Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht 2024

2025
2026
2027
2028
2029
2030

Kath. Datenschutzzentrum
Frankfurt/M.

Tätigkeitsbericht 2024

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

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

Aus redaktionellen Gründen wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen an einigen Stellen verzichtet. Die verkürzte Verwendung gilt im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter und enthält keine Wertung.
Bildnachweise: Titel und Rückseite: DrAfter123 / iStock, S.6 u. 37: Olaf J. Lutz, KDSZ Ffm,
S. 10: Javier Allegue Barros / unsplash, S. 26: Gacro74 / Alamy Stock Foto, S. 15 u. 33: Freepik

Kein „verflixtes 7. Jahr“

Das Kath. Datenschutzzentrum Frankfurt/M. veröffentlicht mit dem hier vorliegenden Bericht des Jahres 2024 seinen nunmehr siebten Tätigkeitsbericht. Das „verflixte 7. Jahr“ ist damit abgeschlossen, die diesem oftmals zugeschriebene Gefahr größerer Veränderungen hat sich nicht bewahrheitet: Leitung, Team, Standort und Aufgabenbereich der Datenschutzaufsicht sind unverändert. Die Zahl 7 sollte daher im biblischen Sinne als etwas Positives verstanden werden.

Die kontinuierliche Umsetzung des Datenschutzes in allen Bereichen und darüber hinaus die Entwicklung neuer sowie die Evaluierung und Anpassung bereits bestehender Datenschutzregelungen haben das Datenschutzjahr 2024 im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. geprägt: Einsichts- und Auskunftsrechte der Aufarbeitungskommissionen wurden geregelt, Meldestellen eingerichtet, Jubiläumsordnungen erlassen, Widerspruchsrechte implementiert und Musterverträge zur Auftragsverarbeitung und zur gemeinsamen Verantwortlichkeit erstellt.

Im staatlichen Datenschutz wurden im Berichtsjahr auf Gesetzgebungsebene EU-Rechtsakte wie die KI-Verordnung und das Cyberresilienzgesetz verabschiedet, die maßgeblich für die europäische Gesetzgebung im digitalen Bereich sind, und der Europäische Gerichtshof hat wieder wichtige Entscheidungen beispielsweise zu den Befugnissen von Datenschutzaufsichten getroffen. Auch die kirchlichen Datenschutzgerichte waren 2024 nicht untätig und schauten unter anderem, dass der Datenschutz auch im Rahmen von Teufelsaustreibungen und der Missbrauchsaufarbeitung die nötige Beachtung findet.

Der vorliegende Tätigkeitsbericht soll jedoch nicht nur die oben erwähnten Eckpunkte des Berichtsjahrs erläutern, sondern er will vor allem die Aufgaben und Aktivitäten des Kath. Datenschutzzentrums Frankfurt/M. veranschaulichen. So sollen unter anderem die Beschreibungen aus dem „Tagesgeschäft“ der Datenschutzaufsicht, wie die datenschutzkonforme Beschriftung einer tiefgefrorenen Plazenta oder die Implementierung sicherer Identifizierungsprozesse bei Mitteilung einer geänderten Kontoverbindung, dazu dienen, die Anforderungen an den Datenschutz zu demonstrieren und Verbesserungsmöglichkeiten aufzuzeigen.

Immer dann, wenn es durch ausreichende Prävention, Information, Beratung und Sensibilisierung der Verantwortlichen nicht zu Datenschutzverletzungen und Beschwerden kommt, ist ein wichtiger Teil der aufsichtlichen Aufgaben gelungen.

Ursula Becker-Rathmair

Diözesandatenschutzbeauftragte
und Leiterin des Kath. Datenschutzzentrums Frankfurt/M.

