsam mit den Verantwortlichen tragfähige Lösungen zu entwickeln.

Daneben weist das Gesetz der Datenschutzaufsicht ausdrücklich umfangreiche Beratungsaufgaben zu. Sie unterstützt Verantwortliche und Auftragsverarbeiter bei der Auslegung und Anwendung des Datenschutzrechts, beantwortet Grundsatzfragen und entwickelt Orientierungshilfen für die Praxis. Hinzu kommen Informations- und Sensibilisierungsmaßnahmen, durch die das Datenschutzbewusstsein innerhalb der kirchlichen Einrichtungen gestärkt und eine datenschutzgerechte Organisationskultur gefördert werden soll.

Der gesetzliche Auftrag umfasst darüber hinaus die Beobachtung technischer Entwicklungen und neuer Formen der Datenverarbeitung. Digitalisierung, cloudbasierte Dienste und der zunehmende Einsatz künstlicher Intelligenz verändern die Verarbeitung personenbezogener Daten in nahezu allen kirchlichen Arbeitsbereichen. Aufgabe der Datenschutzaufsicht ist es daher auch, diese Entwicklungen kontinuierlich zu begleiten, ihre datenschutzrechtlichen Auswirkungen zu bewerten und den kirchlichen Einrichtungen geeignete Orientierung für einen rechtskonformen und verantwortungsvollen Einsatz neuer Technologien zu geben.

Schließlich dient die Tätigkeit der Datenschutzaufsicht der Förderung einer möglichst einheitlichen Anwendung des kirchlichen Datenschutzrechts. Durch Beratung, Veröffentlichungen, Prüfungen sowie den Austausch mit den anderen kirchlichen und staatlichen Datenschutzaufsichten trägt sie dazu bei, dass vergleichbare

Sachverhalte nach einheitlichen Maßstäben bewertet werden und die Einrichtungen Rechtssicherheit bei der Anwendung des KDG erhalten.

Der gesetzliche Auftrag der Datenschutzaufsicht zeigt damit deutlich, dass Kontrolle und Beratung keine Gegensätze darstellen. Beide Aufgaben sind vielmehr gleichrangige Bestandteile einer modernen Datenschutzaufsicht. Während die Kontrolle die wirksame Durchsetzung des Datenschutzrechts gewährleistet, schafft die Beratung die Voraussetzungen dafür, datenschutzrechtliche Anforderungen frühzeitig zu erkennen und rechtskonforme Lösungen bereits vor ihrer Umsetzung zu entwickeln. Eine wirksame Datenschutzaufsicht zeichnet sich daher nicht allein durch ihre Eingriffsbefugnisse aus, sondern ebenso durch ihre Fähigkeit, Verantwortliche und betriebliche Datenschutzbeauftragte bei der datenschutzgerechten Gestaltung ihrer Verfahren kompetent und verlässlich zu unterstützen.

> Moderne Datenschutzaufsicht verbindet Kontrolle, Beratung, Information und Sensibilisierung. Diese Aufgaben ergänzen sich und dienen gemeinsam einer wirksamen Durchsetzung des Datenschutzrechts.

3.3.3 Ansprechpartner für Betroffene

Die Datenschutzaufsicht ist nicht nur Ansprechpartnerin für Verantwortliche und betriebliche Datenschutzbeauftragte, sondern in besonderem Maße auch für die von einer Datenverarbeitung betroffenen Personen. Sie gewährleistet, dass Betroffene ihre datenschutzrechtlichen Anliegen unabhängig von der verantwortlichen Einrichtung vorbringen können und ihre Rechte wirksam geschützt und durchgesetzt werden.

Zu den gesetzlichen Aufgaben der Datenschutzaufsicht gehört insbesondere die Bearbeitung von Beschwerden betroffener Personen. Diese können sich an die Datenschutzaufsicht wenden, wenn sie der Auffassung sind, dass die Verarbeitung ihrer personenbezogenen Daten gegen die Bestimmungen des KDG verstößt oder ihre Betroffenenrechte nicht ausreichend berücksichtigt wurden. Die Datenschutz-

aufsicht prüft den vorgetragenen Sachverhalt unabhängig und entscheidet, ob und welche aufsichtsrechtlichen Maßnahmen erforderlich sind.

Die Bearbeitung einer Beschwerde beschränkt sich dabei regelmäßig nicht auf eine rein rechtliche Bewertung. In vielen Fällen können bereits durch einen frühzeitigen Dialog zwischen den Beteiligten Missverständnisse ausgeräumt und datenschutzgerechte Lösungen entwickelt werden. Die Datenschutzaufsicht übernimmt hierbei eine vermittelnde Funktion zwischen den Interessen der betroffenen Person und den Pflichten des Verantwortlichen, ohne dabei ihre Neutralität und Unabhängigkeit aufzugeben.

Darüber hinaus unterstützt die Datenschutzaufsicht betroffene Personen bei der Wahrnehmung ihrer gesetzlich garantierten Rechte. Hierzu gehören insbesondere das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch gegen eine Datenverarbeitung. Ziel ist es, den wirksamen Schutz der Persönlichkeitsrechte sicherzustellen und das Vertrauen der Menschen in einen verantwortungsvollen Umgang mit ihren personenbezogenen Daten zu stärken.

Die Wahrung der Rechte natürlicher Personen bildet damit den eigentlichen Maßstab der datenschutzaufsichtlichen Tätigkeit. Sämtliche gesetzlichen Aufgaben – von der Beratung bis zum Erlass aufsichtsrechtlicher Maßnahmen – dienen letztlich diesem Zweck.

> Die Datenschutzaufsicht schützt nicht nur personenbezogene Daten, sondern vor allem die Rechte der betroffenen Personen.

3.3.4 Aufsicht über Verantwortliche und Auftragsverarbeiter

Neben ihrer Beratungs- und Vermittlungstätigkeit obliegt der Datenschutzaufsicht die unabhängige Kontrolle der Verantwortlichen und Auftragsverarbeiter. Diese Kontrollfunktion ist wesentlicher Bestandteil eines wirksamen Datenschutzsystems und dient der Überprüfung, ob die Anforderungen des KDG in der Praxis eingehalten werden.

Ein Schwerpunkt der Aufsichtstätigkeit liegt in der Prüfung gemeldeter Datenschutzverletzungen. Verantwortliche sind verpflichtet, Verletzungen des Schutzes personenbezogener Daten unter den gesetzlichen Voraussetzungen der Datenschutzaufsicht zu melden. Die Datenschutzaufsicht bewertet diese Meldungen, prüft die getroffenen Abhilfemaßnahmen und entscheidet, ob weitere Maßnahmen erforderlich sind. Dabei steht nicht allein die Bewertung des eingetretenen Vorfalls im Mittelpunkt, sondern insbesondere die Frage, wie vergleichbare Ereignisse künftig vermieden werden können.

Darüber hinaus führt die Datenschutzaufsicht anlassbezogene Prüfverfahren sowie planmäßige Vor-Ort-Prüfungen und Audits durch. Anlassbezogene Prüfungen ergeben sich beispielsweise aus Beschwerden, gemeldeten Datenschutzverletzungen oder sonstigen Erkenntnissen der Datenschutzaufsicht. Ergänzend hierzu dienen regelmäßige Audits dazu, datenschutzrechtliche Strukturen und Prozesse unabhängig zu bewerten sowie Verbesserungspotenziale frühzeitig zu identifizieren.

Aufsicht endet dabei nicht mit der Feststellung eines Mangels. Soweit erforderlich, überprüft die Datenschutzaufsicht im Rahmen von Nachkontrollen, ob vereinbarte oder angeordnete Maßnahmen umgesetzt wurden und die festgestellten Defizite dauerhaft behoben sind. Ziel ist eine nachhaltige Verbesserung des Datenschutzes in den kirchlichen Einrichtungen.

Die praktische Umsetzung dieser unterschiedlichen Prüfungsformen sowie die im Berichtsjahr gewonnenen Erfahrungen werden in den folgenden Kapiteln dieses Tätigkeitsberichts anhand ausgewählter Beispiele näher dargestellt.

> Prüfungen dienen nicht allein der Feststellung von Mängeln. Ziel ist die nachhaltige Verbesserung des Datenschutzes innerhalb der kirchlichen Einrichtungen.

3.3.5 Aufsichtsrechtliche Befugnisse

Damit die Datenschutzaufsicht ihren gesetzlichen Auftrag wirksam erfüllen kann, räumt ihr § 47 KDG umfassende Untersuchungs- und Abhilfebefugnisse ein. Diese reichen von der Einholung von Auskünften und der Einsichtnahme in Unterlagen und Systeme zur Datenverarbeitung über Prüfungen vor Ort bis hin zum Erlass aufsichtsrechtlicher Maßnahmen gegenüber Verantwortlichen und Auftragsverarbeitern.

Zu den gesetzlichen Befugnissen gehören insbesondere Auskunftsverlangen, Einsichts- und Prüfungsrechte, Beanstandungen, Verwarnungen sowie Anordnungen zur Herstellung eines datenschutzkonformen Zustands. In besonders gelagerten Fällen kann die Datenschutzaufsicht auch einzelne Verarbeitungsvorgänge ganz oder teilweise untersagen oder – soweit die gesetzlichen Voraussetzungen vorliegen – Geldbußen verhängen. Die Ausübung dieser Befugnisse erfolgt stets auf Grundlage des Verhältnismäßigkeitsgrundsatzes und unter Berücksichtigung der Besonderheiten des jeweiligen Einzelfalls.

Aufsichtsrechtliche Maßnahmen stellen dabei keinen Selbstzweck dar. Sie dienen nicht dazu, Verantwortliche zu sanktionieren oder Fehler zu bestrafen. Ihr Ziel besteht vielmehr darin, rechtswidrige Zustände zu beseitigen, künftige Datenschutzverstöße zu verhindern und die Rechte der betroffenen Personen wirksam zu schützen.

Aus diesem Grund orientiert sich die Datenschutzaufsicht bei der Auswahl ihrer Maßnahmen an einem abgestuften Vorgehen. Wo eine datenschutzkonforme Lösung durch Beratung, Hinweise oder freiwillige Abhilfemaßnahmen erreicht werden kann, haben diese regelmäßig Vorrang. Erst wenn erhebliche oder fortdauernde Verstöße dies erfordern oder Verantwortliche ihren gesetzlichen Pflichten nicht nachkommen, werden weitergehende aufsichtsrechtliche Maßnahmen erforderlich.

Dieses risikoorientierte und verhältnismäßige Vorgehen entspricht dem gesetzlichen Leitbild einer modernen Datenschutzaufsicht. Es verbindet die konsequente Durchsetzung des Datenschutzrechts mit dem Ziel, Verantwortliche bei der nachhaltigen Verbesserung ihres Datenschutzmanagements zu unterstützen und dadurch den Schutz personenbezogener Daten dauerhaft zu stärken.

> Aufsichtsrechtliche Maßnahmen sind kein Selbstzweck. Sie dienen dazu, rechtswidrige Zustände zu beseitigen und den Schutz personenbezogener Daten dauerhaft zu gewährleisten.

3.3.6 Beratung und Kooperation als Leitbild moderner Datenschutzaufsicht

Die gesetzlichen Aufgaben der Datenschutzaufsicht beschränken sich nicht auf die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften. Ebenso versteht das KDSZ Bayern seine Tätigkeit nicht ausschließlich als reaktive Aufsicht über bereits eingetretene Datenschutzverstöße. Vielmehr verfolgt es das Ziel, Datenschutz bereits im Vorfeld wirksam zu gestalten und die kirchlichen Einrichtungen bei der Erfüllung ihrer gesetzlichen Verantwortung nachhaltig zu unterstützen.

Dieses Selbstverständnis prägt die tägliche Arbeit der Datenschutzaufsicht. Frühzeitige Beratung, vertrauensvolle Zusammenarbeit und ein kontinuierlicher Dialog mit Verantwortlichen und betrieblichen Datenschutzbeauftragten tragen dazu bei, datenschutzrechtliche Fragestellungen bereits während der Planung neuer Verfahren zu erkennen und praxisgerechte Lösungen zu entwickeln. Datenschutz wird dadurch nicht als Hindernis für organisatorische oder technische Entwicklungen verstanden, sondern als Qualitätsmerkmal einer verantwortungsvollen und rechtskonformen Verwaltung.

Ein wesentlicher Bestandteil dieser präventiven Tätigkeit ist die Bereitstellung verständlicher Orientierungshilfen für die Praxis. Hierzu zählen insbesondere Handreichungen, Praxisblätter, Muster sowie Hinweise zur Anwendung des kirchlichen Datenschutzrechts. Ergänzt werden diese durch Fachvorträge, Schulungen und

Informationsveranstaltungen, mit denen Verantwortliche, betriebliche Datenschutzbeauftragte und Beschäftigte bei der Umsetzung datenschutzrechtlicher Anforderungen unterstützt werden.

Das KDSZ Bayern versteht sich dabei als verlässlicher Ansprechpartner für alle kirchlichen Einrichtungen in Bayern. Ziel ist es, gemeinsam mit den Verantwortlichen tragfähige Lösungen zu entwickeln, die sowohl den gesetzlichen Anforderungen als auch den praktischen Bedürfnissen der Einrichtungen gerecht werden. Beratung und Kooperation ersetzen dabei nicht die unabhängige Kontrollfunktion der Datenschutzaufsicht, sondern ergänzen diese in sinnvoller Weise.

Ein funktionierendes Datenschutzmanagement entsteht nicht erst durch aufsichtsrechtliche Maßnahmen. Es entwickelt sich dort, wo Verantwortliche Datenschutz als Bestandteil guter Organisationsführung verstehen, betriebliche Datenschutzbeauftragte frühzeitig eingebunden werden und die Datenschutzaufsicht ihre Erfahrungen und ihre fachliche Expertise beratend einbringen kann. Prävention, Information und Kooperation bilden deshalb einen wesentlichen Bestandteil moderner Datenschutzaufsicht.

> Beratung und Kontrolle stehen nicht im Widerspruch. Sie bilden gemeinsam das Leitbild einer modernen Datenschutzaufsicht.

3.3.7 Einheitliche Anwendung des kirchlichen Datenschutzrechts

Ein wirksamer Datenschutz setzt voraus, dass vergleichbare Sachverhalte nach vergleichbaren rechtlichen Maßstäben beurteilt werden. Die Förderung einer möglichst einheitlichen Anwendung des kirchlichen Datenschutzrechts gehört deshalb zu den gesetzlichen Aufgaben der Datenschutzaufsicht. Sie schafft Rechtssicherheit für die kirchlichen Einrichtungen und gewährleistet zugleich einen gleichwertigen Schutz der Rechte betroffener Personen innerhalb des gesamten Geltungsbereichs des KDG.

Dieses Ziel kann nur durch einen kontinuierlichen fachlichen Austausch erreicht werden. Das KDSZ Bayern arbeitet deshalb eng mit den übrigen kirchlichen Datenschutzaufsichten in Deutschland zusammen. Gemeinsame Abstimmungen, fachliche Arbeitsgruppen und der regelmäßige Austausch zu Rechtsfragen tragen dazu bei, unterschiedliche Rechtsauffassungen frühzeitig zu erkennen und möglichst einheitliche Lösungen zu entwickeln.

Ebenso wichtig ist die Zusammenarbeit mit den staatlichen Datenschutzaufsichtsbehörden. Zahlreiche datenschutzrechtliche Fragestellungen betreffen kirchliche und staatliche Stellen gleichermaßen oder erfordern eine abgestimmte Bewertung. Der fachliche Austausch mit dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD), dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) sowie weiteren staatlichen oder spezifischen Datenschutzaufsichtsbehörden leistet daher einen wichtigen Beitrag zur Fortentwicklung einer kohärenten Datenschutzpraxis.

Zur Förderung einer einheitlichen Rechtsanwendung veröffentlicht das KDSZ Bayern regelmäßig Orientierungshilfen, Handreichungen, Praxisblätter sowie Entscheidungen von grundsätzlicher Bedeutung. Diese Veröffentlichungen dienen nicht allein der Information, sondern sollen den Verantwortlichen und den betrieblichen Datenschutzbeauftragten eine verlässliche Grundlage für die datenschutzkonforme Gestaltung ihrer Verfahren bieten.

Die Mitwirkung in überdiözesanen Arbeitsgruppen sowie der kontinuierliche Austausch mit den anderen kirchlichen Datenschutzaufsichten ermöglichen es darüber hinaus, praktische Erfahrungen aus unterschiedlichen Bereichen zusammenzuführen und in die Weiterentwicklung des kirchlichen Datenschutzrechts einfließen zu lassen. Datenschutzaufsicht endet daher nicht bei der Bearbeitung einzelner Verfahren. Sie umfasst ebenso die Aufgabe, durch fachliche Zusammenarbeit, transparente Kommunikation und einheitliche Maßstäbe die Fortentwicklung des kirchlichen Datenschutzes insgesamt zu fördern.

Die in den nachfolgenden Kapiteln dargestellten Beratungen, Prüfungen und Projekte verdeutlichen, wie dieses Selbstverständnis im Berichtsjahr praktisch umgesetzt wurde. Sie zeigen zugleich, dass wirksame Datenschutzaufsicht nicht allein durch Kontrolle entsteht, sondern vor allem durch einen offenen Dialog, gegenseitiges Vertrauen und das gemeinsame Ziel, den Schutz personenbezogener Daten in den kirchlichen Einrichtungen nachhaltig zu stärken.

> Rechtssicherheit entsteht durch transparente Entscheidungen, fachlichen Austausch und eine möglichst einheitliche Anwendung des kirchlichen Datenschutzrechts.

3.4 Zusammenarbeit statt Gegeneinander

Die Wahrnehmung der gesetzlichen Aufgaben der Datenschutzaufsicht setzt ein ausgewogenes Verhältnis von Beratung und Kontrolle voraus. Verantwortliche, betriebliche Datenschutzbeauftragte und Datenschutzaufsicht verfolgen dabei ein gemeinsames Ziel. Gemeinsam tragen sie dazu bei, den Schutz personenbezogener Daten zu gewährleisten und die Rechte der betroffenen Personen wirksam zu sichern. Ihre Aufgaben unterscheiden sich, ihr gemeinsames Anliegen bleibt jedoch dasselbe.

Das KDSZ Bayern versteht Datenschutzaufsicht daher nicht ausschließlich als reaktive Kontrollinstanz. Ein wesentlicher Bestandteil seiner Tätigkeit besteht darin, kirchliche Einrichtungen frühzeitig zu unterstützen und datenschutzrechtliche Fragestellungen bereits im Vorfeld gemeinsam zu lösen. Dies geschieht durch die Beantwortung von Grundsatzfragen, die Entwicklung von Orientierungshilfen und Handreichungen, die Durchführung von Schulungen und Informationsveranstaltungen sowie den kontinuierlichen Dialog mit Verantwortlichen und betrieblichen Datenschutzbeauftragten. Ziel ist es, Datenschutz als Bestandteil guter Organisationsführung nachhaltig in den Einrichtungen zu verankern und ein wirksames Datenschutzmanagement zu fördern.