1 Aus der Datenschutzaufsicht

Das Kath. Datenschutzzentrum Frankfurt/M. KdöR ist nun seit mehr als eineinhalb Jahren am neuen Standort im Herzen von Frankfurt. Am 5. Juli 2024 wurde – erstmals in den neuen Räumlichkeiten – ein Tätigkeitsbericht, der des Jahres 2023, von der Diözesandatenschutzbeauftragten Ursula Becker-Rathmair an den Vorsitzenden des Verwaltungsrats Dr. Sascha Koller übergeben.

Dr. Sascha Koller, Vorsitzender des Verwaltungsrats, erhält als Erster den druckfrischen Tätigkeitsbericht 2023 aus den Händen der Diözesandatenschutzbeauftragten Ursula Becker-Rathmair

Der Tätigkeitsbericht 2023 endete mit den Worten „Datenschutz ist spannend – und er wird es bleiben!“. Diese Prognose hat sich im Laufe des Jahres 2024 durchaus bestätigt.

Nicht nur die Themen des „Tagesgeschäfts“ der katholischen Datenschutzaufsicht in Frankfurt, die neben der Beratung von Verantwortlichen und der Wahrnehmung der datenschutzrechtlichen Aufsicht auch die Bearbeitung von Beschwerden, Anfragen und Datenschutzverletzungen und die Durchführung von Prüfungen umfassen, waren so breit gefächert und interessant wie in den vergangenen Jahren. Auch beim Austausch mit den Teilnehmerinnen und Teilnehmern der zum ersten Mal in den neuen Räumlichkeiten am Roßmarkt durchgeführten Veranstaltungen wurden wieder ganz unterschiedliche und sehr spannende Themen diskutiert.

Vielfältig war darüber hinaus auch der Austausch mit den anderen Aufsichtsbehörden, sowohl die Auswahl der diskutierten Themenbereiche betreffend als auch im Hinblick auf die Anzahl der Treffen (mehr dazu ist in Kapitel 5 zu lesen).

Erstmalig seit Gründung des Kath. Datenschutzzentrums Frankfurt/M. wurde die Möglichkeit zur Absolvierung eines juristischen Praktikums angeboten und so konnte einer Studentin der Rechtswissenschaften vier Wochen lang Einblick in die Aufgaben und Arbeitsweisen der Datenschutzaufsicht gewährt werden.

2 Entwicklung des Datenschutzes

Die Bedeutung der IT-Sicherheit und deren zunehmende, oftmals sehr enge Verzahnung mit dem Datenschutz waren bereits im Tätigkeitsbericht des Jahres 2023 ein Thema. Ein Blick auf wichtige EU-Verordnungen und -Richtlinien des Jahres 2024 zeigt, dass diese Entwicklung weiter voranschreitet.

Sowohl die im Jahr 2024 bereits in Kraft getretenen EU-Verordnungen „AI-Act“, „Cyber Resilience Act (CRA)“ und „Data-Act“ als auch die „EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2-Richtlinie)“, deren Umsetzung in nationales Recht erst nach der Verhandlung im neuen Bundestag eingeleitet werden kann, machen deutlich, dass es Datenschutz ohne Datensicherheit nicht geben kann.

Durch das noch vom alten Bundestag verabschiedete und am 26. März 2024 in Kraft getretene „Gesundheitsdatennutzungsgesetz (GDNG)“ wird die Nutzung von Gesundheitsdaten für gemeinwohlorientierte Zwecke geregelt. Forschung und Innovation sollen gefördert und das digitalisierte Gesundheitssystem auf Grundlage einer soliden Datenbasis weiterentwickelt werden.

Das Thema der Künstlichen Intelligenz (KI) ist mittlerweile aus kaum einem Lebensbereich mehr wegzudenken. Mal mehr und mal weniger offensichtlich spielt KI eine Rolle, daher gewinnt auch der Schutz der dort verarbeiteten personenbezogenen Daten eine immer größere Bedeutung.

Papst Franziskus hat dies in seiner Botschaft zur Feier des 57. Weltfriedenstages am 1. Januar 2024 eindrucksvoll zusammengefasst:

„Es reicht auch nicht aus, bei denjenigen, die Algorithmen und digitale Technologien entwickeln, eine Verpflichtung zu ethischem und verantwortungsvollem Handeln vorauszusetzen. Es müssen Organismen gestärkt oder gegebenenfalls geschaffen werden, die sich mit den neu auftretenden ethischen Fragen befassen und die Rechte derjenigen schützen, die Formen der künstlichen Intelligenz nutzen oder von ihnen beeinflusst werden.“

„Es reicht auch nicht aus, bei denjenigen, die Algorithmen und digitale Technologien entwickeln, eine Verpflichtung zu ethischem und verantwortungsvollem Handeln vorauszusetzen. Es müssen Organismen gestärkt oder gegebenenfalls geschaffen werden, die sich mit den neu auftretenden ethischen Fragen befassen und die Rechte derjenigen schützen, die Formen der künstlichen Intelligenz nutzen oder von ihnen beeinflusst werden.“

2.1 Staatliche Gesetzgebung

2.1.1 Novellierung des Bundesdatenschutzgesetzes

Am 15. Mai 2024 hat der Bundestag in erster Lesung über die Novellierung des Bundesdatenschutzgesetzes (BDSG) beraten. Nach der Debatte überwiesen die Abgeordneten den Gesetzentwurf an die Ausschüsse, federführend für die weiteren Beratungen wird der Ausschuss für Inneres und Heimat sein.

Durch diesen Gesetzentwurf sollen unter anderem Ergebnisse einer Evaluierung des BDSG umgesetzt werden. Darüber hinaus soll die Datenschutzkonferenz (DSK) im BDSG institutionalisiert und Unternehmen und Forschungseinrichtungen mit länderübergreifenden Vorhaben soll ermöglicht werden, einer einzigen Landesdatenschutzaufsichtsbehörde zu unterstehen. Verantwortliche haben dann als Ansprechpartner für ihr gemeinsames Datenverarbeitungsvorhaben nur eine Aufsichtsbehörde, wodurch Rechtsunsicherheit durch unterschiedliche Rechtsauffassungen verschiedener zuständiger Aufsichtsbehörden vermieden werden soll.

2.1.2 AI-Act – KI-Verordnung

Der Rat der 27 EU-Mitgliedstaaten hat am 21. Mai 2024 den AI-Act (KI-Verordnung) und damit einen einheitlichen Rahmen für den Einsatz von Künstlicher Intelligenz in der Europäischen Union verabschiedet. Diese Verordnung ist das weltweit erste umfassende Regelwerk für KI, sie tritt ab 1. August 2024 nach und nach in Kraft und wird 24 Monate nach ihrem Inkrafttreten in vollem Umfang anwendbar sein.

Die Pflichten aus der KI-Verordnung gelten für Hersteller, Händler und Anbieter von KI-Systemen, also praktisch für jedes Unternehmen und jeden beruflichen Anwender von KI.

Die KI-Verordnung verfolgt ebenso wie die Europäische Datenschutzgrundverordnung (DSGVO) und das Gesetz über den Kirchlichen Datenschutz (KDG) einen risikobasierten Ansatz: Je höher das Risiko, desto strenger die Vorschriften. KI-Systeme, die zum Beispiel eingesetzt werden können, um das Verhalten von Personen gezielt zu beeinflussen und sie so zu manipulieren, gelten als inakzeptabel und sind verboten, genauso wie KI-basiertes „Social Scoring“, also die Klassifizierung von Menschen auf der Grundlage von Verhalten, sozioökonomischem Status und persönlichen Merkmalen.

Neben der Umsetzung in nationales Recht, die die EU-Mitgliedstaaten nun vornehmen müssen, soll jeder Mitgliedstaat zur Durchsetzung der Vorschriften eine oder mehrere zuständige nationale Behörden benennen, die die Anwendung und Umsetzung beaufsichtigen und die Marktüberwachung wahrnehmen.