Diese beratungsorientierte Arbeitsweise setzt ein vertrauensvolles Miteinander voraus. Die Datenschutzaufsicht versteht sich dabei als fachkundige Ansprechpartnerin, die ihre Erfahrungen aus zahlreichen Beratungs- und Prüfungsverfahren bündelt und den kirchlichen Einrichtungen für vergleichbare Fragestellungen zur Verfügung stellt. Dadurch können datenschutzrechtliche Risiken häufig bereits im Vorfeld erkannt und rechtskonforme Lösungen entwickelt werden.

Beratung ersetzt jedoch nicht die unabhängige Kontrollfunktion der Datenschutzaufsicht. Wo Rechte betroffener Personen verletzt werden, Datenschutzverletzungen auftreten oder gesetzliche Vorgaben dauerhaft nicht eingehalten werden, ist die Datenschutzaufsicht verpflichtet, ihren gesetzlichen Auftrag konsequent wahrzunehmen. Unabhängigkeit und Durchsetzungsfähigkeit bleiben daher unverzichtbare Voraussetzungen einer wirksamen Datenschutzaufsicht.

Beratung und Kontrolle ergänzen sich zu einem ausgewogenen System moderner Datenschutzaufsicht. Beratung trägt dazu bei, Datenschutzverstöße möglichst zu vermeiden; unabhängige Kontrolle gewährleistet die wirksame Durchsetzung des Datenschutzrechts und den Schutz der Rechte betroffener Personen.

> Moderne Datenschutzaufsicht setzt auf Prävention, Dialog und unabhängige Kontrolle. Nur das Zusammenspiel dieser Elemente gewährleistet einen wirksamen und nachhaltigen Datenschutz.

Dieses kooperative Verständnis prägt die Arbeit des KDSZ Bayern seit seiner Gründung. Es verbindet die unabhängige Wahrnehmung der gesetzlichen Aufsicht mit dem Anspruch, die kirchlichen Einrichtungen als kompetenter und verlässlicher Partner bei der Umsetzung des kirchlichen Datenschutzrechts zu begleiten. Ziel bleibt dabei stets ein wirksamer, praxistauglicher und nachhaltig verankerter Datenschutz in allen kirchlichen Einrichtungen Bayerns.

Wie sich dieses Selbstverständnis einer modernen, beratungsorientierten Datenschutzaufsicht im Berichtsjahr 2025 konkret ausgewirkt hat, zeigen die nachfolgenden Kapitel anhand ausgewählter Beratungen, Beschwerden, Datenschutzverletzungen und Prüfungen.

3.5 Voraussetzungen einer leistungsfähigen Datenschutzaufsicht

Leistungsfähige Datenschutzaufsicht braucht mehr als gesetzliche Zuständigkeiten

Eine moderne Datenschutzaufsicht kann ihren gesetzlichen Auftrag nur erfüllen, wenn sie über angemessene personelle, fachliche und organisatorische Ressourcen verfügt. Wesentliche Voraussetzungen sind insbesondere:

- ☑ **qualifiziertes Personal** mit juristischer, technischer und organisatorischer Expertise,
- ☑ **präventive Beratung** zur Vermeidung von Datenschutzverstößen,
- ☑ **zentrale Bündelung von Fachwissen** für alle sieben bayerischen (Erz-)Diözesen,
- ☑ **Begleitung der Digitalisierung** und neuer Technologien,
- ☑ **nachhaltige organisatorische und finanzielle Ausstattung**.

3.5.1 Der gesetzliche Auftrag erfordert angemessene Ressourcen

Die dem KDSZ Bayern durch das Gesetz über den Kirchlichen Datenschutz übertragenen Aufgaben sind in den vergangenen Jahren kontinuierlich gewachsen. Neben der Bearbeitung von Beschwerden und Datenschutzverletzungen umfasst die Tätigkeit der Datenschutzaufsicht heute insbesondere die Beratung von Verantwortlichen und betrieblichen Datenschutzbeauftragten, die Durchführung von Audits und Prüfungen, die Entwicklung von Orientierungshilfen und Handreichungen, die Mitwirkung an der Fortentwicklung des kirchlichen Datenschutzrechts sowie umfangreiche Informations- und Schulungsangebote. Hinzu treten Grund-

satzfragen, die Beobachtung technischer Entwicklungen und die zunehmende Begleitung komplexer Digitalisierungsprojekte.

Gleichzeitig steigen die fachlichen Anforderungen an die Datenschutzaufsicht. Digitalisierung, cloudbasierte Dienste, Künstliche Intelligenz, Cybersicherheit und zunehmend vernetzte IT-Infrastrukturen verändern die Verarbeitung personenbezogener Daten grundlegend. Datenschutzrechtliche Fragestellungen betreffen heute regelmäßig hochkomplexe technische und organisatorische Zusammenhänge und erfordern interdisziplinäre Fachkenntnisse, die weit über klassische Rechtsberatung hinausgehen.

Eine moderne Datenschutzaufsicht kann diesen gesetzlichen Auftrag daher nur erfüllen, wenn sie über ausreichend qualifizierte Mitarbeiterinnen und Mitarbeiter mit unterschiedlichen fachlichen Schwerpunkten verfügt. Die Qualität datenschutzaufsichtlicher Entscheidungen, die Intensität der Beratung sowie die Fähigkeit, neue technische Entwicklungen sachgerecht zu begleiten, hängen unmittelbar von einer angemessenen personellen und fachlichen Ausstattung ab.

3.5.2 Prävention ist wirtschaftlicher als nachträgliche Konfliktlösung

Wirksame Datenschutzaufsicht beginnt nicht erst mit einer Beschwerde oder einem Datenschutzverstoß. Frühzeitige Beratung, verständliche Orientierungshilfen, regelmäßige Schulungen sowie risikoorientierte Audits tragen wesentlich dazu bei, Datenschutzverletzungen bereits im Vorfeld zu vermeiden und datenschutzrechtliche Anforderungen von Beginn an in organisatorische Entscheidungen einzubeziehen.

Dieser präventive Ansatz kommt sowohl den kirchlichen Einrichtungen als auch der Datenschutzaufsicht zugute. Werden datenschutzrechtliche Risiken frühzeitig erkannt und geeignete Maßnahmen umgesetzt, können aufwendige Beschwerdeverfahren, Datenschutzverletzungen oder umfangreiche aufsichtsrechtliche Maßnahmen häufig vermieden werden. Prävention stärkt damit nicht nur den

Schutz personenbezogener Daten, sondern trägt zugleich zu einem effizienten Einsatz personeller und finanzieller Ressourcen auf allen Seiten bei.

Investitionen in Beratung, Information und Sensibilisierung sind deshalb zugleich Investitionen in eine wirksame und wirtschaftliche Datenschutzaufsicht.

> Jede vermiedene Datenschutzverletzung spart Ressourcen – bei den Verantwortlichen ebenso wie bei der Datenschutzaufsicht. Prävention ist deshalb der wirtschaftlichste Teil wirksamer Datenschutzaufsicht.

3.5.3 Zentrale Kompetenz entlastet die sieben bayerischen (Erz-)Diözesen

Das KDSZ Bayern nimmt seine Aufgaben für alle sieben bayerischen (Erz-)Diözesen wahr. Diese gemeinsame Organisation ermöglicht es, datenschutzrechtliche Expertise an einer Stelle zu bündeln und den kirchlichen Einrichtungen zentral zur Verfügung zu stellen.

Grundsatzfragen müssen dadurch nicht in jeder Diözese gesondert bearbeitet werden. Orientierungshilfen, Handreichungen und Praxisblätter werden zentral entwickelt und stehen anschließend allen Verantwortlichen und betrieblichen Datenschutzbeauftragten gleichermaßen zur Verfügung. Gleiches gilt für Schulungsangebote, Prüfungsmaßstäbe, fachliche Empfehlungen sowie die Bewertung neuer technischer und rechtlicher Entwicklungen.

Diese Bündelung hochspezialisierten Fachwissens schafft erhebliche Synergieeffekte. Ohne eine zentrale Datenschutzaufsicht müssten zahlreiche Kompetenzen in jeder einzelnen Diözese separat aufgebaut, fortentwickelt und dauerhaft personell vorgehalten werden. Die gemeinsame Wahrnehmung der Datenschutzaufsicht führt demgegenüber zu einer einheitlichen Rechtsanwendung, einer höheren Beratungsqualität und einem wirtschaftlicheren Einsatz personeller Ressourcen.

Eine leistungsfähige Datenschutzaufsicht entlastet damit nicht nur die Verantwortlichen und die betrieblichen Datenschutzbeauftragten der kirchlichen Einrichtungen. Sie trägt zugleich dazu bei, dass hochspezialisiertes Fachwissen nur einmal

aufgebaut werden muss und anschließend allen sieben bayerischen (Erz-)Diözesen gleichermaßen zugutekommt.

3.5.4 Datenschutzaufsicht als Investition in Rechtssicherheit und Digitalisierung

Die Digitalisierung kirchlicher Einrichtungen wird sich in den kommenden Jahren weiter beschleunigen. Elektronische Verwaltungsverfahren, cloudbasierte Fachanwendungen, digitale Kommunikationsplattformen und Anwendungen der Künstlichen Intelligenz werden die Arbeitsabläufe nachhaltig verändern. Gleichzeitig steigen die Anforderungen an Informationssicherheit, digitale Souveränität und den Schutz personenbezogener Daten.

Eine leistungsfähige Datenschutzaufsicht schafft hierfür den notwendigen rechtlichen Orientierungsrahmen. Sie unterstützt Verantwortliche dabei, neue Technologien datenschutzkonform einzusetzen, begleitet Innovationsprozesse mit ihrer fachlichen Expertise und trägt dazu bei, rechtliche Unsicherheiten frühzeitig zu beseitigen. Datenschutz wird dadurch nicht zum Hemmnis der Digitalisierung, sondern zu einer ihrer wesentlichen Voraussetzungen.

Gerade im kirchlichen Bereich, in dem vielfach besonders schutzwürdige personenbezogene Daten verarbeitet werden, stärkt eine kompetente Datenschutzaufsicht das Vertrauen in digitale Verwaltungsverfahren und neue Technologien. Sie leistet damit zugleich einen wichtigen Beitrag zur digitalen Souveränität der Kirche. Wer Digitalisierung verantwortungsvoll gestalten will, benötigt nicht weniger, sondern mehr datenschutzrechtliche Kompetenz.

Eine leistungsfähige Datenschutzaufsicht ist deshalb nicht allein ein Instrument zur Kontrolle gesetzlicher Vorgaben. Sie ist zugleich ein Motor für rechtssichere Innovation, nachhaltige Digitalisierung und eine moderne kirchliche Verwaltung.

> Datenschutzaufsicht schafft Rechtssicherheit für die Digitalisierung. Sie ermöglicht Innovation, indem sie rechtliche Risiken frühzeitig bewertet und Verantwortliche bei datenschutzkonformen Lösungen unterstützt.

3.5.5 Leistungsfähigkeit als gemeinsame Verantwortung

Datenschutz kann dauerhaft nur gelingen, wenn alle Beteiligten ihre jeweilige Verantwortung wahrnehmen. Verantwortliche schaffen die organisatorischen Voraussetzungen, betriebliche Datenschutzbeauftragte begleiten die Umsetzung innerhalb der Einrichtungen und die Datenschutzaufsicht überwacht, berät und unterstützt unabhängig die Einhaltung des Datenschutzrechts.

Dieses Zusammenspiel setzt voraus, dass jede dieser Funktionen angemessen ausgestattet ist. Ebenso wie Verantwortliche ausreichende personelle und organisatorische Ressourcen für ihr Datenschutzmanagement bereitstellen müssen, benötigt auch die Datenschutzaufsicht die personellen und fachlichen Voraussetzungen, um ihren gesetzlichen Auftrag wirksam erfüllen zu können.

Die personelle und fachliche Ausstattung der Datenschutzaufsicht ist daher kein Selbstzweck. Sie bildet vielmehr eine wesentliche Voraussetzung dafür, dass die gesetzlichen Aufgaben wirksam erfüllt, die Verantwortlichen nachhaltig unterstützt und die Rechte der betroffenen Personen dauerhaft geschützt werden können.

Eine leistungsfähige Datenschutzaufsicht stärkt damit nicht nur den Datenschutz in den kirchlichen Einrichtungen, sondern leistet zugleich einen wesentlichen Beitrag zu einer rechtssicheren, wirtschaftlichen und zukunftsfähigen Verwaltung in der katholischen Kirche in Bayern.

4 Aufsichtstätigkeit im Berichtsjahr 2025

Die gesetzlichen Aufgaben der Datenschutzaufsicht verwirklichen sich nicht allein durch abstrakte Zuständigkeiten und gesetzliche Befugnisse. Ihre praktische Bedeutung zeigt sich vielmehr in der täglichen Zusammenarbeit mit den kirchlichen Einrichtungen, den Verantwortlichen, den betrieblichen Datenschutzbeauftragten sowie den betroffenen Personen. Beratung, Beschwerden, Meldungen von Datenschutzverletzungen und risikoorientierte Audits bilden dabei die wesentlichen Instrumente einer modernen Datenschutzaufsicht.

Die nachfolgenden Abschnitte geben einen Überblick über die Tätigkeit des KDSZ Bayern im Berichtsjahr 2025. Die Darstellung erhebt dabei keinen Anspruch auf Vollständigkeit. Sie zeigt vielmehr exemplarisch die Schwerpunkte der Aufsichtspraxis sowie die Fragestellungen auf, welche die kirchlichen Einrichtungen und die Datenschutzaufsicht im Berichtsjahr in besonderer Weise beschäftigt haben.

Die Erfahrungen aus den einzelnen Verfahren verdeutlichen zugleich die fortschreitende Veränderung der Datenschutzpraxis. Während in den vergangenen Jahren häufig einzelne datenschutzrechtliche Fragestellungen im Mittelpunkt standen, prägen heute zunehmend komplexe Organisations- und Digitalisierungsprojekte, Künstliche Intelligenz, Informationssicherheit und digitale Verwaltungsprozesse die Arbeit der Datenschutzaufsicht. Datenschutzrechtliche Bewertungen erfordern deshalb immer häufiger ein Zusammenspiel juristischer, technischer und organisatorischer Expertise.

Die Tätigkeit der Datenschutzaufsicht beschränkt sich dabei nicht auf die Bearbeitung einzelner Verfahren. Erkenntnisse aus Beratungen, Beschwerden, Datenschutzverletzungen und Audits ergänzen sich gegenseitig und fließen kontinuierlich in Orientierungshilfen, Schulungsangebote sowie die Weiterentwicklung der Aufsichtspraxis ein. Die einzelnen Aufgabenbereiche stehen daher nicht isoliert nebeneinander, sondern bilden gemeinsam die Grundlage einer präventiven, risikoorientierten und praxisnahen Datenschutzaufsicht.

Die nachfolgenden Kapitel geben einen Überblick über die Beratungs- und Prüfungsschwerpunkte des Berichtsjahres und zeigen anhand ausgewählter Beispiele, wie das KDSZ Bayern seinen gesetzlichen Auftrag im Berichtsjahr 2025 wahrgenommen hat.

4.1 Beratungen

Die Beratung der Verantwortlichen und der betrieblichen Datenschutzbeauftragten gehört zu den gesetzlichen Kernaufgaben der Datenschutzaufsicht. Sie dient nicht nur der Beantwortung konkreter Rechtsfragen, sondern verfolgt das Ziel, datenschutzrechtliche Risiken frühzeitig zu erkennen und rechtskonforme Lösungen bereits vor der Einführung neuer Verfahren oder dem Eintritt von Datenschutzverletzungen zu entwickeln. Die nachfolgende Darstellung erhebt daher keinen Anspruch auf Vollständigkeit. Sie zeigt vielmehr die Themenbereiche auf, welche die Beratungstätigkeit im Berichtsjahr in besonderer Weise geprägt haben.

Beratungsschwerpunkte 2025

Die Beratungstätigkeit des KDSZ Bayern wurde im Berichtsjahr insbesondere durch folgende Themen geprägt:

- ☑ **Digitalisierung in kirchlichen Einrichtungen**
- ☑ **Künstliche Intelligenz**
- ☑ **Datenschutzmanagement und Organisation**
- ☑ **kirchliche Bildungseinrichtungen**
- ☑ **kirchliche Sozialwirtschaft**
- ☑ **Öffentlichkeitsarbeit und digitale Kommunikation**

Der zunehmende Beratungsbedarf zeigt, dass Datenschutz heute bereits in frühen Planungsphasen organisatorischer und technischer Projekte berücksichtigt wird.

4.1.1 Digitalisierung prägt die Beratungspraxis

Den größten Teil der Beratungsanfragen bildeten Fragestellungen im Zusammenhang mit der fortschreitenden Digitalisierung in kirchlichen Einrichtungen. Im Mittelpunkt standen die Einführung neuer Softwarelösungen, der datenschutzkonforme Einsatz von Cloud-Diensten, die Entwicklung von Ausstiegsszenarien für Cloud-Anwendungen sowie Fragen zur sicheren Authentifizierung, insbesondere durch den Einsatz von Mehrfaktor-Authentifizierung.

Darüber hinaus begleitete das KDSZ Bayern verschiedene Digitalisierungsprojekte der bayerischen (Erz-)Diözesen beratend, unter anderem bei der Einführung neuer Verwaltungsverfahren und digitaler Fachanwendungen. Ebenso nahmen Fragestellungen zu Datenschutzinformationen auf Internetseiten sowie zur datenschutzkonformen Gestaltung digitaler Prozesse einen breiten Raum ein.

4.1.2 Künstliche Intelligenz als neues Beratungsschwerpunktthema

Künstliche Intelligenz entwickelte sich im Berichtsjahr erstmals zu einem eigenständigen Beratungsthema. Verantwortliche und betriebliche Datenschutzbeauftragte suchten insbesondere Unterstützung bei der datenschutzrechtlichen Bewertung verschiedener KI-Anwendungen sowie bei der Frage, unter welchen Voraussetzungen personenbezogene Daten in KI-Systemen verarbeitet werden dürfen.

Die Beratungspraxis zeigte deutlich, dass die Einrichtungen den Chancen neuer Technologien offen gegenüberstehen, gleichzeitig aber einen hohen Bedarf an rechtlicher Orientierung und praxisgerechten Handlungsempfehlungen haben.

> Künstliche Intelligenz entwickelte sich im Berichtsjahr erstmals zu einem eigenständigen Schwerpunkt der Beratungstätigkeit.

4.1.3 Schulen, Kindertageseinrichtungen und kirchliche Bildung

Auch Schulen und Kindertageseinrichtungen gehörten zu den beratungsintensiven Bereichen. Gegenstand der Anfragen waren insbesondere der Einsatz digitaler Lernplattformen, datenschutzrechtliche Fragestellungen im Verhältnis zu Sorge- und Nichtsorgeberechtigten sowie die Rollen verschiedener Funktionsträger innerhalb der Einrichtungen, etwa von Medienbeauftragten oder Elternvertretungen.

Hinzu kamen Fragen zur datenschutzgerechten Gestaltung von Schul- und Einrichtungswebseiten sowie zur Nutzung digitaler Kommunikationsformen.

Dauerbrenner in der Beratung blieben Fragen zu Fotos und Videos von Kindern und Jugendlichen. Ob bei der Erstellung, dem Ausdruck oder der Veröffentlichung im Internet stellten sich viele Fragen und es ergab sich ein hoher Beratungsbedarf.

4.1.4 Datenschutz in Organisation und Verwaltung

Breiten Raum nahmen Fragestellungen zur Organisation des Datenschutzes innerhalb kirchlicher Einrichtungen ein. Hierzu gehörten insbesondere die Weitergabe personenbezogener Daten zwischen kirchlichen und nichtkirchlichen Stellen, datenschutzrechtliche Anforderungen bei Vertragsgestaltungen – etwa im Zusammenhang mit Auftragsverarbeitungen sowie Arbeits-, Schul- oder Kindertagesstättenverträgen –, Löschkonzepte und Aufbewahrungsfristen sowie einzelne Fragen der Amtshilfe und des Umgangs mit personenbezogenen Daten verstorbener Personen.

Auch Einrichtungen der kirchlichen Sozialwirtschaft nahmen die Beratung des KDSZ Bayern im Berichtsjahr in erheblichem Umfang in Anspruch. Im Mittelpunkt standen dabei insbesondere Fragestellungen zur datenschutzkonformen Gestaltung organisatorischer Abläufe, zur Zusammenarbeit zwischen Trägern und ihren Einrichtungen, zum Einsatz neuer Fachverfahren sowie zur Umsetzung datenschutzrechtlicher Anforderungen im Rahmen fortschreitender Digitalisierungsprozesse. Aufgrund der Verarbeitung besonders sensibler personenbezogener Daten kommt einem funktionierenden Datenschutzmanagement in diesem Bereich eine besondere Bedeu-

tung zu. Der intensive fachliche Austausch mit den Sozialträgern bildete zugleich eine wichtige Grundlage für die Entwicklung des im Berichtsjahr begonnenen Auditkonzepts für die katholische Sozialwirtschaft, auf das im weiteren Verlauf dieses Tätigkeitsberichts näher eingegangen wird.

Diese Beratungen verdeutlichen, dass Datenschutz heute zunehmend als Bestandteil einer geordneten Organisations- und Verwaltungsstruktur verstanden wird und nicht mehr ausschließlich als rechtliche Einzelfrage..

4.1.5 Öffentlichkeitsarbeit und digitale Kommunikation

Regelmäßig nachgefragt wurden zudem datenschutzrechtliche Anforderungen bei der Anfertigung und Veröffentlichung von Foto- und Filmaufnahmen sowie beim Einsatz sozialer Netzwerke und digitaler Kommunikationsplattformen. Hinzu kamen Beratungen zur Videoüberwachung in kirchlichen Einrichtungen sowie zu datenschutzrechtlichen Rahmenbedingungen bei öffentlich zugänglichen Bereichen.

Gerade diese Themen zeigen, dass Digitalisierung und Öffentlichkeitsarbeit heute untrennbar miteinander verbunden sind und eine sorgfältige datenschutzrechtliche Bewertung bereits im Vorfeld erfordern.

4.1.6 Beispiele aus der Beratungspraxis

Einführung einer verpflichtenden Mehrfaktorauthentifizierung

Im Vorfeld der Einführung einer verpflichtenden Mehrfaktorauthentifizierung für eine in mehreren (Erz-)Diözesen eingesetzte Fachanwendung wurde das KDSZ Bayern frühzeitig um eine datenschutzrechtliche Einschätzung gebeten. Gegenstand der Beratung waren insbesondere die Auswahl geeigneter Authentifizierungsverfahren, die datenschutzgerechte Ausgestaltung des Rollouts sowie die Vereinbarkeit verschiedener Verfahren mit den Anforderungen des KDG.

Die Beratung verdeutlichte, dass Datenschutz und Informationssicherheit heute eng miteinander verzahnt sind. Eine verpflichtende Mehrfaktorauthentifizierung stellt einen wesentlichen Baustein zum Schutz personenbezogener Daten dar und trägt dazu bei, unbefugte Zugriffe auf IT-Systeme wirksam zu erschweren. Durch die frühzeitige Einbindung der Datenschutzaufsicht konnten datenschutzrechtliche Fragestellungen bereits vor der Einführung des Verfahrens geklärt und eine datenschutzfreundliche Umsetzung unterstützt werden.

Amtshilfeersuchen nach dem Tod einer betroffenen Person

Eine kirchliche Einrichtung wandte sich mit der Frage an das KDSZ Bayern, ob medizinische und pflegerische Unterlagen einer verstorbenen Person auf Anforderung eines Nachlassgerichts zur Prüfung der Testierfähigkeit herausgegeben werden dürfen. Die Einrichtung war unsicher, ob die gerichtliche Anfrage allein eine ausreichende Rechtsgrundlage für die Übermittlung besonders sensibler personenbezogener Daten darstellt.

Im Rahmen der Beratung wurden die datenschutzrechtlichen Voraussetzungen einer Datenübermittlung, die Anforderungen an eine hinreichende Rechtsgrundlage sowie die Bedeutung gesetzlicher Verschwiegenheitspflichten geprüft. Der Fall verdeutlicht, dass Auskunfts- und Herausgabeverlangen öffentlicher Stellen sorgfältig rechtlich bewertet werden müssen und eine Datenübermittlung nicht allein deshalb zulässig ist, weil sie von einer Behörde oder einem Gericht angefordert wird. Eine frühzeitige datenschutzrechtliche Beratung trägt dazu bei, sowohl die Rechte der betroffenen Personen als auch die berechtigten Interessen der anfragenden Stellen in einen angemessenen Ausgleich zu bringen.

Videoüberwachung auf einem Friedhof

Eine Kirchengemeinde wandte sich an das KKDSZ Bayern mit der Frage, ob nach wiederholten Sachbeschädigungen und Verwüstungen auf dem kirchlichen Friedhof eine Videoüberwachung eingerichtet werden dürfe.

Im Rahmen der Beratung waren insbesondere die Erforderlichkeit und Verhältnismäßigkeit einer Videoüberwachung, mögliche alternative Schutzmaßnahmen sowie die berechtigten Interessen der Friedhofsbesucher gegeneinander abzuwägen. Der Fall verdeutlicht, dass der Einsatz von Videoüberwachung stets eine sorgfältige Prüfung des Einzelfalls erfordert und nicht allein durch das Eigentum an einem Grundstück oder das Vorliegen von Sachbeschädigungen gerechtfertigt ist. Bereits im Vorfeld der Einführung technischer Überwachungsmaßnahmen empfiehlt sich daher eine datenschutzrechtliche Beratung, um eine rechtmäßige und verhältnismäßige Lösung zu entwickeln.

Auskunftsrechte bei gemeinsamem Sorgerecht

Eine Kindertageseinrichtung bat das KDSZ Bayern um Beratung im Zusammenhang mit einem Auskunftsersuchen eines Elternteils. Dieser begehrte Auskunft darüber, ob sein Kind eine bestimmte Einrichtung besucht. Gleichzeitig bestanden innerhalb der Einrichtung Zweifel, ob eine Auskunft erteilt werden durfte, da unklar war, ob das gemeinsame Sorgerecht fortbestand und eine Offenlegung des Aufenthaltsortes des Kindes möglicherweise dessen Schutzinteressen beeinträchtigen könnte.

Im Rahmen der Beratung wurden insbesondere die datenschutzrechtlichen Voraussetzungen des Auskunftsrechts, die Bedeutung des elterlichen Sorgerechts sowie die erforderliche Sachverhaltsaufklärung vor einer Entscheidung erörtert. Der Fall verdeutlicht, dass Auskunftsersuchen sorgfältig geprüft werden müssen und neben den datenschutzrechtlichen Vorgaben häufig auch familienrechtliche Besonderheiten zu berücksichtigen sind. Eine datenschutzkonforme Entscheidung setzt daher regelmäßig eine vollständige Klärung der tatsächlichen und rechtlichen Verhältnisse voraus, bevor personenbezogene Daten offengelegt oder eine Auskunft erteilt wird.

4.1.7 Entwicklung der Beratungstätigkeit

Die Beratungstätigkeit hat sich im Berichtszeitraum erneut deutlich intensiviert. Gegenüber den Vorjahren hat sich das Beratungsaufkommen innerhalb weniger Jahre um ein Vielfaches erhöht und den langfristigen Trend einer kontinuierlich steigenden Nachfrage eindrucksvoll bestätigt.

Gleichzeitig verändert sich die Art der Anfragen. Während früher häufig einzelne datenschutzrechtliche Fragestellungen im Vordergrund standen, betreffen Beratungen heute zunehmend komplexe Organisations- und Digitalisierungsprojekte, die eine enge Verzahnung rechtlicher, technischer und organisatorischer Aspekte erfordern. Besonders die Themen Künstliche Intelligenz, Cloud-Nutzung, Informationssicherheit und digitale Verwaltungsverfahren werden die Beratungstätigkeit der Datenschutzaufsicht auch in den kommenden Jahren maßgeblich prägen.

> Die Beratung entwickelt sich von der Beantwortung einzelner Rechtsfragen hin zur Begleitung komplexer Digitalisierungs- und Organisationsprojekte.

Diese Entwicklung bestätigt zugleich den präventiven Ansatz des KDSZ Bayern. Frühzeitige Beratung ermöglicht es den kirchlichen Einrichtungen, datenschutzrechtliche Anforderungen bereits bei der Planung neuer Verfahren zu berücksichtigen. Dadurch lassen sich spätere Datenschutzverletzungen, Beschwerden und aufwendige aufsichtsrechtliche Verfahren vielfach vermeiden. Beratung ist deshalb nicht nur gesetzlicher Auftrag der Datenschutzaufsicht, sondern zugleich ein wesentlicher Beitrag zu einer rechtssicheren und zukunftsfähigen Digitalisierung der katholischen Kirche in Bayern.

4.2 Meldungen von Datenschutzverletzungen

Meldungen von Datenschutzverletzungen gehören zu den gesetzlichen Pflichten der Verantwortlichen und bilden einen wesentlichen Bestandteil eines funktionierenden Datenschutzmanagements. Sie dienen nicht der Sanktionierung eingetretener Fehler, sondern ermöglichen es, Risiken für betroffene Personen frühzeitig zu bewerten, geeignete Abhilfemaßnahmen einzuleiten und vergleichbare Vorfälle künftig zu vermeiden.

Für die Datenschutzaufsicht stellen diese Meldungen zugleich eine wertvolle Erkenntnisquelle dar. Sie zeigen auf, welche organisatorischen oder technischen Schwachstellen in der Praxis auftreten und in welchen Bereichen weiterer Beratungs- oder Unterstützungsbedarf besteht. Datenschutzverletzungen sind daher nicht nur Gegenstand aufsichtsrechtlicher Verfahren, sondern zugleich Ausgangspunkt für Präventionsmaßnahmen, Orientierungshilfen und Schulungsangebote.

Datenschutzverletzungen – Erkenntnisse des Berichtsjahres

Die im Berichtsjahr gemeldeten Datenschutzverletzungen zeigen insbesondere:

- ☑ **Fehlversendungen** bleiben die häufigste Ursache.
- ☑ **Cyberangriffe** und IT-Sicherheitsvorfälle gewinnen weiter an Bedeutung.
- ☑ **Organisatorische Maßnahmen** verhindern viele Vorfälle bereits im Vorfeld.
- ☑ **Eine offene Meldekultur** stärkt den Datenschutz.
- ☑ **Jeder Vorfall liefert Erkenntnisse** für die Weiterentwicklung des Datenschutzmanagements.

4.2.1 Datenschutzverletzungen als Bestandteil einer gelebten Datenschutzkultur

Die Meldung einer Datenschutzverletzung darf nicht als Zeichen unzureichenden Datenschutzes verstanden werden. Vielmehr zeigt sie, dass innerhalb einer Einrichtung funktionierende Meldewege bestehen und datenschutzrechtliche Risiken ernst genommen werden. Nicht jede Datenschutzverletzung lässt sich vermeiden. Entscheidend ist vielmehr, dass Vorfälle erkannt, sachgerecht bewertet und die erforderlichen Maßnahmen unverzüglich eingeleitet werden.

Die Erfahrungen der vergangenen Jahre zeigen, dass das Bewusstsein für die gesetzlichen Meldepflichten in den kirchlichen Einrichtungen weiter gewachsen ist. Verantwortliche und betriebliche Datenschutzbeauftragte beziehen die Datenschutzaufsicht zunehmend frühzeitig ein und suchen bereits während der Bearbeitung eines Vorfalls den fachlichen Austausch.

Die erfreuliche Entwicklung hin zu einer frühzeitigen Einbindung der Datenschutzaufsicht führt zugleich zu einem kontinuierlich steigenden Bearbeitungsaufwand. Die sorgfältige Prüfung jeder gemeldeten Datenschutzverletzung erfordert eine individuelle rechtliche Bewertung und bindet entsprechende personelle Ressourcen. Dies kann insbesondere bei einem erhöhten Meldeaufkommen Auswirkungen auf die Bearbeitungsdauer einzelner Verfahren haben.

4.2.2 Typische Ursachen von Datenschutzverletzungen

Die Auswertung der Meldungen zeigt, dass Datenschutzverletzungen zum Teil auf wiederkehrende organisatorische oder menschliche Fehler zurückzuführen sind. Den größten Anteil bilden Fehlversendungen personenbezogener Daten per E-Mail oder Post, etwa durch die Verwendung falscher Empfänger, veralteter Verteiler oder eine fehlerhafte Nutzung von E-Mail-Verteilerfunktionen.

Weitere häufige Ursachen waren fehlerhafte Zugriffs- und Berechtigungskonzepte, der Verlust von Unterlagen oder IT-Geräten, unzulässige Datenweitergaben sowie Fehler bei der Einholung oder Nutzung datenschutzrechtlicher Einwilligungen. Daneben beschäftigten die Datenschutzaufsicht Vorfälle im Zusammenhang mit

Auftragsverarbeitern, der unerlaubten Nutzung privater Endgeräte oder Messenger-Dienste für dienstliche Zwecke sowie der unzulässigen Veröffentlichung von Foto- und Videoaufnahmen.

Zunehmend treten darüber hinaus Datenschutzverletzungen auf, deren Ursache in Cyberangriffen oder sonstigen IT-Sicherheitsvorfällen liegt. Hierzu zählen insbesondere Schadsoftware, Angriffe auf IT-Dienstleister oder unbefugte Zugriffe auf IT-Systeme. Diese Entwicklung verdeutlicht, dass Datenschutz und Informationssicherheit heute enger miteinander verbunden sind als je zuvor.

Die Erfahrungen aus den gemeldeten Vorfällen zeigen zugleich, dass erfolgreiche Angriffe häufig durch unzureichende technische Schutzmaßnahmen begünstigt oder erleichtert werden. Insbesondere werden Cloud-Dienste und Fernzugänge noch nicht durchgängig durch eine verpflichtende Multifaktorauthentifizierung abgesichert. Gerade bei extern erreichbaren IT-Systemen stellt eine konsequent eingesetzte Multifaktorauthentifizierung inzwischen einen wesentlichen Baustein zur Verringerung des Risikos unbefugter Zugriffe dar.

> Die meisten Datenschutzverletzungen entstehen nicht durch technische Defekte, sondern durch organisatorische Schwachstellen oder menschliche Fehler.

4.2.3 Erkenntnisse für das Datenschutzmanagement

Die gemeldeten Datenschutzverletzungen zeigen, dass sich viele Vorfälle durch geeignete organisatorische und technische Maßnahmen vermeiden oder zumindest in ihren Auswirkungen erheblich begrenzen lassen.

Hierzu gehören insbesondere klare Berechtigungskonzepte, standardisierte Arbeitsabläufe, verbindliche Kontrollmechanismen vor dem Versand personenbezogener Daten, regelmäßige Schulungen der Beschäftigten sowie technische Sicherheitsmaßnahmen wie Mehrfaktor-Authentifizierung, aktuelle Datensicherungskonzepte und ein wirksames Berechtigungsmanagement.

Gerade Cyberangriffe der vergangenen Jahre machen deutlich, dass Datenschutz ohne Informationssicherheit nicht wirksam gewährleistet werden kann. Datenschutzmanagement und Informationssicherheitsmanagement müssen daher zunehmend gemeinsam gedacht und organisatorisch aufeinander abgestimmt werden.

4.2.4 Meldeverhalten der Verantwortlichen

Die Auswertung der Meldungen zeigt zugleich, dass die Verantwortlichen ihrer gesetzlichen Meldepflicht zunehmend mit der gebotenen Sorgfalt nachkommen. Im Berichtsjahr gingen auch einzelne Meldungen ein, bei denen sich nach der Prüfung herausstellte, dass die datenschutzrechtliche Verantwortung nicht bei der meldenden Einrichtung lag. Ursache der Vorfälle waren beispielsweise Fehler eines Auftragsverarbeiters, datenschutzrechtliche Verantwortlichkeiten anderer Stellen oder eigenmächtige Handlungen einzelner Beschäftigter außerhalb des Verantwortungsbereichs des Verantwortlichen.

Die Datenschutzaufsicht bewertet auch diese Meldungen ausdrücklich positiv. Verantwortliche stehen im Zeitpunkt einer Datenschutzverletzung häufig unter erheblichem Zeitdruck und müssen kurzfristig beurteilen, ob eine Meldepflicht besteht. Eine sorgfältige Meldung im Zweifelsfall entspricht dem Schutzzweck des Gesetzes und ermöglicht der Datenschutzaufsicht eine sachgerechte rechtliche Einordnung. Das Unterlassen einer erforderlichen Meldung wiegt regelmäßig schwerer als eine Meldung, die sich nachträglich als nicht erforderlich erweist.

Hinzu kommt, dass zum Zeitpunkt der Meldung einer Datenschutzverletzung häufig noch nicht alle für die rechtliche Bewertung erforderlichen Informationen vorliegen. Umfang und Ursachen eines Vorfalls lassen sich vielfach erst im Rahmen der weiteren technischen und organisatorischen Aufarbeitung zuverlässig feststellen. Verantwortliche sind deshalb nicht gehalten, bereits mit der Erstmeldung sämtliche Einzelheiten abschließend darzustellen. Vielmehr können neue Erkenntnisse und ergänzende Informationen im weiteren Verlauf des Verfahrens jederzeit nachgereicht werden. Die frühzeitige Meldung eines Vorfalls und die anschließende konti-

nuierliche Ergänzung des Sachverhalts entsprechen regelmäßig dem gesetzlichen Leitbild und ermöglichen eine sachgerechte Begleitung durch die Datenschutzaufsicht.

Die Entwicklung zeigt, dass sich in den kirchlichen Einrichtungen zunehmend eine verantwortungsbewusste Meldekultur etabliert. Dies trägt wesentlich dazu bei, Datenschutzverletzungen transparent aufzuarbeiten und aus ihnen Erkenntnisse für die weitere Verbesserung des Datenschutzmanagements zu gewinnen.

> Eine Meldung im Zweifel ist Ausdruck einer verantwortungsvollen Datenschutzkultur und ermöglicht eine rechtssichere Bewertung durch die Datenschutzaufsicht.

4.2.5 Meldepflicht und Dokumentationspflicht

Nicht jede Datenschutzverletzung ist zugleich meldepflichtig. Das KDG verpflichtet Verantwortliche vielmehr dazu, im Einzelfall zu prüfen, ob die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Erst wenn diese gesetzlichen Voraussetzungen vorliegen, besteht eine Verpflichtung zur Meldung an die Datenschutzaufsicht.