2.1.3 CRA – Cyberresilienzgesetz

Mit dem Cyber Resilience Act (CRA) wurde im November 2024 eine EU-Verordnung verabschiedet, die den Cybersicherheitsrahmen für Produkte mit digitalen Elementen vereinheitlichen und stärken soll. Nach dem Inkrafttreten im Dezember 2024 werden die Regelungen des CRA bis Dezember 2027 schrittweise umgesetzt.

Der CRA soll ein Mindestmaß an Cybersicherheit über den gesamten Lebenszyklus digitaler Produkte hinweg – von der Entwicklung bis zur Außerbetriebnahme – gewährleisten. Bereits in der Entwicklungsphase eines Produkts müssen Hersteller Cybersicherheitsrisiken identifizieren und minimieren („Security by Design“). Regelmäßige Überprüfungen und die Behebung von Schwachstellen sind festgelegt und es gelten umfangreiche Dokumentations- und Meldepflichten.

Sicherheit im digitalen Umfeld – sowohl DSGVO als auch CRA verfolgen dieses Ziel. Während die DSGVO den Schutz personenbezogener Daten gewährleistet, zielt der CRA auf die Sicherheit digitaler Produkte ab. Der Sicherheits- und Datenschutzrahmen, der von beiden Gesetzen umfasst wird, soll und kann bei entsprechender Umsetzung der Anforderungen ein wirksames Mittel gegen Cyberbedrohungen sein.

2.1.4 Umsetzung des DSA in nationales Recht

Das Digitale-Dienste-Gesetz (DDG) ist am 14. Mai 2024 in Kraft getreten. Das DDG setzt das Gesetz über digitale Dienste (Digital Services Act (DSA)) der Europäischen Union in nationales Recht um und erweitert diese europäische Verordnung.

Die Vorschriften des DSA, die bereits seit dem 17. Februar 2024 für alle Unternehmen, die elektronische Dienste anbieten, gelten, stellen die Basis für das DDG dar. Der DSA soll ein einheitliches Regelwerk für alle EU-Staaten schaffen, um eine faire, einheitliche und freie Online-Umgebung garantieren zu können; so soll der bestehende Binnenmarkt für digitale Dienste sichergestellt und verbessert werden.

Durch das DDG wurden sowohl das Telemediengesetz (TMG) als auch das Netzdurchsetzungsgesetz (NetzDG) abgelöst, außerdem wurde der Aufgabenbereich der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) durch dieses Gesetz erweitert, da auch diese Behörde für eine wirksame Durchsetzung der Regelungen zu sorgen hat.

2.1.5 Orientierungshilfen der Datenschutzkonferenz

DSK-Orientierungshilfe „Künstliche Intelligenz“

▶ DSK-Orientierungshilfe „Künstliche Intelligenz“

Die Datenschutzkonferenz (DSK) hat am 6. Mai 2024 eine Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ veröffentlicht, die als Leitfaden für Unternehmen, Behörden und andere Organisationen dienen kann, um KI-Anwendungen auszuwählen, zu implementieren und zu nutzen. Wichtige Kriterien basierend auf den Vorgaben der DSGVO werden erörtert und Leitlinien für entsprechende Entscheidungen aufgezeigt – auch anhand von Beispielen. So werden praxisnah Fragen dargelegt, die sich datenschutzrechtlich Verantwortliche bei der Konzeption des Einsatzes, der Auswahl, der Implementierung und der Nutzung von KI-Anwendungen stellen und letztlich beantworten müssen. Das besondere Interesse gilt hierbei den „Large Language Models (LLM)“, die angestellten Erwägungen können jedoch auch für zahlreiche weitere KI-Modelle und KI-Anwendungen bedeutsam sein.

Die Orientierungshilfe wird künftig weiterentwickelt und an aktuelle Entwicklungen angepasst.

DSK-Orientierungshilfe „Digitale Dienste“

▶ DSK-Orientierungshilfe „Digitale Dienste“

Eine weitere Orientierungshilfe der DSK erschien am 6. November 2024: „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)“.