Diese rechtliche Bewertung ist in der Praxis häufig anspruchsvoll. Insbesondere unmittelbar nach Bekanntwerden eines Vorfalls liegen oftmals noch nicht alle erforderlichen Informationen vor, sodass die Risikobewertung unter erheblichem Zeitdruck erfolgen muss. Die Entscheidung darüber, ob eine Meldung erfolgt oder nicht, trifft ausschließlich der Verantwortliche. Sie gehört zu seiner originären datenschutzrechtlichen Verantwortung und kann weder auf den betrieblichen Datenschutzbeauftragten noch auf die Datenschutzaufsicht übertragen werden.

Ebenso wichtig wie die Entscheidung für eine Meldung ist die Dokumentation einer Entscheidung gegen eine Meldung. Das KDG verpflichtet Verantwortliche, auch nicht meldepflichtige Datenschutzverletzungen nachvollziehbar zu dokumentieren. Im Rahmen von Audits und Prüfungen legt das KDSZ Bayern daher regelmäßig besonderes Augenmerk auf diese Dokumentation. Dabei wird insbesondere

geprüft, ob die Risikobewertung nachvollziehbar vorgenommen wurde und die Entscheidung, von einer Meldung abzusehen, auf einer tragfähigen datenschutzrechtlichen Bewertung beruht.

> Auch nicht meldepflichtige Datenschutzverletzungen sind zu dokumentieren.

Eine sorgfältige Dokumentation dient nicht nur dem gesetzlichen Nachweis. Sie unterstützt die Einrichtungen zugleich dabei, vergleichbare Vorfälle künftig einheitlich zu bewerten und ihre internen Meldeprozesse kontinuierlich weiterzuentwickeln.

4.2.6 Information der betroffenen Personen

Neben der Meldepflicht gegenüber der Datenschutzaufsicht stellt sich regelmäßig die Frage, ob auch die von einer Datenschutzverletzung betroffenen Personen informiert werden müssen. Diese Verpflichtung ist von der Meldepflicht zu unterscheiden und folgt eigenen gesetzlichen Voraussetzungen. Maßgeblich ist, ob die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen begründet.

Die Bearbeitung der im Berichtsjahr eingegangenen Datenschutzverletzungen hat gezeigt, dass Verantwortliche die Voraussetzungen dieser Informationspflicht teilweise zurückhaltender beurteilen als die Datenschutzaufsicht. In einer Reihe von Verfahren gelangte das KDSZ Bayern nach Prüfung des Einzelfalls zu der Auffassung, dass eine Information der Betroffenen erforderlich war. In den überwiegenden Fällen folgten die Verantwortlichen dieser rechtlichen Bewertung und informierten die Betroffenen freiwillig. Dies zeigt, dass ein fachlicher Dialog häufig geeignet ist, datenschutzkonforme Lösungen zu erreichen. Nur in Einzelfällen war es erforderlich, auf die Möglichkeit aufsichtsrechtlicher Maßnahmen hinzuweisen oder deren Erlass in Aussicht zu stellen.

Mit der Novellierung des KDG wurde die Rechtslage in diesem Bereich zugleich präzisiert. Nach § 47 Abs. 2 Buchst. e KDG kann die Datenschutzaufsicht nun ausdrücklich anordnen, dass betroffene Personen über eine Datenschutzverletzung zu

benachrichtigen sind. Diese Befugnis besteht unabhängig davon, ob die Datenschutzaufsicht selbst zuvor von einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen ausgegangen ist. Die gesetzliche Klarstellung stärkt die Handlungsmöglichkeiten der Datenschutzaufsicht und schafft zugleich mehr Rechtssicherheit für Verantwortliche bei der Umsetzung ihrer Informationspflichten.

Die Information der Betroffenen ist kein bloßer Formalismus. Sie ermöglicht es den Betroffenen, geeignete Schutzmaßnahmen zu ergreifen, etwa Zugangsdaten zu ändern, erhöhte Aufmerksamkeit gegenüber Betrugsversuchen walten zu lassen oder weitere Vorkehrungen zu treffen. Die transparente Information der Betroffenen ist daher ein wesentlicher Bestandteil eines verantwortungsvollen Umgangs mit Datenschutzverletzungen und trägt maßgeblich zur Vertrauensbildung bei.

> Die Information betroffener Personen dient nicht nur der Erfüllung gesetzlicher Pflichten. Sie ermöglicht den Betroffenen, eigene Schutzmaßnahmen zu ergreifen und weitere Schäden zu vermeiden.

4.2.7 Entwicklung des Meldegeschehens

Das Meldegeschehen bewegte sich im Berichtsjahr insgesamt auf einem weiterhin hohen Niveau. Langfristig ist eine kontinuierliche Zunahme der Meldungen festzustellen. Das außergewöhnlich hohe Meldeaufkommen des Vorjahres war jedoch maßgeblich auf einen einzelnen Sicherheitsvorfall bei einem von zahlreichen kirchlichen Einrichtungen gemeinsam genutzten externen Dienstleister zurückzuführen. Dieser führte zu einer Vielzahl gleichgelagerter Meldungen und stellt insoweit einen statistischen Sondereffekt dar.

Bereinigt um dieses außergewöhnliche Ereignis bestätigt sich der bereits seit mehreren Jahren erkennbare Trend eines moderat steigenden Meldeaufkommens. Diese Entwicklung ist nicht ausschließlich Ausdruck einer höheren Zahl datenschutzrechtlicher Vorfälle. Sie verdeutlicht vielmehr auch das gestiegene Bewusstsein der Verantwortlichen für ihre gesetzlichen Meldepflichten sowie die zunehmende Professionalisierung des Datenschutzmanagements in den kirchlichen Einrichtungen.

Checkliste: Nach einer Datenschutzverletzung

Nach Bekanntwerden einer Datenschutzverletzung sollten Verantwortliche **innerhalb der gesetzlichen Meldefrist von 72 Stunden** insbesondere folgende Punkte prüfen:

- ☑ **Vorfall dokumentieren**
  Zeitpunkt, Sachverhalt und erste Erkenntnisse unverzüglich festhalten.
- ☑ **Risiko bewerten**
  Prüfen, welche Auswirkungen der Vorfall auf die Rechte und Freiheiten der betroffenen Personen haben kann.
- ☑ **Meldepflicht prüfen**
  Bewerten, ob eine Meldung an die Datenschutzaufsicht nach den Vorgaben des KDG erforderlich ist
- ☑ **Information der betroffenen Personen prüfen**
  Sofern ein hohes Risiko für die betroffenen Personen besteht, ist zu prüfen, ob diese unverzüglich informiert werden müssen.
- ☑ **Meldung an die Datenschutzaufsicht**
  Bei Gefahr für die Rechte und Freiheiten der betroffenen Personen:
  Meldung an die Datenschutzaufsicht (Frist: 72 Stunden) und ggf. Information der Betroffenen
- ☑ **Zusammenarbeit mit der Datenschutzaufsicht bei der Aufklärung**
  Information der Aufsicht über getroffene und geplante Maßnahmen sowie über Einschaltung externer Stellen, Weiterleitung von Incident Reports
- ☑ **Ursachen analysieren**
  Organisatorische, technische oder menschliche Ursachen des Vorfalls ermitteln.
- ☑ **Verbesserungsmaßnahmen umsetzen**
  Geeignete organisatorische und technische Maßnahmen ergreifen, um vergleichbare Vorfälle künftig zu vermeiden.

4.2.8 Beispiele aus der Praxis

Die im Jahr 2025 bearbeiteten Datenschutzverletzungen verdeutlichen, wie vielfältig die Ursachen datenschutzrechtlicher Vorfälle sein können. Die nachfolgenden anonymisierten Beispiele zeigen typische Fallkonstellationen aus der Aufsichtspraxis und sollen zugleich für vergleichbare Risiken sensibilisieren.

Unzureichende Zugriffsberechtigungen und interne Meldewege

Im Berichtsjahr wurde bekannt, dass personenbezogene Daten über einen längeren Zeitraum auf einem gemeinsam genutzten Netzlaufwerk abgelegt wurden, auf das deutlich mehr Beschäftigte Zugriff hatten als für die Erfüllung ihrer dienstlichen Aufgaben erforderlich war. Die datenschutzrechtliche Problematik war innerhalb der Organisation bereits mehrfach erkannt worden. Hinweise der IT führten jedoch zunächst weder zu einer vollständigen technischen Behebung des Problems noch zu einer datenschutzrechtlichen Bewertung und Meldung an den zuständigen Datenschutzkoordinator. Erst im Rahmen eines späteren internen Vorgangs wurde die Datenschutzverletzung erkannt und der Datenschutzaufsicht gemeldet.

Der Vorfall verdeutlicht, dass Datenschutzverletzungen häufig nicht allein auf technische Schwachstellen zurückzuführen sind. Ebenso entscheidend sind funktionierende interne Meldewege, klare Verantwortlichkeiten und ein wirksames Datenschutzmanagement. Sicherheitsrelevante Hinweise müssen zeitnah an die zuständigen Stellen weitergeleitet, datenschutzrechtlich bewertet und erforderlichenfalls unverzüglich der Datenschutzaufsicht gemeldet werden. Ebenso zeigt der Fall die Bedeutung regelmäßig überprüfter Berechtigungskonzepte und des Grundsatzes, dass Beschäftigte ausschließlich auf diejenigen personenbezogenen Daten Zugriff erhalten sollten, die sie für die Wahrnehmung ihrer Aufgaben tatsächlich benötigen.

Cyberangriff mit Schadsoftware

Nach einem Cyberangriff auf eine kirchliche Einrichtung wurden mehrere IT-Systeme verschlüsselt. Nach derzeitigem Erkenntnisstand gelangte die Schadsoftware über einen Arbeitsplatzrechner in das Netzwerk und nutzte vorhandene Zugriffsberechtigungen, um einen zentralen Server zu verschlüsseln. Betroffen waren insbesondere Systeme mit personenbezogenen Daten aus der Finanzverwaltung. Ob es neben der Verschlüsselung auch zu einem Abfluss personenbezogener Daten gekommen war, ließ sich zunächst nicht mit letzter Sicherheit ausschließen.

Unmittelbar nach Bekanntwerden des Vorfalls wurden die betroffenen Systeme vom Netzwerk getrennt, interne und externe IT-Fachkräfte mit der Analyse beauftragt sowie die Strafverfolgungsbehörden eingeschaltet. Parallel hierzu erfolgte die datenschutzrechtliche Bewertung des Vorfalls und die Prüfung der Melde- und Informationspflichten.

Der Vorfall verdeutlicht, dass Cyberangriffe regelmäßig nicht nur die Verfügbarkeit von IT-Systemen beeinträchtigen, sondern zugleich erhebliche datenschutzrechtliche Fragestellungen aufwerfen. Er zeigt die Bedeutung aktueller Datensicherungen, einer konsequenten Netzsegmentierung sowie wirksamer Schutzmaßnahmen für Fernzugriffe und privilegierte Benutzerkonten. Ebenso wird deutlich, dass organisatorische Notfallkonzepte und ein abgestimmtes Vorgehen zwischen IT, Informationssicherheit, Datenschutz und Strafverfolgungsbehörden wesentliche Voraussetzungen für eine wirksame Bewältigung solcher Vorfälle sind.

Cyberangriff auf eine soziale Einrichtung

Eine große kirchliche Sozialeinrichtung wurde im Berichtsjahr Ziel eines Angriffs mit einem Kryptotrojaner. Nach der Entdeckung des Vorfalls wurden sämtliche Server und Arbeitsplatzsysteme unverzüglich vom Netzwerk getrennt, um eine weitere Ausbreitung der Schadsoftware zu verhindern. Parallel hierzu wurden Passwörter, insbesondere privilegierte Administratorkonten, geändert und die IT-Systeme aus vorhandenen Datensicherungen wiederhergestellt. Da zunächst nicht ausge-

schlossen werden konnte, dass personenbezogene Daten abgeflossen waren, wurde der Vorfall der Datenschutzaufsicht gemeldet und zugleich ein spezialisiertes IT-Forensikunternehmen mit der Untersuchung beauftragt. Darüber hinaus wurden die Strafverfolgungsbehörden eingeschaltet.

Der Vorfall verdeutlicht die Bedeutung einer sorgfältigen Vorbereitung auf IT-Sicherheitsvorfälle. Neben aktuellen Datensicherungen und einem erprobten Notfallmanagement kommt insbesondere der schnellen Reaktion nach der Entdeckung eines Angriffs eine entscheidende Rolle zu. Ebenso zeigt der Fall, dass Datenschutzverletzungen infolge von Cyberangriffen regelmäßig eine enge Zusammenarbeit zwischen IT, Informationssicherheit, Datenschutzaufsicht, externen Forensikern und Strafverfolgungsbehörden erfordern. Die aus der Untersuchung gewonnenen Erkenntnisse wurden zum Anlass genommen, weitere Sicherheitsmaßnahmen umzusetzen, darunter die Überprüfung von Berechtigungskonzepten, die Einführung einer verpflichtenden Mehrfaktorauthentifizierung sowie zusätzliche Sensibilisierungsmaßnahmen für die Beschäftigten.

Kompromittierung einer öffentlich erreichbaren Webseite

Bei einer kirchlichen Einrichtung wurde die Internetseite Ziel eines Angriffs. Der Hosting-Dienstleister stellte ein ungewöhnliches Versandverhalten fest und sperrte vorsorglich den E-Mail-Versand des betroffenen Webspaces. Die Einrichtung reagierte umgehend und nahm die Webseite außer Betrieb, um eine weitere missbräuchliche Nutzung zu verhindern. Hinweise auf einen Abfluss personenbezogener Daten lagen nach derzeitigem Erkenntnisstand nicht vor.

Der Vorfall verdeutlicht, dass auch öffentlich erreichbare Internetauftritte regelmäßig Ziel automatisierter Angriffe werden können. Neben einer zeitnahen Aktualisierung der eingesetzten Software und einer sicheren Konfiguration der Systeme kommt der kontinuierlichen Überwachung sowie einer engen Zusammenarbeit zwischen Verantwortlichen, Systemadministration und Hosting-Dienstleistern besondere Bedeutung zu. Ebenso zeigt der Fall, dass ein schnelles und abge-

stimmtes Vorgehen dazu beitragen kann, mögliche Auswirkungen eines Sicherheitsvorfalls wirksam zu begrenzen.

Einbruch in Verwaltungsräume

Im Berichtsjahr wurde in die Büroräume einer kirchlichen Verwaltung eingebrochen. Neben Sachschäden und der Entwendung von Bargeld bestand insbesondere die Frage, ob unbefugte Dritte Einsicht in personenbezogene Unterlagen oder vertrauliche Dokumente genommen hatten. Zwar konnten keine konkreten Hinweise auf einen Abfluss personenbezogener Daten festgestellt werden, eine Kenntnisnahme sensibler Informationen ließ sich jedoch nicht mit letzter Sicherheit ausschließen. Der Vorfall wurde deshalb vorsorglich der Datenschutzaufsicht gemeldet und parallel den Strafverfolgungsbehörden angezeigt.

Der Fall verdeutlicht, dass Datenschutz nicht ausschließlich eine Frage der IT-Sicherheit ist. Auch der Schutz papiergebundener Unterlagen, die Absicherung besonders sensibler Arbeitsbereiche sowie organisatorische und bauliche Sicherheitsmaßnahmen gehören zu einem wirksamen Datenschutzmanagement. Ebenso zeigt der Vorfall, dass bereits der begründete Verdacht einer unbefugten Kenntnisnahme personenbezogener Daten eine sorgfältige datenschutzrechtliche Bewertung erfordert, selbst wenn sich ein tatsächlicher Datenabfluss später nicht nachweisen lässt.

Zweckwidrige Nutzung einer Videoüberwachungsanlage

Anlass der Meldung war, dass eine vorhandene Videoanlage entgegen ihrem vorgesehenen Zweck genutzt wurde, um einen Beschäftigten während seiner Tätigkeit abzubilden und die Aufnahme anschließend an eine vorgesetzte Stelle weiterzuleiten. Der Vorfall wurde der Datenschutzaufsicht gemeldet und datenschutzrechtlich überprüft.

Im Rahmen der Prüfung wurde deutlich, dass Videoüberwachung ausschließlich zu den hierfür festgelegten und rechtlich zulässigen Zwecken eingesetzt werden darf. Eine Nutzung zur Beobachtung oder Kontrolle von Beschäftigten ist grundsätzlich

unzulässig, sofern hierfür keine besondere gesetzliche Grundlage besteht. Die verantwortliche Einrichtung wurde deshalb erneut auf die Zweckbindung der Videoüberwachung sowie die datenschutzrechtlichen Anforderungen an deren Betrieb hingewiesen und stellte sicher, dass künftig keine entsprechenden Aufnahmen mehr erfolgen.

4.2.9 Lessons Learned – Aus Fehlern lernen

Jede Datenschutzverletzung bietet die Möglichkeit, bestehende Prozesse zu überprüfen und daraus Erkenntnisse für die Weiterentwicklung des Datenschutzmanagements zu gewinnen. Ziel der Datenschutzaufsicht ist es daher nicht allein, einzelne Vorfälle datenschutzrechtlich zu bewerten, sondern wiederkehrende Ursachen zu erkennen und daraus Empfehlungen für alle kirchlichen Einrichtungen abzuleiten.

Die Erfahrungen des Berichtsjahres zeigen erneut, dass Datenschutzverletzungen häufig auf organisatorische Schwachstellen oder unzureichend etablierte Arbeitsabläufe zurückzuführen sind. Ein wirksames Datenschutzmanagement zeichnet sich deshalb nicht dadurch aus, dass Datenschutzverletzungen vollständig ausgeschlossen werden können. Entscheidend ist vielmehr, dass Vorfälle systematisch aufgearbeitet, geeignete Verbesserungsmaßnahmen umgesetzt und die gewonnenen Erkenntnisse dauerhaft in die Organisation einfließen.

Die Erkenntnisse aus den gemeldeten Datenschutzverletzungen fließen deshalb kontinuierlich in die Beratungstätigkeit, die Entwicklung von Orientierungshilfen und Handreichungen sowie in die Audit- und Prüftätigkeit des KDSZ Bayern ein. Datenschutzverletzungen sind damit nicht nur Anlass für aufsichtsrechtliches Handeln, sondern zugleich Motor für die Weiterentwicklung des Datenschutzes. Aus den Erfahrungen einzelner Einrichtungen entstehen so Handlungsempfehlungen, die allen kirchlichen Verantwortlichen zugutekommen und dazu beitragen, vergleichbare Vorfälle künftig möglichst zu vermeiden.

4.3 Beschwerden

Das Recht, sich an die Datenschutzaufsicht zu wenden, gehört zu den wesentlichen Betroffenenrechten des kirchlichen Datenschutzrechts. Es gewährleistet, dass jede betroffene Person datenschutzrechtliche Sachverhalte unabhängig überprüfen lassen kann, wenn sie sich in ihren Rechten verletzt sieht. Beschwerden leisten damit einen wichtigen Beitrag zur Durchsetzung des Datenschutzrechts und ermöglichen zugleich eine unabhängige Kontrolle der Datenverarbeitung in den kirchlichen Einrichtungen.

Für die Datenschutzaufsicht stellen Beschwerden darüber hinaus eine wichtige Erkenntnisquelle dar. Sie zeigen auf, in welchen Bereichen Unsicherheiten bei der Anwendung des Datenschutzrechts bestehen und welche Fragestellungen die Betroffenen besonders beschäftigen. Nicht selten können Beschwerden bereits durch eine sachliche rechtliche Einordnung oder durch die Vermittlung zwischen den Beteiligten einvernehmlich geklärt werden.

Beschwerdeschwerpunkte 2025

Die im Berichtsjahr eingegangenen Beschwerden betrafen insbesondere:

- ☑ Verarbeitung und Weitergabe personenbezogener Daten
- ☑ Auskunftsansprüche betroffener Personen
- ☑ Veröffentlichung von Bild- und Personendaten
- ☑ Beschäftigtendatenschutz
- ☑ Elektronische Kommunikation

Beschwerden leisten einen wichtigen Beitrag zur Fortentwicklung der Datenschutzpraxis und geben Hinweise auf Bereiche mit besonderem Beratungs- und Unterstützungsbedarf.

4.3.1 Schwerpunkte des Beschwerdegeschehens

Die Beschwerden des Berichtsjahres betrafen überwiegend die Verarbeitung und Weitergabe personenbezogener Daten. Im Mittelpunkt standen insbesondere die Rechtmäßigkeit von Datenübermittlungen innerhalb kirchlicher Strukturen sowie an andere kirchliche oder externe Stellen. Ebenso wurden wiederholt Fragen zur Wirksamkeit datenschutzrechtlicher Einwilligungen und zu den Voraussetzungen einer zulässigen Datenverarbeitung aufgeworfen.

Häufig betrafen die Beschwerden die unzureichende Erfüllung datenschutzrechtlicher Auskunftsansprüche. Betroffene beanstandeten insbesondere ausbleibende oder verspätete Antworten sowie den Umfang der erteilten Auskünfte, vor allem, wenn Unterlagen zum Schutz von Rechten Dritter geschwärzt wurden. Die Auswertung der Verfahren zeigt, dass eine frühzeitige Kommunikation und eine sorgfältige Bearbeitung von Betroffenenanfragen wesentlich dazu beitragen können, Beschwerden bereits im Vorfeld zu vermeiden.

Daneben beschäftigten die Datenschutzaufsicht weiterhin Beschwerden im Zusammenhang mit der Veröffentlichung personenbezogener Daten und Bildaufnahmen sowie vereinzelt Fragestellungen aus dem Beschäftigtendatenschutz und der elektronischen Kommunikation.

4.3.2 Entwicklung des Beschwerdegeschehens

Das Beschwerdeaufkommen ist gegenüber den Vorjahren erneut deutlich angestiegen. Diese Entwicklung ist jedoch nicht allein Ausdruck einer größeren Zahl datenschutzrechtlicher Konflikte. Sie zeigt zugleich, dass die Datenschutzaufsicht als unabhängige Anlaufstelle zunehmend bekannt ist und betroffene Personen ihre gesetzlichen Rechte häufiger wahrnehmen.

Mit der steigenden Zahl der Beschwerden hat sich zugleich deren Komplexität verändert. Während in den vergangenen Jahren häufig einzelne datenschutzrechtliche Fragestellungen im Mittelpunkt standen, betreffen Beschwerden heute zunehmend umfangreichere Sachverhalte mit mehreren Beteiligten und komplexen

organisatorischen oder technischen Zusammenhängen. Dies führt regelmäßig zu einem höheren Prüfungs- und Abstimmungsaufwand sowohl bei den Verantwortlichen als auch bei der Datenschutzaufsicht.

> Der Anstieg der Beschwerden zeigt nicht nur eine höhere Inanspruchnahme der Datenschutzaufsicht. Er verdeutlicht zugleich, dass Betroffene ihre datenschutzrechtlichen Rechte zunehmend kennen und wahrnehmen.

4.3.3 Erkenntnisse aus den Beschwerden

Die Auswertung der Beschwerden bestätigt erneut, dass viele Konflikte durch transparente Kommunikation und klar geregelte interne Verfahren vermieden werden können. Insbesondere die zeitnahe Bearbeitung von Betroffenenanfragen, nachvollziehbare Entscheidungen sowie eine sorgfältige Prüfung der datenschutzrechtlichen Rechtsgrundlagen tragen wesentlich dazu bei, Beschwerden bereits im Vorfeld zu vermeiden.

Die Erkenntnisse aus den Beschwerdeverfahren fließen deshalb kontinuierlich in die Beratungsarbeit, die Entwicklung von Orientierungshilfen sowie in die Audit- und Prüftätigkeit des KDSZ Bayern ein. Beschwerden dienen damit nicht allein der Klärung individueller Sachverhalte. Sie liefern zugleich wichtige Hinweise auf wiederkehrende Fragestellungen und tragen dazu bei, die Datenschutzpraxis in den kirchlichen Einrichtungen kontinuierlich weiterzuentwickeln.

4.3.4 Praxisbeispiele

Die folgenden Fallbeispiele beruhen auf tatsächlichen Beschwerdeverfahren des Berichtsjahres. Sie wurden anonymisiert und teilweise redaktionell zusammengefasst. Ziel ist es, typische datenschutzrechtliche Fragestellungen zu veranschaulichen und Hinweise für vergleichbare Fallgestaltungen zu geben.

Auskunfts- und Löschungsansprüche im Zusammenhang mit einer Taufe

Ein Elternteil beschwerte sich beim KDSZ Bayern darüber, dass ein kirchlicher Verantwortlicher seinem datenschutzrechtlichen Auskunfts- und Löschungsverlangen im Zusammenhang mit der Taufe seines Kindes nicht vollständig nachgekommen sei. Im Verlauf des Beschwerdeverfahrens waren insbesondere die jeweiligen Sorgerechtsverhältnisse zum Zeitpunkt der Taufe sowie zum Zeitpunkt der Antragstellung zu berücksichtigen.

Im Rahmen der datenschutzrechtlichen Prüfung wurde der Verantwortliche um ergänzende Stellungnahme gebeten und die Auskunft gegenüber dem Beschwerdeführer vervollständigt. Darüber hinaus war zu prüfen, inwieweit kirchenrechtliche Vorschriften über die Führung kirchlicher Register einer Löschung personenbezogener Daten entgegenstehen. Der Fall verdeutlicht, dass Betroffenenrechte sorgfältig mit spezialgesetzlichen Regelungen des kirchlichen Rechts in Einklang zu bringen sind und eine differenzierte rechtliche Prüfung des jeweiligen Einzelfalls erfordern.

Einwilligungen für Foto- und Filmaufnahmen

Beanstandet wurde die datenschutzrechtliche Ausgestaltung einer Einwilligungserklärung für Foto- und Filmaufnahmen im Rahmen einer kirchlichen Veranstaltung. Beanstandet wurden insbesondere die fehlende Differenzierung zwischen verschiedenen Verarbeitungszwecken, unzureichende Informationen über die Datenverarbeitung sowie die Frage, ob die Einwilligung den gesetzlichen Anforderungen an Freiwilligkeit und Transparenz genügte.

Im Rahmen des Beschwerdeverfahrens wurden die Einwilligungserklärung und die zugrunde liegenden Informationsunterlagen datenschutzrechtlich überprüft. Dabei standen insbesondere die Anforderungen an eine informierte und freiwillige Einwilligung, die Möglichkeit einer differenzierten Auswahl einzelner Nutzungszwecke sowie die Erfüllung der gesetzlichen Informationspflichten im Mittelpunkt. Der Fall verdeutlicht, dass Einwilligungserklärungen nicht lediglich formalen Anforderungen genügen müssen, sondern den betroffenen Personen eine selbstbestimmte und

nachvollziehbare Entscheidung über die Verwendung ihrer personenbezogenen Daten ermöglichen sollen. Dies gilt insbesondere dann, wenn Bildaufnahmen von Kindern und Jugendlichen oder andere besonders schutzwürdige personenbezogene Daten betroffen sind.

Zweckbindung bei Kontaktdaten

Ein Angehöriger rügte die Nutzung seiner im Rahmen einer stationären Aufnahme im Krankenhaus hinterlegten Telefonnummer für einen anderen als den ursprünglich angegebenen Zweck. Die Rufnummer war zur Erreichbarkeit bei medizinischen Rückfragen angegeben worden. Im weiteren Verlauf wurde sie von der Einrichtung genutzt, um den Angehörigen wegen organisatorischer und verwaltungstechnischer Angelegenheiten zu kontaktieren. Der Beschwerdeführer sah hierin eine zweckwidrige Verwendung seiner personenbezogenen Daten.

Im Rahmen des Beschwerdeverfahrens war insbesondere zu prüfen, zu welchem Zweck die Telefonnummer erhoben worden war, auf welcher Rechtsgrundlage eine weitergehende Nutzung erfolgen konnte und ob die Verwendung noch vom ursprünglichen Erhebungszweck gedeckt war. Der Fall verdeutlicht die praktische Bedeutung des Grundsatzes der Zweckbindung. Personenbezogene Daten dürfen grundsätzlich nur für diejenigen Zwecke verwendet werden, für die sie erhoben wurden, soweit nicht eine gesetzliche Grundlage oder ein anderer datenschutzrechtlicher Erlaubnistatbestand eine weitergehende Verarbeitung rechtfertigt. Eine transparente Kommunikation gegenüber den betroffenen Personen trägt wesentlich dazu bei, Missverständnisse und Beschwerden zu vermeiden.

Kommunikationswege und Datensicherheit

Im Mittelpunkt dieser Beschwerde stand die datenschutzgerechte Ausgestaltung der elektronischen Kommunikation mit einer kirchlichen Behörde. Beanstandet wurde insbesondere, dass Anfragen künftig regelmäßig auf elektronischem Weg gestellt werden sollten und hierfür bereits bei der ersten Kontaktaufnahme personenbezogene Daten erforderlich waren. Der Beschwerdeführer äußerte daten-

schutzrechtliche Bedenken hinsichtlich der Sicherheit der Datenübermittlung und der angebotenen Kommunikationswege.

Im Rahmen des Beschwerdeverfahrens wurde insbesondere geprüft, welche Kommunikationswege tatsächlich zur Verfügung standen, ob die betroffenen Personen oder deren Bevollmächtigte zwischen verschiedenen Übermittlungswegen wählen konnten und welche technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten vorgesehen waren. Dabei war auch zu berücksichtigen, dass die elektronische Kommunikation lediglich eine zusätzliche Serviceleistung darstellte und daneben weitere, datenschutzgerechte Übermittlungswege zur Verfügung standen.

Der Fall verdeutlicht, dass bei der Einführung neuer Kommunikationsverfahren neben den Anforderungen an die Datensicherheit auch eine klare und verständliche Information über die verfügbaren Kommunikationswege von wesentlicher Bedeutung ist. Transparente Hinweise auf alternative Übermittlungswege und vorhandene sichere Kommunikationsmöglichkeiten können dazu beitragen, datenschutzrechtliche Bedenken auszuräumen und das Vertrauen der Nutzerinnen und Nutzer in digitale Verwaltungsverfahren zu stärken.

Auskunft über eine mögliche Datenweitergabe

Anlass dieser Beschwerde war der Verdacht, dass personenbezogene Unterlagen und Kontaktdaten einer ehemaligen Beschäftigten nach Beendigung ihrer Tätigkeit unbefugt eingesehen oder an Dritte weitergegeben worden sein könnten. Anlass der Beschwerde waren anonyme Zusendungen, die den Schluss zuließen, dass Dritte Kenntnis von zuvor ausschließlich intern aufbewahrten Unterlagen erlangt haben könnten. Zugleich machte die betroffene Person von ihrem datenschutzrechtlichen Auskunftsrecht Gebrauch und begehrte insbesondere Auskunft über mögliche Empfänger ihrer personenbezogenen Daten sowie über deren Verarbeitung innerhalb der Einrichtung.

Im Rahmen des Beschwerdeverfahrens war insbesondere zu prüfen, ob Anhaltspunkte für eine unzulässige Offenlegung personenbezogener Daten vorlagen, welche Verarbeitungsvorgänge innerhalb der Einrichtung nachvollzogen werden konnten und in welchem Umfang der Auskunftsanspruch auch Angaben zu möglichen Datenempfängern umfasst. Der Fall verdeutlicht die Bedeutung einer nachvollziehbaren Dokumentation von Datenzugriffen sowie eines wirksamen Berechtigungs- und Dokumentenmanagements. Nur wenn Verarbeitungsvorgänge und Zugriffsberechtigungen hinreichend dokumentiert sind, können Verantwortliche Auskunftsersuchen sachgerecht beantworten und mögliche Datenschutzverstöße wirksam aufklären.

Fehlzustellung personenbezogener Unterlagen

Beanstandet wurde die Übersendung eines Schreibens an eine unbeteiligte Person mit gleichem Namen. Aufgrund der Fehlzustellung wurden personenbezogene Daten, darunter steuerliche Informationen sowie weitere vertrauliche Angaben, einer nicht empfangsberechtigten Dritten bekannt.

Im Rahmen des Beschwerdeverfahrens war insbesondere zu prüfen, welche organisatorischen Ursachen zu der Fehlzustellung geführt hatten, welche personenbezogenen Daten betroffen waren und welche Maßnahmen der Verantwortliche zur Vermeidung vergleichbarer Vorfälle ergriffen hatte. Darüber hinaus war zu bewerten, ob die gesetzlichen Anforderungen an den Umgang mit der festgestellten Datenschutzverletzung eingehalten worden waren.

Der Fall verdeutlicht, dass bereits scheinbar geringfügige Fehler bei der Identifizierung von Empfängern erhebliche datenschutzrechtliche Auswirkungen haben können. Gerade bei der Verarbeitung sensibler personenbezogener Daten sind eindeutige Identifizierungsmerkmale und sorgfältige Plausibilitätskontrollen unverzichtbar. Organisatorische Maßnahmen zur Vermeidung von Namensverwechslungen leisten daher einen wesentlichen Beitrag zum Schutz personenbezogener Daten.

4.4 Prüfungen und Audits

Prüfungen und Audits gehören zu den gesetzlichen Kernaufgaben der Datenschutzaufsicht. Sie dienen der unabhängigen Überprüfung, ob Verantwortliche und Auftragsverarbeiter die Anforderungen des Gesetzes über den Kirchlichen Datenschutz einhalten und ein wirksames Datenschutzmanagement etabliert haben. Ziel der Datenschutzaufsicht ist dabei nicht die Suche nach einzelnen Verstößen, sondern die nachhaltige Verbesserung datenschutzrechtlicher Strukturen und Prozesse in den kirchlichen Einrichtungen.

Vor diesem Hintergrund hat das KDSZ Bayern im Berichtsjahr seine Auditstrategie grundlegend weiterentwickelt. An die Stelle einer überwiegend anlassbezogenen Prüfung einzelner Sachverhalte tritt zunehmend ein risikoorientierter Prüfungsansatz, der den Blick auf das gesamte Datenschutzmanagement einer Einrichtung richtet. Damit wird die Datenschutzaufsicht ihrer gesetzlichen Aufgabe gerecht, Datenschutz nicht nur zu kontrollieren, sondern zugleich nachhaltig zu fördern und weiterzuentwickeln.

Prüfungsschwerpunkte 2025

Die Audit- und Prüftätigkeit des KDSZ Bayern wurde im Berichtsjahr insbesondere durch folgende Schwerpunkte geprägt:

- ☑ **Risikoorientierter Prüfungsansatz**
- ☑ **Vor-Ort-Audits**
- ☑ **Jahresbesuche in den Ordinariaten**
- ☑ **Auditreihe in der kirchlichen Sozialwirtschaft**
- ☑ **Bistumsweite Webseitenaudits**

Ziel aller Prüfungen ist die nachhaltige Weiterentwicklung des Datenschutzmanagements in den kirchlichen Einrichtungen.

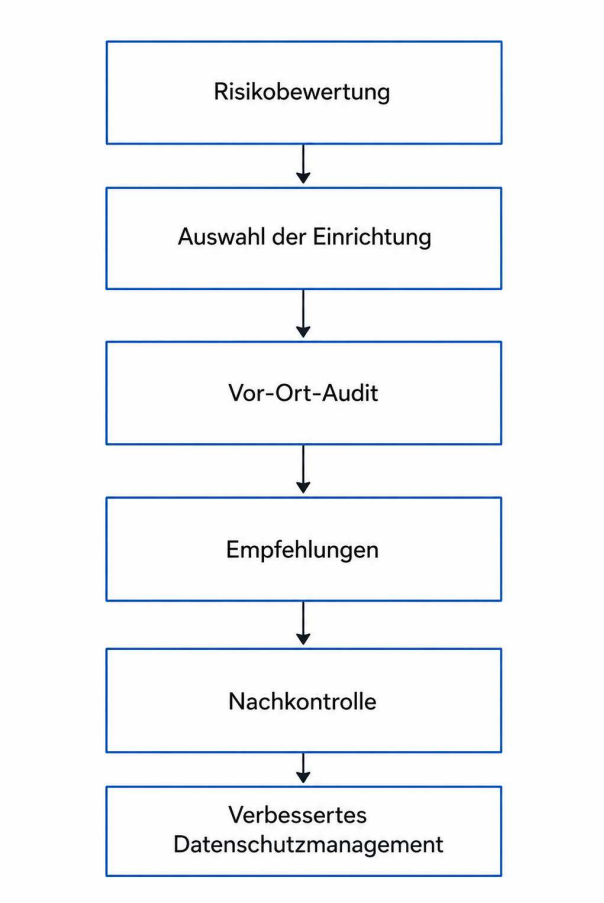
4.4.1 Der risikoorientierte Prüfungsansatz

Die Auswahl der Prüfungen erfolgt nach einem risikoorientierten Ansatz. Maßgeblich sind insbesondere Art, Umfang und Sensibilität der verarbeiteten personenbezogenen Daten sowie die mit der jeweiligen Datenverarbeitung verbundenen Risiken für die Rechte der betroffenen Personen. Einrichtungen mit besonders komplexen Verarbeitungsprozessen oder einem hohen Schutzbedarf stehen dabei stärker im Fokus als Bereiche mit geringem datenschutzrechtlichem Risiko.

Der risikoorientierte Prüfungsansatz ermöglicht einen zielgerichteten und zugleich wirtschaftlichen Einsatz der vorhandenen Ressourcen. Nicht jede Einrichtung benötigt dieselbe Prüftiefe oder denselben Prüfungsumfang. Vielmehr richtet sich die Intensität der Aufsicht nach dem konkreten Datenschutzrisiko und den Besonderheiten der jeweiligen Einrichtung.

Dieser Ansatz verbindet die unabhängige Kontrollfunktion der Datenschutzaufsicht mit ihrem gesetzlichen Beratungsauftrag. Prüfungen dienen nicht allein der Feststellung datenschutzrechtlicher Defizite, sondern sollen den Verantwortlichen zugleich konkrete Hinweise für die Weiterentwicklung ihres Datenschutzmanagements geben. Auf diese Weise entsteht eine Aufsicht, die Kontrolle und Beratung sinnvoll miteinander verbindet und die Einrichtungen bei der Umsetzung datenschutzrechtlicher Anforderungen nachhaltig unterstützt.