Bereits im Dezember 2021 veröffentlichte die DSK zu dieser Thematik eine Orientierungshilfe, die nun im November 2024 als überarbeitete Version erschienen ist.

Doch nicht nur, um der Umbenennung des „Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG)“ in „Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG)“

Rechnung zu tragen und um einige sprachliche Anpassungen vorzunehmen, wurde die neue Version der Orientierungshilfe dort veröffentlicht. Neben Ergänzungen bezüglich der Gestaltung von Cookie-Bannern und zum Einsatz von Cookies sind auch weitergehende Erläuterungen zu Informationspflichten und einigen Betroffenenrechten zu finden.

2.1.6 Stellungnahmen des Europäischen Datenschutzausschusses

EDSA-Stellungnahme zu (Unter-)Auftragsverarbeitern

Der Europäische Datenschutzausschuss (EDSA) kommt in seiner Stellungnahme 22/2024 vom 7. Oktober 2024 zu dem Schluss, dass Verantwortlichen die Pflicht obliegt, die Identität (d. h. Name, Adresse, Kontaktperson) und die Tätigkeiten aller Auftragsverarbeiter und Unterauftragsverarbeiter zu kennen und diese Informationen jederzeit bereitzuhalten, um ihre Verpflichtungen gemäß Art. 28 DSGVO erfüllen zu können. Auch gelte dies unabhängig von dem Risiko, das mit einer Verarbeitungstätigkeit verbunden ist.

▶ EDSA-Stellungnahme zu (Unter-) Auftragsverarbeitern

Zu diesem Zweck soll der Auftragsverarbeiter proaktiv dem Verantwortlichen die notwendigen Informationen sowohl des Auftragsverarbeiters selbst als auch des Unterauftragsverarbeiters zur Verfügung stellen und diese Informationen stets auf dem neuesten Stand halten. Diese Pflichten sind bereits im Auftragsverarbeitungsvertrag festzulegen.

Ebenfalls soll damit sichergestellt werden, dass der Verantwortliche seiner Informationspflicht über die Empfänger von Daten nachkommen, schnell auf Datenschutzverstöße in der gesamten Verarbeitungskette reagieren und darüber hinaus die Auskunftsrechte betroffener Personen gewährleisten kann.

EDSA-Stellungnahme zu KI-Modellen

In seiner Stellungnahme 28/2024 vom 18. Dezember 2024 hat der EDSA die Anforderungen an den Umgang mit personenbezogenen Daten in der Entwicklung und Nutzung von KI-Modellen präzisiert.

▶ EDSA-Stellungnahme zu KI-Modellen

Ausgearbeitet wurde die Stellungnahme auf Anfrage der irischen Datenschutzbehörde und unter Einbeziehung von Interessenträgern, wie etwa dem stellvertretenden Bundesdatenschutzbeauftragten.

Im Fokus stehen in dieser Stellungnahme Fragen zur Anonymität von KI-Modellen, zur Anwendung des berechtigten Interesses als Rechtsgrundlage für die Datenverarbeitung sowie zur Nutzung unrechtmäßig erhobener Daten. Darüber hinaus werden auch die Transparenz der Verarbeitung der Daten und die Informationspflichten gegenüber der betroffenen Person erörtert, die insbesondere bei der Nutzung von Daten aus öffentlich zugänglichen Quellen zu beachten sind.

Das Ziel soll sein – so ist es der Stellungnahme zu entnehmen –, Innovationen in der KI-Entwicklung zu fördern, ohne die Prinzipien der DSGVO zu gefährden. Dabei wird eine europaweite Vereinheitlichung der Rechtsvorschriften angestrebt.