> Der Umfang einer Prüfung richtet sich nach dem Datenschutzrisiko. Maßgeblich sind insbesondere Art, Umfang und Sensibilität der Datenverarbeitung sowie die möglichen Auswirkungen auf die Rechte der betroffenen Personen.



Ablauf eines Audits

4.4.2 Vor-Ort-Audits als Instrument moderner Datenschutzaufsicht

Ein wesentlicher Bestandteil dieses Prüfungsansatzes sind strukturierte Vor-Ort-Audits. Sie ermöglichen der Datenschutzaufsicht, das Datenschutzmanagement einer Einrichtung umfassend zu bewerten und dabei sowohl organisatorische als auch technische Rahmenbedingungen in den Blick zu nehmen. Im Mittelpunkt steht nicht die isolierte Betrachtung einzelner Verarbeitungsvorgänge, sondern die Frage, ob Datenschutz dauerhaft und systematisch in den Arbeitsabläufen der Einrichtung verankert ist.

Die Audits umfassen neben einer vorbereitenden Auswertung von angeforderten Unterlagen regelmäßig Gespräche mit Verantwortlichen, betrieblichen Datenschutzbeauftragten und weiteren Beschäftigten, die Prüfung datenschutzrelevan-

ter Dokumentationen sowie die Bewertung technischer und organisatorischer Maßnahmen. Eine gemeinsame Abschlussbesprechung bietet Gelegenheit, die wesentlichen Feststellungen zu erläutern, offene Fragen zu klären und gemeinsam mögliche Verbesserungsmaßnahmen zu erörtern.

Vor-Ort-Audits verstehen sich dabei ausdrücklich nicht als Momentaufnahme einzelner Arbeitsabläufe. Ziel ist vielmehr die Bewertung der bestehenden Organisationsstrukturen und des gelebten Datenschutzmanagements. Dadurch können sowohl bereits etablierte gute Lösungen als auch Optimierungspotenziale identifiziert werden. Die gewonnenen Erkenntnisse bilden zugleich die Grundlage für eine kontinuierliche Weiterentwicklung des Datenschutzes innerhalb der jeweiligen Einrichtung.

4.4.3 Schwerpunkte des Berichtsjahres

Im Berichtsjahr wurden die verschiedenen Prüfungsformate des KDSZ Bayern weiter ausgebaut und aufeinander abgestimmt. Neben klassischen Vor-Ort-Audits wurden neue Formate eingeführt, die einen kontinuierlichen Austausch mit den kirchlichen Einrichtungen ermöglichen und die risikoorientierte Aufsicht sinnvoll ergänzen.

Jahresbesuche in den Ordinariaten

Mit der Gründung des KDSZ Bayern wurde begonnen, alle sieben bayerischen (Erz-)Diözesen im Rahmen von Antrittsbesuchen kennenzulernen. Die Gespräche mit den Generalvikaren dienten dazu, die Datenschutzaufsicht als unabhängigen Ansprechpartner vorzustellen, bestehende Datenschutzstrukturen kennenzulernen und einen regelmäßigen Austausch zu etablieren. Ergänzend hierzu wurden ausgewählte Organisationseinheiten der Ordinariate im Rahmen erster Vor-Ort-Audits geprüft.

Nach den Besuchen in den Ordinariaten von Augsburg, Regensburg, Passau und Würzburg im Jahr 2024 konnten diese Antrittsbesuche im Berichtsjahr mit den

Ordinariaten München und Freising, Eichstätt sowie Bamberg abgeschlossen werden.

Auf Grundlage der bisherigen Erkenntnisse wurde im Berichtsjahr zugleich die Weiterentwicklung dieses Formats vorbereitet. Künftig sollen die bisherigen Antrittsbesuche in regelmäßige Jahresgespräche überführt werden. Der Fokus wird künftig weniger auf der Auditierung einzelner Organisationseinheiten liegen, sondern auf dem kontinuierlichen fachlichen Austausch mit den Generalvikaren, den Verantwortlichen und den betrieblichen Datenschutzbeauftragten. Ziel ist es, aktuelle datenschutzrechtliche Entwicklungen frühzeitig zu begleiten, Erfahrungen auszutauschen und die Umsetzung datenschutzrechtlicher Anforderungen dauerhaft zu unterstützen.

Die ersten Jahresgespräche fanden Anfang 2026 statt und werden Gegenstand des nächsten Tätigkeitsberichts sein.

Auditreihe in der kirchlichen Sozialwirtschaft

Prägend für das Berichtsjahr war zudem der Beginn einer systematischen Auditreihe bei Einrichtungen der kirchlichen Sozialwirtschaft. Ausgangspunkt hierfür war der Informationstag ‚Datenschutz in der katholischen Sozialwirtschaft“, auf dessen Grundlage ein risikoorientiertes Auditkonzept entwickelt wurde.

Im Berichtsjahr wurde dieses Konzept erstmals bei einem Diözesan-Caritasverband sowie ergänzend bei einem großen kirchlichen Träger der Kinder- und Jugendhilfe erprobt. Dabei wurden sowohl die Datenschutzorganisation der Träger als auch ausgewählte Einrichtungen und deren Prozesse in die Prüfung einbezogen.

Die weiteren Audits der bayerischen Diözesan-Caritasverbände werden im Jahr 2026 fortgeführt. Das entwickelte Auditkonzept sowie die hierbei gewonnenen Erkenntnisse werden in einem eigenen Kapitel später ausführlich dargestellt.

Bistumsweite Webseitenaudits

Ein weiteres zentrales Vorhaben war die Entwicklung eines skalierbaren Prüfungsansatzes für eine große Zahl vergleichbarer kirchlicher Einrichtungen. Ausgangspunkt war die systematische Erfassung aller dem KDSZ Bayern unterstehenden Verantwortlichen. Dabei zeigte sich zugleich der tiefgreifende organisatorische Wandel innerhalb der bayerischen (Erz-)Diözesen. Viele Einzelpfarreien wurden in den vergangenen Jahren zu größeren Verwaltungseinheiten, Pfarreiengemeinschaften, Pfarrverbänden oder Seelsorgebereichen zusammengeführt.

Diese neuen Organisationsstrukturen wurden bewusst zum Ausgangspunkt der Prüfungen gewählt. Anstatt sämtliche Internetauftritte der einzelnen Kirchenstiftungen zu prüfen, konzentrierte sich das KDSZ Bayern auf die Webseiten der jeweiligen Verwaltungseinheiten. Dadurch konnte die Zahl der zu prüfenden Internetauftritte erheblich reduziert werden, ohne auf eine flächendeckende Wirkung zu verzichten. Gleichzeitig wurden die Verwaltungseinheiten als Multiplikatoren eingebunden, um festgestellte Mängel innerhalb ihres jeweiligen Zuständigkeitsbereichs weiterzugeben und eine einheitliche Umsetzung datenschutzrechtlicher Anforderungen zu fördern.

Die orientierenden Prüfungen konzentrierten sich bewusst auf zentrale datenschutzrechtliche Transparenzpflichten. Gegenstand der Überprüfung waren insbesondere die Angaben zum Verantwortlichen und zum betrieblichen Datenschutzbeauftragten, die Vollständigkeit und Verständlichkeit der Datenschutzhinweise sowie die korrekte Benennung der zuständigen Datenschutzaufsicht im Zusammenhang mit dem Beschwerderecht. Anlass für diese Schwerpunktsetzung waren wiederkehrende Anfragen betroffener Personen, die auf unklare oder fehlerhafte Angaben in Datenschutzerklärungen zurückzuführen waren.

Im Berichtsjahr wurden die Webseitenaudits in den (Erz-)Diözesen Augsburg, Bamberg, Eichstätt und Passau durchgeführt. Die Prüfungen der Internetauftritte in den (Erz-)Diözesen München und Freising, Regensburg sowie Würzburg werden im Jahr 2026 fortgesetzt. Die Ergebnisse werden den jeweiligen Diözesen in strukturierter Form zur Verfügung gestellt und bilden eine wichtige Grundlage für die weitere

Vereinheitlichung der datenschutzrechtlichen Informationspflichten im gesamten Aufsichtsgebiet.

> Die unterschiedlichen Prüfungsformate verfolgen ein gemeinsames Ziel: Datenschutz frühzeitig in den Organisationsstrukturen der kirchlichen Einrichtungen zu verankern und nachhaltig weiterzuentwickeln.

4.4.4 Empfehlungen statt Beanstandungen

Das KDSZ Bayern versteht Audits in erster Linie als Instrument zur Verbesserung des Datenschutzmanagements. Ziel der Prüfungen ist es daher nicht, einzelne Beanstandungen zu dokumentieren, sondern gemeinsam mit den Verantwortlichen tragfähige und praxistaugliche Lösungen zu entwickeln.

Soweit datenschutzrechtliche Optimierungspotenziale festgestellt werden, stehen Empfehlungen und fachliche Hinweise im Vordergrund. Beanstandungen oder weitergehende aufsichtsrechtliche Maßnahmen bleiben den Fällen vorbehalten, in denen erhebliche oder fortdauernde Verstöße dies erforderlich machen. Ebenso wichtig ist es, bereits gut umgesetzte Datenschutzlösungen sichtbar zu machen und als Beispiele guter Praxis in die weitere Beratungsarbeit einfließen zu lassen.

4.4.5 Nachkontrollen und nachhaltige Umsetzung

Die Wirksamkeit eines Audits bemisst sich nicht allein an den während der Prüfung getroffenen Feststellungen, sondern vor allem an der nachhaltigen Umsetzung der vereinbarten Maßnahmen. Nachkontrollen bilden deshalb einen festen Bestandteil des risikoorientierten Prüfungsansatzes.

Dabei steht weniger die Frage im Vordergrund, ob einzelne Feststellungen formell abgearbeitet wurden. Entscheidend ist vielmehr, ob die Einrichtung ihr Datenschutzmanagement dauerhaft weiterentwickelt, organisatorische Verbesserungen umgesetzt und datenschutzrechtliche Anforderungen nachhaltig in ihre Arbeitsabläufe integriert hat.

Die im Rahmen eines Audits ausgesprochenen Empfehlungen dienen den Verantwortlichen dazu, erkannte Risiken frühzeitig zu beseitigen und datenschutzrechtliche Anforderungen dauerhaft umzusetzen. Werden festgestellte Defizite trotz entsprechender Hinweise nicht behoben und werden diese in späteren Beschwerde-, Prüfungs- oder Datenschutzverletzungsverfahren erneut relevant, kann dies bei der aufsichtsrechtlichen Bewertung berücksichtigt werden. Umgekehrt dokumentiert die Umsetzung der Empfehlungen ein funktionierendes Datenschutzmanagement und den verantwortungsvollen Umgang mit den Feststellungen der Datenschutzaufsicht.

Nachkontrollen erfolgen dabei risikoorientiert. In besonders bedeutsamen oder komplexen Fällen überprüft das KDSZ Bayern die Umsetzung der empfohlenen Maßnahmen selbst. In anderen Fällen werden die Feststellungen und Empfehlungen bewusst in die Verantwortung der jeweiligen Einrichtung übergeben. Dies entspricht dem gesetzlichen Leitbild, wonach die Verantwortlichen selbst für die datenschutzkonforme Gestaltung ihrer Verarbeitungsvorgänge verantwortlich sind. Die Eigenverantwortung der Einrichtungen wird dadurch gestärkt und ein nachhaltiges Datenschutzmanagement gefördert. Zugleich ermöglicht der risikoorientierte Ansatz, die vorhandenen Ressourcen der Datenschutzaufsicht gezielt dort einzusetzen, wo sie den größten Nutzen für den Schutz personenbezogener Daten entfalten.

4.4.6 Audits als Motor der Organisationsentwicklung

Die Erfahrungen des Berichtsjahres bestätigen, dass Audits weit über eine reine Kontrollfunktion hinausgehen. Sie schaffen Transparenz, stärken die Eigenverantwortung der Verantwortlichen und fördern eine nachhaltige Datenschutzkultur innerhalb der kirchlichen Einrichtungen.

Die im Rahmen der Audits gewonnenen Erkenntnisse fließen unmittelbar in die Beratungsarbeit, die Entwicklung von Orientierungshilfen sowie die Planung zukünftiger Prüfungen ein. Dadurch profitieren nicht nur die jeweils geprüften Einrichtungen, sondern alle kirchlichen Rechtsträger in Bayern von den gewonnenen Erfahrungen.

Audits dienen damit nicht allein der Überprüfung datenschutzrechtlicher Anforderungen. Sie leisten zugleich einen wesentlichen Beitrag zur Weiterentwicklung des Datenschutzmanagements und fördern eine nachhaltige Datenschutzkultur in den kirchlichen Einrichtungen Bayerns.

> Audits dienen nicht allein der Kontrolle. Sie fördern nachhaltige Organisationsentwicklung, stärken die Eigenverantwortung der Einrichtungen und schaffen die Grundlage für eine kontinuierliche Verbesserung des Datenschutzmanagements.

4.5 Die Auditreihe in der katholischen Sozialwirtschaft

Auditreihe in der katholischen Sozialwirtschaft

Mit der Auditreihe verfolgt das KDSZ Bayern mehrere Ziele gleichzeitig:

- ☑ **Beratung zu ausgewählten Themen und Vertiefung des fachlichen Austauschs**
- ☑ **Bewertung des Datenschutzmanagements**
- ☑ **Entwicklung praxistauglicher Empfehlungen**
- ☑ **Stärkung der Zusammenarbeit mit den Sozialträgern**
- ☑ **Übertragbarkeit bewährter Lösungen auf andere Einrichtungen**

Die Auditreihe versteht sich als gemeinsamer Entwicklungsprozess und nicht als reine Kontrolle.

4.5.1 Ausgangslage

Neben den Einrichtungen der verfassten Kirche unterliegen auch zahlreiche privatrechtlich organisierte Einrichtungen der Datenschutzaufsicht des KDSZ Bayern. Hierzu zählen insbesondere die Diözesan-Caritasverbände sowie weitere katholische Sozialträger, die als Wesens- und Lebensäußerung der Kirche dem Anwendungsbereich des Gesetzes über den Kirchlichen Datenschutz unterfallen.

Um den fachlichen Austausch mit der Sozialwirtschaft weiter zu intensivieren und zugleich einen vertieften Einblick in deren Datenschutzorganisation zu gewinnen, begann das KDSZ Bayern im Berichtsjahr eine systematische Auditreihe bei sozialen Trägern.

Auch aufgrund ihrer besonderen Bedeutung als Multiplikatoren weit über die eigenen Einrichtungen hinaus wurden zunächst die Diözesan-Caritasverbände aller

sieben bayerischen (Erz-)Diözesen sowie weitere große katholische Sozialträger in den Blick genommen.

4.5.2 Entwicklung des Auditkonzepts

Den Ausgangspunkt der Auditreihe bildete der Informationstag ‚Datenschutz in der katholischen Sozialwirtschaft". Die dort gewonnenen Erkenntnisse wurden genutzt, um ein speziell auf die Anforderungen der kirchlichen Sozialwirtschaft zugeschnittenes Auditkonzept zu entwickeln.

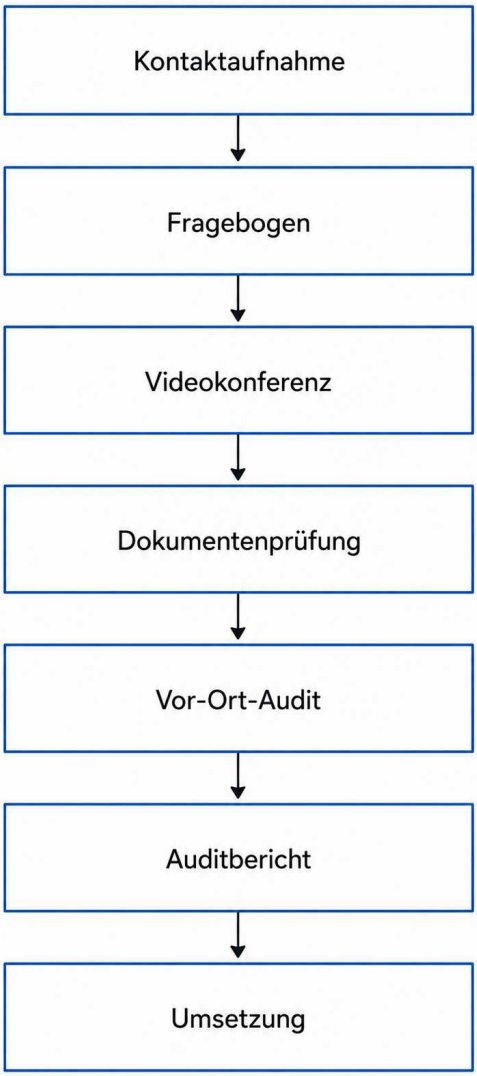
Während sich anlassbezogene Prüfungen häufig auf einzelne Verarbeitungsvorgänge oder konkrete Fragestellungen beschränken, verfolgt dieses Auditkonzept einen ganzheitlichen Ansatz. Ziel ist es, die Datenschutzorganisation eines Trägers insgesamt zu betrachten, organisatorische Strukturen zu bewerten und zugleich den fachlichen Austausch mit den Verantwortlichen zu fördern.

Dabei zeigte sich bereits im Vorfeld eine große Bandbreite unterschiedlicher Organisationsformen. Während einzelne Verbände mehrere hundert eigene Einrichtungen betreiben, nehmen andere Diözesan-Caritasverbände heute überwiegend nur noch verbandliche beziehungsweise spitzenverbandliche Aufgaben wahr und unterhalten nur wenige eigene Einrichtungen. Unterstützungsleistungen für Einrichtungen in Trägerschaft oder für Mitgliedseinrichtungen erfolgen dabei regelmäßig in den Bereichen Personalverwaltung, Buchhaltung, Rechnungswesen, IT-Dienstleistungen sowie teilweise bei der Betreuung von Internetauftritten oder sozialen Medien.

> Das Auditkonzept wurde gemeinsam mit der kirchlichen Sozialwirtschaft entwickelt und gezielt auf deren organisatorische Besonderheiten abgestimmt.

4.5.3 Durchführung der Audits

Die Audits folgten einem einheitlichen Ablauf. Nach der ersten Kontaktaufnahme wurden die Träger zunächst um eine Selbsteinschätzung anhand eines strukturierten Fragebogens sowie um die Vorlage ausgewählter Datenschutzdokumentationen gebeten. Die Themen orientierten sich an den wesentlichen Anforderungen des KDG sowie an bewährten Standards einer funktionierenden Datenschutzorganisation.



Ablauf eines risikoorientierten Audits in der katholischen Sozialwirtschaft

Die eingereichten Unterlagen wurden vorab ausgewertet und bildeten die Grundlage für die anschließenden Vor-Ort-Audits. Ergänzend fanden vorbereitende Videokonferenzen statt, um Rückfragen zum Fragebogen oder zu den eingereichten Unterlagen frühzeitig zu klären.

Um neben der zentralen Datenschutzorganisation auch deren praktische Umsetzung bewerten zu können, wurden zusätzlich ausgewählte Einrichtungen der jeweiligen Träger in die Audits einbezogen. Dadurch konnten die organisatorischen Vorgaben der Träger unmittelbar mit ihrer praktischen Umsetzung verglichen werden. Die Ergebnisse wurden in strukturierten Auditberichten zusammengefasst und gemeinsam mit den Verantwortlichen erörtert.

4.5.4 Erste Erkenntnisse

Besondere Schwerpunkte der Auditierungen bildeten die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Hierzu gehörten insbesondere gemeinsam genutzte Laufwerke, die Absicherung interner und externer Datenübertragungen, Berechtigungskonzepte sowie der Einsatz einer Mehrfaktorauthentifizierung für Cloud- und Fernzugriffe. Darüber hinaus wurden aktuelle Fragestellungen zum Einsatz Künstlicher Intelligenz, zur Videoüberwachung sowie zu weiteren Digitalisierungsvorhaben in die Prüfungen einbezogen.

Im Mittelpunkt der Audits standen darüber hinaus die Datenschutzorganisation der jeweiligen Träger sowie die Zusammenarbeit zwischen Datenschutz, Informationssicherheit, IT und den Leitungsorganen. Dabei zeigte sich, dass Datenschutz in den meisten Einrichtungen inzwischen als Querschnittsaufgabe verstanden wird und vielfach bereits in funktionierende Organisationsstrukturen eingebunden ist.

Den bislang geprüften kirchlichen Stellen oder Trägern konnte insgesamt ein hohes Datenschutzniveau sowie eine ausgeprägte Sensibilität im Umgang mit personenbezogenen Daten bescheinigt werden. Die im Rahmen der Audits identifizierten Optimierungspotenziale wurden von den Verantwortlichen überwiegend bereits während der Prüfungen aufgegriffen oder befinden sich in der Umsetzung.

> Die Audits bestätigten insgesamt ein hohes Datenschutzniveau.
> Optimierungspotenziale betrafen überwiegend organisatorische und technische Detailfragen und wurden vielfach bereits während der Audits aufgegriffen.

4.5.5 Mehr als eine Prüfung

Die Audits dienten nicht ausschließlich der Überprüfung datenschutzrechtlicher Anforderungen. Ebenso standen der fachliche Austausch mit den Verantwortlichen sowie die gemeinsame Entwicklung praxisgerechter Lösungen im Vordergrund. Zahlreiche Fragestellungen konnten bereits während der Auditgespräche geklärt werden. Gleichzeitig boten die Audits den beteiligten Sozialträgern die Möglichkeit, bewährte Vorgehensweisen miteinander zu vergleichen und Erfahrungen auszutauschen.

Die Auditreihe wird im Jahr 2026 fortgesetzt. Ziel bleibt es, den fachlichen Austausch mit den Sozialträgern weiter zu vertiefen, bewährte Praxisansätze sichtbar zu machen und die datenschutzrechtliche Organisation innerhalb der katholischen Sozialwirtschaft nachhaltig zu stärken.

4.6 Infotag Datenschutz – katholische Sozialwirtschaft

Zum Aufsichtsbereich des KDSZ Bayern gehören neben den Organen und Einrichtungen der verfassten Kirche auch zahlreiche Träger der katholischen Sozialwirtschaft. Hierzu zählen insbesondere die Diözesan-Caritasverbände sowie eine Vielzahl weiterer sozialer Einrichtungen unterschiedlicher Größe und Rechtsform, die unter dem Dach der Caritas tätig sind. Aufgrund ihrer vielfältigen Aufgaben und der Verarbeitung besonders sensibler personenbezogener Daten kommt dem Datenschutz in diesem Bereich eine besondere praktische Bedeutung zu.

> ### Infotag Datenschutz – katholische Sozialwirtschaft
>
> Der Infotag verfolgte mehrere Ziele:
>
> - ☑ **Fachlicher Austausch** zwischen Datenschutzaufsicht und Sozialträgern
> - ☑ **Praxisnahe Diskussion** aktueller Datenschutzfragen
> - ☑ **Klärung von Zuständigkeiten** im kirchlichen Datenschutz
> - ☑ **Entwicklung gemeinsamer Lösungsansätze**
> - ☑ **Grundlage für die Auditreihe der katholischen Sozialwirtschaft**
>
> Aus dem fachlichen Dialog entstand ein dauerhaftes Auditkonzept für die katholische Sozialwirtschaft.

Um den fachlichen Austausch mit diesen Einrichtungen zu intensivieren und aktuelle Fragestellungen der Datenschutzpraxis gemeinsam zu erörtern, veranstaltete das KDSZ Bayern im Berichtsjahr erstmals den ‚Infotag Datenschutz für die katholische Sozialwirtschaft“. Die Veranstaltung bildete den Auftakt für einen intensiveren Dialog mit den Sozialträgern und legte zugleich den Grundstein für die im weiteren Verlauf des Berichtsjahres entwickelte Auditreihe in der katholischen Sozialwirtschaft.

Dank der Unterstützung des Diözesan-Caritasverbandes der Erzdiözese Bamberg konnte die Veranstaltung als zweitägiger Workshop im Bistumshaus St. Otto durchgeführt werden. Eingeladen waren Einrichtungen und Träger der katholischen Sozialwirtschaft in Bayern, unabhängig von ihrer Größe oder Rechtsform. Die Bekanntmachung erfolgte unter anderem über die Diözesan-Caritasverbände sowie über die Kommunikationskanäle des KDSZ Bayern.

Die Inhalte des Workshops orientierten sich an typischen Fragestellungen aus der Aufsichtspraxis. Behandelt wurden insbesondere Datenschutzverletzungen, Beschwerdeverfahren, Audits sowie häufige Beratungsanfragen. Ziel war es, praktische Erfahrungen aus der Arbeit der Datenschutzaufsicht zu vermitteln und gemeinsam mit den Teilnehmenden konkrete Lösungsansätze für datenschutzrechtliche Fragestellungen zu entwickeln.

> Der Infotag vermittelte nicht nur rechtliche Grundlagen, sondern griff typische Fragestellungen aus der täglichen Datenschutzpraxis der katholischen Sozialwirtschaft auf.

Die Veranstaltung richtete sich insbesondere an betriebliche Datenschutzbeauftragte und Datenschutzkoordinatoren. Dabei wurde deutlich, dass neben materiell-rechtlichen Fragestellungen insbesondere die datenschutzrechtlichen Zuständigkeiten in komplexen Organisationsstrukturen häufig Erläuterungsbedarf aufweisen.

Diskutiert wurden unter anderem die unterschiedlichen Zuständigkeiten kirchlicher und staatlicher Datenschutzaufsichtsbehörden. Besondere Aufmerksamkeit fanden dabei Spezialkonstellationen, etwa die Unterscheidung zwischen Orden bischöflichen und päpstlichen Rechts. Während Orden bischöflichen Rechts der Zuständigkeit des KDSZ Bayern unterliegen, besteht für Orden päpstlichen Rechts eine eigene kirchliche Datenschutzaufsicht. Diese Differenzierung war vielen Teilnehmenden bislang nicht bekannt und wurde anhand praktischer Beispiele erläutert.

Ebenso intensiv wurde die Zuständigkeitsverteilung bei Datenschutzverletzungen diskutiert. Von besonderem Interesse war dabei der sogenannte Mitarbeiterexzess.

Verarbeitet ein Beschäftigter personenbezogene Daten ausschließlich zu eigenen, nicht dienstlich veranlassten Zwecken, handelt er regelmäßig außerhalb der Verantwortlichkeit des Arbeitgebers. Die datenschutzrechtliche Zuständigkeit liegt in diesen Fällen grundsätzlich bei der staatlichen Datenschutzaufsicht. Gerade diese Abgrenzungen erwiesen sich für die praktische Arbeit der Datenschutzbeauftragten und Datenschutzkoordinatoren als von besonderer Bedeutung.

> Gerade komplexe Zuständigkeitsfragen gehören zu den häufigsten Beratungsanlässen in der katholischen Sozialwirtschaft und lassen sich am besten im unmittelbaren fachlichen Austausch klären.

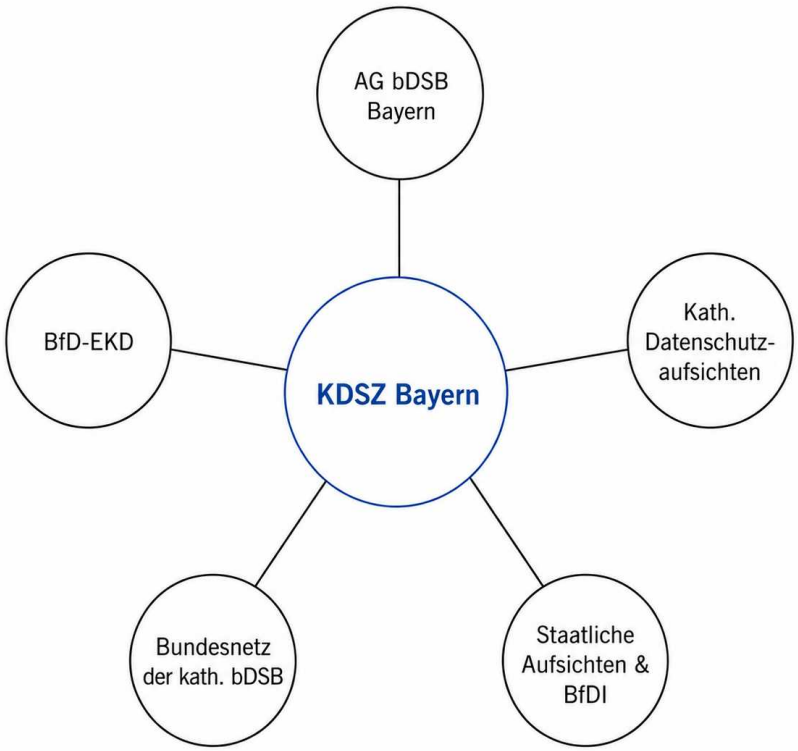
Der Infotag bot darüber hinaus Gelegenheit, gegenseitige Erwartungen offen anzusprechen und Erfahrungen aus der täglichen Datenschutzpraxis auszutauschen. Viele der dort gewonnenen Erkenntnisse flossen unmittelbar in die Entwicklung des risikoorientierten Auditkonzepts für die katholische Sozialwirtschaft ein, das im Anschluss gemeinsam mit einem Diözesan-Caritasverband entwickelt und im Berichtsjahr erstmals praktisch erprobt wurde.

Die positive Resonanz der Teilnehmenden hat gezeigt, dass ein regelmäßiger fachlicher Austausch einen wichtigen Beitrag zur Weiterentwicklung des Datenschutzes in der katholischen Sozialwirtschaft leisten kann. Das Veranstaltungsformat soll deshalb auch künftig fortgeführt und weiterentwickelt werden.

5 Zusammenarbeit und Vernetzung

Die Wahrnehmung der gesetzlichen Aufgaben einer Datenschutzaufsicht endet nicht an den Grenzen des eigenen Aufsichtsbereichs. Datenschutzrecht entwickelt sich kontinuierlich weiter und wirft regelmäßig neue rechtliche, technische und organisatorische Fragestellungen auf. Eine möglichst einheitliche Rechtsanwendung setzt deshalb einen engen fachlichen Austausch zwischen den beteiligten Akteuren voraus.

Das KDSZ Bayern ist hierzu auf unterschiedlichen Ebenen vernetzt. Der Austausch mit den betrieblichen Datenschutzbeauftragten, den kirchlichen und staatlichen Datenschutzaufsichtsbehörden sowie weiteren Fachgremien trägt wesentlich dazu bei, Erfahrungen aus der Praxis zusammenzuführen, gemeinsame Lösungen zu entwickeln und neue Entwicklungen frühzeitig aufzugreifen.



Netzwerk des KDSZ Bayern

Zusammenarbeit auf mehreren Ebenen

Das KDSZ Bayern ist auf unterschiedlichen Ebenen fachlich vernetzt:

- ☑ **Katholische Datenschutzaufsichten** in Deutschland
- ☑ **Betriebliche Datenschutzbeauftragte** der bayerischen (Erz-)Diözesen
- ☑ **Bundesweites Netzwerk** der Datenschutzbeauftragten aller 27 (Erz-)Diözesen
- ☑ **Staatliche Datenschutzaufsichtsbehörden**
- ☑ **Ökumenischer Austausch** mit der EKD

Ziel aller Kooperationen ist eine möglichst einheitliche, praxisgerechte und zukunftsorientierte Anwendung des Datenschutzrechts.

5.1 Austausch mit den bDSB der bayerischen (Erz-)Diözesen

Der regelmäßige Austausch mit den betrieblichen Datenschutzbeauftragten der bayerischen (Erz-)Diözesen bildet einen wichtigen Bestandteil der Präventions- und Beratungstätigkeit des KDSZ Bayern. Hierzu nimmt das KDSZ Bayern regelmäßig als Gast an den Sitzungen der Arbeitsgemeinschaft der betrieblichen Datenschutzbeauftragten (AG Datenschutz Bayern) teil. Die Arbeitsgemeinschaft hat sich als etabliertes Forum für den fachlichen Austausch zwischen den sieben bayerischen (Erz-)Diözesen entwickelt und ermöglicht es, aktuelle datenschutzrechtliche Fragestellungen gemeinsam zu erörtern.

Im Mittelpunkt der Beratungen stehen regelmäßig Themen, die alle Diözesen gleichermaßen betreffen. Hierzu zählen insbesondere neue gesetzliche Entwicklungen, der Einsatz Künstlicher Intelligenz, datenschutzrechtliche Fragestellungen bei gemeinsamen IT-Verfahren, Videoüberwachung sowie Fragen der Archivierung und Löschung personenbezogener Daten. Ebenso werden Erfahrungen aus der Beratungspraxis, aus Datenschutzverletzungen und aus laufenden Auditierungen ausgetauscht und gemeinsam bewertet.

Der Austausch bietet zugleich die Möglichkeit, praktische Herausforderungen frühzeitig zu erkennen und gemeinsame Lösungsansätze zu entwickeln. Die dabei gewonnenen Erkenntnisse fließen sowohl in die Beratungs- und Prüfungstätigkeit des KDSZ Bayern als auch in die Arbeit der betrieblichen Datenschutzbeauftragten ein. Ergänzt wird die Zusammenarbeit durch gemeinsame Workshops und Informationsveranstaltungen, die den Wissenstransfer zwischen Datenschutzaufsicht und betrieblichem Datenschutz weiter stärken.

5.2 Bundesweite Zusammenarbeit der bDSB

Der fachliche Austausch der betrieblichen Datenschutzbeauftragten beschränkt sich nicht auf Bayern. Darüber hinaus besteht ein bundesweites Netzwerk der Datenschutzbeauftragten aller 27 deutschen (Erz-)Diözesen. Regelmäßige Präsenztreffen und Videokonferenzen dienen dem Erfahrungsaustausch, der Erörterung aktueller datenschutzrechtlicher Fragestellungen sowie der Entwicklung gemeinsamer Arbeitshilfen und Projekte. Dadurch können Erfahrungen aus den einzelnen Diözesen gebündelt, Doppelarbeiten vermieden und praxisgerechte Lösungen gemeinsam entwickelt werden.

Ein herausragendes Beispiel dieser bundesweiten Zusammenarbeit ist die gemeinsame Entwicklung der Onlineschulung zum kirchlichen Datenschutz (OSKD). Das Projekt wurde ursprünglich von mehreren (Erz-)Diözesen gemeinsam mit einem externen Dienstleister ins Leben gerufen, um Mitarbeitenden eine zeitgemäße und einheitliche Grundschulung zum kirchlichen Datenschutz zur Verfügung zu stellen. Die Schulungsinhalte wurden zunächst auf der Plattform des Dienstleisters bereitgestellt und konnten von den Diözesen gegen Erwerb entsprechender Lizenzen genutzt werden.

Seit Ende 2021 wird die OSKD im Rahmen einer bundesweiten Arbeitsgruppe grundlegend weiterentwickelt. Ziel ist es, die Inhalte kontinuierlich zu aktualisieren, neue Zielgruppen zu erschließen und zugleich die digitale Souveränität der beteiligten (Erz-)Diözesen zu stärken. Hierzu entstehen neben der Grundschulung weitere Module, unter anderem für Pfarreien, Kindertageseinrichtungen sowie Verwaltungsleitungen.

Mit der Novellierung des Gesetzes über den Kirchlichen Datenschutz wurde zudem die Entwicklung einer vollständig überarbeiteten Grundschulung erforderlich, deren Fertigstellung für das Jahr 2026 vorgesehen ist. Die fachlichen Inhalte werden durch Arbeitsgruppen der betrieblichen Datenschutzbeauftragten erarbeitet und anschließend durch einen spezialisierten Dienstleister nach den Grundsätzen der Erwachsenenbildung in moderne digitale Lernmodule umgesetzt.

Ein besonderer Vorteil dieses Kooperationsmodells besteht darin, dass die entwickelten Schulungsmodule den beteiligten (Erz-)Diözesen dauerhaft zur Verfügung stehen. Sie können auf den jeweils eigenen Lernplattformen betrieben, im Corporate Design der jeweiligen Diözese gestaltet und unabhängig von einer externen Schulungsplattform eingesetzt werden. Die Inhalte verbleiben damit langfristig in kirchlicher Hand und können gemeinschaftlich weiterentwickelt werden. Das Projekt leistet damit nicht nur einen wichtigen Beitrag zur datenschutzrechtlichen Qualifizierung der Beschäftigten, sondern ist zugleich ein gelungenes Beispiel für digitale Souveränität und wirtschaftliche Zusammenarbeit innerhalb der katholischen Kirche in Deutschland.

Das KDSZ Bayern begleitet dieses Projekt nicht in seiner Funktion als Datenschutzaufsichtsbehörde, sondern übernimmt koordinierende Aufgaben innerhalb der Arbeitsgruppe. Dadurch unterstützt es den bundesweiten Wissenstransfer und trägt dazu bei, dass die gemeinsam entwickelten Schulungsangebote allen beteiligten (Erz-)Diözesen dauerhaft zugutekommen.

> Die gemeinsame Entwicklung der Onlineschulung (OSKD) zeigt, wie bundesweite Zusammenarbeit Fachwissen bündelt, Ressourcen schont und zugleich die digitale Souveränität der Kirche stärkt.

5.3 Zusammenarbeit der kirchlichen Datenschutzaufsichten

Das Gesetz über den Kirchlichen Datenschutz wird bundesweit durch fünf katholische Datenschutzaufsichtsbehörden angewendet. Um eine möglichst einheitliche Rechtsanwendung sicherzustellen und gemeinsame Positionen zu aktuellen datenschutzrechtlichen Fragestellungen zu entwickeln, arbeiten die Diözesandatenschutzbeauftragten in der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands eng zusammen.

Die Konferenz dient dem regelmäßigen fachlichen Austausch und der Abstimmung grundsätzlicher Rechtsfragen. Hierzu finden regelmäßig Präsenzsitzungen und Videokonferenzen statt. Ergänzend bearbeiten verschiedene Arbeitsgruppen aktuelle Themen des kirchlichen Datenschutzrechts und entwickeln gemeinsame Lösungen für Fragestellungen, die alle kirchlichen Datenschutzaufsichten gleichermaßen betreffen.