2.2 Kirchliche Gesetzgebung

2.2.1 Weitere Ordnungen zur Regelung von Einsichts- und Auskunftsrechten der Aufarbeitungskommissionen in Kraft – Limburg und Rottenburg-Stuttgart

Zum 1. Oktober 2024 hat das Bistum Limburg nunmehr auch die „Musterordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- oder hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung“ der Deutschen Bischofskonferenz (DBK) in Kraft gesetzt. Wie bereits einige Bistümer im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. zuvor in ihren entsprechenden Ordnungen festgelegt haben, regelt auch diese in Limburg die Offenlegung von Unterlagen aller kirchlichen Rechtsträger und deren Einrichtungen in der Diözese, unabhängig von ihrer Rechtsform, in Form der Übermittlung und Bereitstellung gegenüber unabhängigen Aufarbeitungskommissionen, zu Forschungszwecken sowie gegenüber Anwaltskanzleien.

§ 2 des Regelwerks stellt klar, dass für die Verarbeitung personenbezogener Daten weiterhin die allgemeinen kirchlichen datenschutz- und archivrechtlichen Regeln gelten – soweit sich aus der Musterordnung nichts Abweichendes ergibt.

Das bedeutet im Umkehrschluss auch, dass die Musterordnung gemäß § 2 Abs. 2 KDG das Datenschutzniveau des KDG nicht unterschreiten darf. Heikel wird dieser Punkt vor allem dann, wenn die Musterordnung Einsicht und Auskunft in Unterlagen ohne die Einwilligung der betroffenen Person gewährt.

Eine abgespeckte Version der Musterordnung wurde im November 2024 im Bistum Rottenburg-Stuttgart auf den Weg gebracht. Die Vorschrift über die Rechtmäßigkeit der Datenverarbeitung bei der Offenlegung von personenbezogenen Daten gegenüber Rechtsanwaltskanzleien wurde nicht übernommen.

Sie trägt daher den leicht verkürzten Titel: „Ordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommission zur Aufarbeitung des sexuellen Missbrauchs in der Diözese Rottenburg-Stuttgart (Aufarbeitungskommission Diözese Rottenburg-Stuttgart – AK-DRS) sowie für Forschungszwecke in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung“.

Die Bistümer Limburg und Rottenburg-Stuttgart haben im Jahr 2024 ihre Ordnungen zur Regelung der Einsichts- und Auskunftsrechte für die Kommissionen zur Missbrauchsaufarbeitung erlassen.

Nr. 323 Musterordnung[1] zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- oder hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung

Präambel

In Anerkennung, dass Kleriker und sonstige Beschäftigte im Dienst der katholischen Kirche in Deutschland in der Vergangenheit Kinder, Jugendliche und schutz- oder hilfebedürftige Erwachsene sexuell missbraucht haben,

in der Absicht, das Leid der Betroffenen in den Fokus zu stellen, die strukturelle Beteiligung von Betroffenen am Prozess der Aufarbeitung zu sichern und ansprechbar zu sein für die Anliegen Betroffener und ihrer Angehörigen,

ferner in der Absicht, die Umstände von sexuellem Missbrauch in der Vergangenheit und in der Gegenwart in den Blick zu nehmen und die Aufarbeitung des sexuellen Missbrauchs insbesondere durch die quantitative Erhebung des sexuellen Missbrauchs, die Untersuchung des administrativen Umgangs mit Tätern und Betroffenen und die Identifikation von Strukturen, die sexuellen Missbrauch zugelassen oder erleichtert oder dessen Aufdeckung erschwert haben, sowie die qualitative Analyse der spezifischen Bedingungen des Entstehens und des Aufdeckens von Missbrauchsfällen zu ermöglichen,

zu dem Zweck, dem Gebot von Unabhängigkeit und Transparenz der Aufarbeitung Rechnung zu tragen sowie

unter größtmöglicher Wahrung der Privatsphäre und der Persönlichkeitsrechte betroffener Personen wird die folgende Ordnung erlassen:

§ 1 Geltungsbereich

Diese Ordnung regelt die Offenlegung von Unterlagen aller kirchlichen Rechtsträger und deren Einrichtungen in der Diözese Limburg, unabhängig von ihrer Rechtsform, in Form der Übermittlung (Auskunft) und in Form der Bereitstellung (Einsicht) gegenüber unabhängigen Aufarbeitungskommissionen, zu Forschungszwecken sowie gegenüber Rechtsanwaltskanzleien.