Die fünf katholischen Datenschutzaufsichten bilden zusammen die Konferenz der Diözesandatenschutzbeauftragten

Im Mittelpunkt der Zusammenarbeit stand im Berichtsjahr die Begleitung der Novellierung des Gesetzes über den Kirchlichen Datenschutz sowie der Entwicklung gemeinsamer Orientierungshilfen und Handreichungen für Verantwortliche und betriebliche Datenschutzbeauftragte. Die enge Abstimmung zwischen den kirchlichen Datenschutzaufsichten trägt wesentlich dazu bei, dass vergleichbare Sach-

verhalte bundesweit nach möglichst einheitlichen Maßstäben bewertet werden und Verantwortliche verlässliche Orientierung erhalten.

Der Leiter des KDSZ Bayern gehört der Konferenz der Diözesandatenschutzbeauftragten an und nimmt dort im Berichtsjahr die Aufgabe des Sprechers wahr. Neben der Koordination der Konferenzarbeit gehört hierzu insbesondere die Vertretung gemeinsamer Positionen gegenüber anderen kirchlichen und staatlichen Stellen sowie die Mitwirkung an der Weiterentwicklung des kirchlichen Datenschutzrechts.

Zur kirchlichen Datenschutzaufsicht gehören neben den fünf Diözesandatenschutzbeauftragten auch die Gemeinsamen Ordensdatenschutzbeauftragten der Deutschen Ordensobernkonferenz (DOK). Sie nehmen auf Grundlage der Kirchlichen Datenschutzregelung der Ordensgemeinschaften päpstlichen Rechts (KDR-OG) die unabhängige Datenschutzaufsicht für die an diesem System teilnehmenden Ordensgemeinschaften päpstlichen Rechts und deren Einrichtungen wahr. Inhaltlich entspricht ihre Aufgabe derjenigen der Diözesandatenschutzbeauftragten für die Einrichtungen der verfassten Kirche.

Die Arbeit der Konferenz beschränkt sich dabei nicht auf die Abstimmung rechtlicher Bewertungen. Sie bildet zugleich die Grundlage für einen kontinuierlichen Erfahrungsaustausch zwischen den katholischen Datenschutzaufsichten und erfolgt unter regelmäßiger Einbindung der Gemeinsamen Ordensdatenschutzbeauftragten (DOK). Dieser Austausch ermöglicht es, Erkenntnisse aus Beschwerden, Datenschutzverletzungen, Beratungen und Audits zusammenzuführen und aktuelle Fragestellungen gemeinsam zu bewerten. Auf diese Weise profitieren alle kirchlichen Datenschutzaufsichten von den Erfahrungen der jeweils anderen und tragen gemeinsam zu einer qualitativ hochwertigen und möglichst einheitlichen Anwendung des kirchlichen Datenschutzrechts bei.

5.4 Zusammenarbeit mit den staatlichen Datenschutzaufsichten

Die Zusammenarbeit mit den staatlichen Datenschutzaufsichtsbehörden bildet einen weiteren wichtigen Bestandteil der Tätigkeit des KDSZ Bayern. Zahlreiche datenschutzrechtliche Fragestellungen betreffen kirchliche und staatliche Verantwortliche gleichermaßen. Ein regelmäßiger fachlicher Austausch trägt deshalb wesentlich dazu bei, aktuelle Entwicklungen frühzeitig aufzugreifen und eine möglichst einheitliche Anwendung datenschutzrechtlicher Grundsätze zu fördern.

Auf Landesebene besteht ein kontinuierlicher Austausch mit dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) sowie dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD). Gegenstand der Gespräche sind insbesondere aktuelle rechtliche Entwicklungen, Fragen der praktischen Rechtsanwendung sowie Themen von gemeinsamem Interesse, die sowohl staatliche als auch kirchliche Verantwortliche betreffen.

Darüber hinaus nehmen die kirchlichen Datenschutzaufsichten regelmäßig an den gemeinsamen Treffen mit der Datenschutzkonferenz (DSK) mit den spezifischen Aufsichtsbehörden teil. Diese Zusammenkünfte dienen dem gegenseitigen Informations- und Erfahrungsaustausch zwischen den staatlichen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie den spezifischen Datenschutzaufsichten nach Art. 91 DSGVO. Ziel ist es, gemeinsame Herausforderungen frühzeitig zu erkennen und datenschutzrechtliche Fragestellungen möglichst abgestimmt zu bewerten.

Ergänzt wird diese Zusammenarbeit durch die Teilnahme der katholischen Datenschutzaufsichten in verschiedenen Arbeitskreisen der Datenschutzkonferenz. Dort werden aktuelle Entwicklungen, insbesondere im Bereich der Digitalisierung, der Künstlichen Intelligenz sowie weiterer Querschnittsthemen des Datenschutzrechts, fachlich begleitet und diskutiert. Die hierbei gewonnenen Erkenntnisse fließen unmittelbar in die Arbeit des K KDSZ Bayern ein und tragen dazu bei, neue Entwicklungen frühzeitig in die Beratungs-, Prüfungs- und Aufsichtspraxis einzubeziehen.

Die enge Zusammenarbeit mit den staatlichen Datenschutzaufsichtsbehörden stärkt damit nicht nur den fachlichen Austausch, sondern leistet zugleich einen wichtigen Beitrag zu einer kohärenten Anwendung des Datenschutzrechts und fördert das gegenseitige Verständnis zwischen staatlicher und kirchlicher Datenschutzaufsicht.

5.5 Ökumenischer Austausch

Der Datenschutz endet nicht an den Grenzen der Konfessionen. Zahlreiche kirchliche Einrichtungen arbeiten im Alltag eng zusammen oder stehen vor vergleichbaren rechtlichen und technischen Herausforderungen. Der regelmäßige Austausch zwischen den katholischen Datenschutzaufsichten und der Datenschutzaufsicht der Evangelischen Kirche in Deutschland (EKD) trägt deshalb wesentlich dazu bei, gemeinsame Fragestellungen frühzeitig aufzugreifen und voneinander zu lernen.

Ein fester Bestandteil dieser Zusammenarbeit ist der jährlich stattfindende Ökumenische Datenschutztag. Er bietet den kirchlichen Datenschutzaufsichten beider Konfessionen die Möglichkeit, aktuelle Entwicklungen des Datenschutzrechts, neue technische Herausforderungen sowie Fragen der praktischen Rechtsanwendung gemeinsam zu erörtern. Neben dem fachlichen Austausch stehen insbesondere der Vergleich unterschiedlicher Lösungsansätze und die Diskussion gemeinsamer Herausforderungen im Mittelpunkt der Veranstaltung.

Der ökumenische Dialog beschränkt sich dabei nicht auf den gegenseitigen Erfahrungsaustausch. Vielmehr entstehen hieraus regelmäßig gemeinsame Impulse für Orientierungshilfen, Fachveranstaltungen und weitere Projekte, die den Datenschutz in beiden Kirchen gleichermaßen weiterentwickeln. Im Berichtsjahr gewann der fachliche Austausch zusätzlich an Bedeutung, da sowohl das Gesetz über den Kirchlichen Datenschutz (KDG) als auch das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) umfassend überarbeitet wurden. Der regelmäßige Austausch ermöglichte es, die jeweiligen Gesetzgebungsverfahren zu begleiten, Erfahrungen frühzeitig auszutauschen und bei vergleichba-

ren Fragestellungen ein möglichst einheitliches Verständnis datenschutzrechtlicher Anforderungen zu fördern.

Der Ökumenische Datenschutztag hat sich damit als wichtiges Forum der kirchlichen Datenschutzaufsichten etabliert. Er stärkt die Zusammenarbeit über Konfessionsgrenzen hinweg und leistet einen wertvollen Beitrag zur Weiterentwicklung eines praxisgerechten und modernen kirchlichen Datenschutzes.

Nicht zuletzt wurde auch das Kirchengesetz über den Datenschutz in der evangelischen Kirche in Deutschland (DSG-EKD) ebenfalls im Jahr 2025 überarbeitet.

5.6 Vernetzung schafft Qualität

Die Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten, den kirchlichen und staatlichen Datenschutzaufsichtsbehörden sowie weiteren Fachgremien trägt wesentlich dazu bei, die Qualität der Datenschutzaufsicht kontinuierlich weiterzuentwickeln. Erkenntnisse aus Beratungen, Beschwerden, Datenschutzverletzungen und Audits fließen in die gemeinsame Gremienarbeit ein. Umgekehrt kommen die dort entwickelten Orientierungshilfen, Empfehlungen und Erfahrungen unmittelbar den kirchlichen Einrichtungen zugute.

Die Vernetzung dient damit nicht allein dem fachlichen Austausch. Sie schafft die Grundlage für eine möglichst einheitliche Anwendung des kirchlichen Datenschutzrechts, stärkt die Rechtssicherheit der Verantwortlichen und ermöglicht es, neue rechtliche und technische Entwicklungen frühzeitig aufzugreifen. Sie ist damit ein wesentlicher Bestandteil einer modernen, leistungsfähigen Datenschutzaufsicht.

> Vernetzung schafft Qualität. Der kontinuierliche Austausch zwischen Datenschutzaufsichten und betrieblichen Datenschutzbeauftragten fördert eine einheitliche Rechtsanwendung, stärkt die Rechtssicherheit und verbessert die Datenschutzpraxis nachhaltig.

6 Presseberichte

KI EINSATZ GENAU DEFINIEREN, KRITISCH PRÜFEN UND RISIKEN MINIMIEREN

Aufwand für die Einhaltung eines rechtskonformen Einsatzes bei der Einführung von Assistenztools nicht scheuen

Dürfen wir das überhaupt und was ist aus Datenschutzsicht zu beachten? Fragen, die Kindertageseinrichtungen stellen, wenn es um den potenziellen Einsatz von KI in der Kita geht. Die ImpulsKita Redaktion hat sich beim Diözesandatenschutzbeauftragten für die bayerischen Bistümer Dominikus Zettl erkundigt.

ImpulsKita: Wie wird der Einsatz von KI für Organisationen/Einrichtungen der katholischen Kirche in Bayern aus Datenschutzsicht generell bewertet?

Dominikus Zettl: Das Katholische Datenschutzzentrum Bayern (KDSZ Bayern) bewertet den Einsatz von KI in den Organisationen und Einrichtungen der katholischen Kirche in Bayern als notwendig, positiv und bereichernd.

Grundsätzlich sind Tools, die Elemente von sog. Künstlicher Intelligenz enthalten, wie jede andere Software auch, den üblichen (datenschutz)rechtlichen Regelungen unterworfen. Es ist eine ausführliche Risikoanalyse durchzuführen, ob das einzuführende Tool die Anforderungen von IT-Sicherheit, Informationssicherheit und Datenschutz erfüllt.

ImpulsKita: Welche Schritte sind zu unternehmen, wenn ein Tool mit KI eingeführt werden soll?

Dominikus Zettl: Das KDSZ Bayern geht davon aus, dass aufgrund der Neuartigkeit der Technologie bei allen Tools, die in irgendeiner Form KI beinhalten, in jedem Falle eine Datenschutzfolgenabschätzung nach § 35 des Gesetzes über den Kirchlichen Datenschutz (KDG) erforderlich wird.

Ein wesentlicher Punkt bei der Prüfung ist, sich klarzumachen, bei welchen Tätigkeiten bzw. Verarbeitungen genau das KI-Tool unterstützen soll. Im nächsten Schritt ist darzustellen, ob und wenn ja, welche personenbezogenen Daten der Mitarbeitenden oder Klienten (z.B. Kinder) in das Tool eingespeist werden müssen, um das gewünschte Ergebnis zu erzielen.

Zur Erstellung einer Lerngeschichte oder die Übersetzung einer Elterninformation in eine Fremdsprache ist üblicherweise gar keine Eingabe von personenbezogenen Daten erforderlich. Die Formulierung individueller Texte für die Entwicklungsdokumentation eines Kindes oder die Unterstützung der Eltern bei der Beantragung einer Individualbetreuung mit der Hilfe von Assistenten wie z.B. ChatGPT oder vergleichbaren ist dagegen schon kritischer zu sehen. Denn hier darf man personenbezogene Daten nur dann eingeben, wenn deren Schutz gewährleistet ist.

ImpulsKita: Wie lassen sich die datenschutzrechtlichen Risiken reduzieren?

Dominikus Zettl: Maßnahmen zur Risikoreduzierung könnten sein, dass man sicherstellt, dass die

eingesetzten KI-Tools von Anbietern im deutschen Sprachraum stammen und die Daten der Sprachmodelle auf Servern liegen, die dem Geltungsbereich der Datenschutzgrundverordnung (DSGVO) und dem KDG unterfallen und die Anbieter auch nur Unterauftragsverarbeiter einsetzen, für die diese Regelungen gelten.

Diese Themen sollten im Softwarenutzungsvertrag sowie im Vertrag zur Auftragsverarbeitung ausdrücklich geregelt sein. Ein besonders wichtiger Punkt ist, dass der Anbieter zusichern muss, dass die KI-Tools sämtliche Eingaben, egal ob mit oder ohne Personenbezug, nicht zu eigenen Trainingszwecken nutzen.

Aus Sicht des KDSZ Bayern könnten viele der technischen, rechtlichen und datenschutzrechtlichen Anforderungen dadurch gelöst werden, dass für staatliche und kirchliche Einrichtungen von US-amerikanischen Großkonzernen unabhängige KI-Produkte im europäischen Rechtsraum geschaffen werden, sozusagen eine Deutschland-KI oder noch besser ein Kirchen-KI.

ImpulsKita: Gibt es weitere Bestimmungen, die zu beachten sind?

Dominikus Zettl: Neben den bereits genannten rechtlichen Anforderungen aus dem KDG, sind die ethischen Grundsätze und die Grundwerte der katholischen Kirche zu beachten. Hierzu gehört neben den Persönlichkeitsrechten der Kinder und Eltern auch ein Blick auf den Energiebedarf der Sprachmodelle und damit die notwendige Rechenleistung zur Generierung der Ergebnisse. Die Arbeitserleichterungen durch den Einsatz von Technik und der mögliche Verlust der Kontrolle über personenbezogene Daten sollten immer gut abgewogen werden.

ImpulsKita: Wie sollen katholische Kindertageseinrichtungen vorgehen, wenn sie KI einsetzen möchten?

Dominikus Zettl: Es ist sinnvoll und wichtig, dass die Kindertageseinrichtungen nicht im Alleingang handeln, sondern die betrieblichen Datenschutzbeauftragten und die IT-Abteilungen der Träger, z.B. Caritasverbände und Ordinariate, in den Beschaffungsprozess mit einbeziehen.

Nachdem klar ist, dass KI in fast allen Lebensbereichen Einzug halten wird und vielfach unterstützend und hilfreich sein kann, sollte man den Aufwand der Einhaltung eines rechtskonformen Einsatzes bei der Einführung der Tools nicht scheuen.

Auch hier gilt, dass eine mindestens bayernweite Vernetzung der Träger hilfreich ist, da in allen Einrichtungen ähnliche Fragestellungen auftauchen und gelöst werden müssen.

INTERVIEWPARTNER

DOMINIKUS ZETTL
Diözesandatenschutzbeauftragter für die bayerischen Bistümer
Katholisches Datenschutzzentrum Bayern (KdöR)
Datenschutzaufsicht für die bayerischen (Erz-)Diözesen
>> www.kdsz.bayern

7 Ausblick auf das Jahr 2026

Ausblick 2026

Die Arbeit des KDSZ Bayern wird im kommenden Berichtszeitraum insbesondere durch folgende Themen geprägt sein:

- ☑ Umsetzung der KDG-Novelle und der KDG-DVO
- ☑ Digitalisierung und Künstliche Intelligenz
- ☑ Informationssicherheit und Cyberresilienz
- ☑ Digitale Souveränität kirchlicher Einrichtungen
- ☑ Ausbau von Beratung, Audits und digitalen Serviceangeboten

Datenschutz bleibt eine wesentliche Voraussetzung für eine verantwortungsvolle Digitalisierung der Kirche.

Mit dem Inkrafttreten der Novellierung des Gesetzes über den Kirchlichen Datenschutz (KDG) und der zugehörigen Durchführungsverordnung (KDG-DVO) zum 1. März 2026 beginnt für die kirchlichen Einrichtungen eine neue Phase der praktischen Umsetzung des kirchlichen Datenschutzrechts. Das KDSZ Bayern wird diesen Prozess auch künftig beratend begleiten und die Verantwortlichen bei der Anwendung der neuen gesetzlichen Vorgaben unterstützen. Ziel bleibt es, Datenschutz nicht nur rechtssicher, sondern zugleich praxisnah und zukunftsfähig zu gestalten.

Darüber hinaus werden die fortschreitende Digitalisierung und der zunehmende Einsatz Künstlicher Intelligenz die Datenschutzpraxis nachhaltig verändern. Gleichzeitig gewinnen Informationssicherheit, Cyberresilienz und der verantwortungsvolle Umgang mit digitalen Technologien weiter an Bedeutung. Datenschutz lässt sich heute nur noch im Zusammenspiel mit wirksamen technischen und organisatorischen Schutzmaßnahmen verwirklichen. Die zunehmende Verzahnung von Datenschutz und Informationssicherheit wird deshalb auch künftig einen Schwerpunkt unserer Arbeit bilden.

Ein besonderes Augenmerk wird weiterhin auf der Stärkung der digitalen Souveränität kirchlicher Einrichtungen liegen. Sichere, transparente und möglichst unabhängige digitale Infrastrukturen leisten einen wichtigen Beitrag zum Schutz personenbezogener Daten und stärken zugleich die langfristige Handlungsfähigkeit kirchlicher Organisationen. Das KDSZ Bayern wird die Einrichtungen auch künftig im Rahmen seiner Möglichkeiten dabei unterstützen, Digitalisierung verantwortungsvoll zu gestalten und datenschutzfreundliche Lösungen zu fördern.

> Datenschutz, Informationssicherheit und digitale Souveränität bilden gemeinsam die Grundlage einer zukunftsfähigen Digitalisierung kirchlicher Einrichtungen.

Ebenso werden wir den begonnenen Dialog mit den kirchlichen Einrichtungen konsequent fortsetzen. Die Auditierungsreihe bei den Sozialträgern, Informationsveranstaltungen, Schulungsangebote sowie der kontinuierliche fachliche Austausch sollen weiter ausgebaut werden. Datenschutz lebt von Zusammenarbeit, gegenseitigem Verständnis und einer frühzeitigen Sensibilisierung aller Beteiligten. Diesen präventiven Ansatz werden wir auch in Zukunft weiterverfolgen.

Auch die digitalen Serviceangebote des KDSZs Bayern werden kontinuierlich weiterentwickelt. Unser Ziel ist es, Verantwortlichen, Datenschutzbeauftragten und betroffenen Personen zeitgemäße Informations- und Unterstützungsangebote zur Verfügung zu stellen und den Zugang zu datenschutzrechtlichen Informationen weiter zu erleichtern.

Bleiben Sie deshalb auch künftig mit uns im Austausch. Neben unserer Internetseite informieren wir regelmäßig über unsere Präsenzen im Fediverse – insbesondere über https://katholisch.social.

Die bewusste Entscheidung für offene, datenschutzfreundliche und werbefreie Kommunikationsplattformen verstehen wir dabei als Ausdruck unseres eigenen Anspruchs an Datenschutz und digitale Souveränität. Wir freuen uns darauf, diesen Weg gemeinsam mit Ihnen auch künftig fortzusetzen.