§ 2 Verhältnis zum KDG und zur KAO

Für die Verarbeitung personenbezogener Daten finden das Gesetz über den Kirchlichen Datenschutz (KDG) und die zu seiner Durchführung ergangenen Vorschriften, insbesondere die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO), sowie die Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche (Kirchliche Archivordnung – KAO) in ihrer jeweils geltenden Fassung Anwendung, soweit sich aus dieser Ordnung nichts Abweichendes ergibt. Die Vorschrift des § 2 Abs. 2 KDG bleibt unberührt.

§ 3 Begriffsbestimmungen

Im Sinne dieser Ordnung bezeichnet der Ausdruck

a) „Aufarbeitung" die Erfassung von Tatsa-

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifische Personenbezeichnungen differenziert. Die gewählte männliche Form schließt adäquate andere Formen gleichberechtigt ein.

Gesetz zur Änderung der Bistums-KODA-Ordnung

Artikel 1

(1) In der Präambel, Satz 2 wird „Art. 7" durch „Art. 9" ersetzt. Außerdem werden nach „Grundordnung des kirchlichen Dienstes" die Worte „im Rahmen kirchlicher Arbeitsverhältnisse" gestrichen.

(2) In § 3 Abs. 2 wird „§ 3 Abs. 1 Zentral-KODA-Ordnung" durch „§ 2 Abs. 1 ZAK-Ordnung" ersetzt. Weiterhin wird „Art. 7" durch „Art. 9" ersetzt.

(3) In § 3 Abs. 3 werden die Worte „Zentralen Kommission zur Ordnung des Arbeitsvertragsrechtes im kirchlichen Dienst (Zentral-KODA)" durch die Worte „ZAK (Zentrale Arbeitsrechtliche Kommission)" ersetzt. Ferner wird „§ 3 Abs. 3 Zentral-KODA-Ordnung" durch „§ 2 Abs. 3 ZAK-Ordnung" ersetzt.

(4) In § 17 S. 2 wird „Art. 5 Abs. 3 bis 5" durch „Art. 7 Abs. 3 bis 5" ersetzt.

(5) Im gesamten Ordnungstext wird „Zentral-KODA" durch „ZAK" ersetzt, namentlich in § 3 Abs. 1 und 2 sowie in § 19 Abs. 6.

Artikel 2
Inkrafttreten

Dieses Änderungsgesetz tritt zum 1. November 2024 in Kraft.

BO-Nr. 4729 – 09.10.2024

Ordnung[1]
zur Regelung von Einsichts- und Auskunftsrechten für die Kommission zur Aufarbeitung des sexuellen Missbrauchs in der Diözese Rottenburg-Stuttgart (Aufarbeitungskommission Diözese Rottenburg-Stuttgart – AK-DRS) sowie für Forschungszwecke in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung

Präambel

In Anerkennung, dass Kleriker und sonstige Beschäftigte im Dienst der katholischen Kirche in Deutschland in der Vergangenheit Kinder, Jugendliche und schutz- oder hilfebedürftige Erwachsene sexuell missbraucht haben, in der Absicht, das Leid der Betroffenen in den Fokus zu stellen, die strukturelle Beteiligung von Betroffenen am Prozess der Aufarbeitung zu sichern und ansprechbar zu sein für die Anliegen Betroffener und ihrer Angehörigen, ferner in der Absicht, die Umstände von sexuellem Missbrauch in der Vergangenheit und in der Gegenwart in den Blick zu nehmen und die Aufarbeitung des sexuellen Missbrauchs insbesondere durch die quantitative Erhebung des sexuellen Missbrauchs, die Untersuchung des administrativen Umgangs mit Tätern und Betroffenen und die Identifikation von Strukturen, die sexuellen Missbrauch zugelassen oder erleichtert oder dessen Aufdeckung erschwert haben, sowie die qualitative Analyse der spezifischen Bedingungen des Entstehens und des Aufdeckens von Missbrauchsfällen zu ermöglichen, zu dem Zweck, dem Gebot von Unabhängigkeit und Transparenz der Aufarbeitung Rechnung zu tragen sowie unter größtmöglicher Wahrung der Privatsphäre und der Persönlichkeitsrechte betroffener Personen wird die folgende Ordnung erlassen:

§ 1
Geltungsbereich

Diese Ordnung regelt die Offenlegung von Unterlagen aller kirchlichen Rechtsträger und deren Einrichtungen in der Diözese Rottenburg-Stuttgart, unabhängig von ihrer Rechtsform, in Form der Übermittlung (Auskunft) und in Form der Bereitstellung (Einsicht) gegenüber der AK-DRS und zu Forschungszwecken.

§ 2
Verhältnis zum KDG und zur KAO

Für die Verarbeitung personenbezogener Daten finden das Gesetz über den Kirchlichen Datenschutz (KDG) und die zu seiner Durchführung ergangenen Vorschriften, insbesondere die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO), sowie die Anordnung über die Sicherung und Nutzung der Archive der katholischen Kirche (Kirchliche Archivordnung – KAO) in ihrer jeweils geltenden Fassung Anwendung, soweit sich aus dieser Ordnung nichts Abweichendes ergibt. Die Vorschrift des § 2 Abs. 2 KDG bleibt unberührt.

§ 3
Begriffsbestimmungen

Im Sinne dieser Ordnung bezeichnet der Ausdruck

a) „Aufarbeitung" die Erfassung von Tatsachen, Ursachen und Folgen von sexuellem Missbrauch an Kindern, Jugendlichen und schutz- und hilfebedürftigen Erwachsenen in der katholischen Kirche zu dem Zweck, eine quantitative Erhebung des sexuellen Missbrauchs vorzunehmen, den administrativen Umgang mit Tätern und Betroffenen zu untersuchen und die Identifikation von Strukturen, die sexuellen Missbrauch zugelassen oder erleichtert oder dessen Aufdeckung erschwert haben, sowie die qualitative Analyse der spezifischen Bedingungen des Entstehens und des Aufdeckens von Missbrauchsfällen zu ermöglichen; dies kann auch anhand von Einzelfällen erfolgen;

b) „Unterlagen" die in Sachakten, Verfahrensakten, Registraturakten und vergleichbaren Aktenbeständen vorliegenden Aufzeichnungen jeglicher Art unabhängig von ihrer Speicherungsform sowie alle Hilfsmittel und ergänzenden Daten, die für Erhaltung, Verständnis und Nutzung dieser Informationen notwendig sind;

c) „AK-DRS" die unabhängige Kommission zur Aufarbeitung des sexuellen Missbrauchs auf der Ebene der Diözese, die aufgrund der von dem Diözesanbischof für seine Diözese verbindlich erklärten ‚Gemein-

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifische Personenbezeichnungen differenziert. Die gewählte männliche Form schließt adäquate andere Formen gleichberechtigt ein.

2.2.2 Gemeinsame Verantwortlichkeit bei „kitaplus“ in Rottenburg-Stuttgart

Darüber hinaus hat das Bistum Rottenburg-Stuttgart im April 2024 in seinem Amtsblatt Nr. 4/2024 (S. 138) Informationen zur gemeinsamen Verantwortlichkeit nach § 28 Abs. 2 S. 2 KDG beim Einsatz von „kitaplus“ veröffentlicht. Die Diözese führt das standardisierte Kindergartenverwaltungsprogramm „kitaplus“ und die zentrale Kindergartenverwaltungsplattform „drsKita“ in den Verwaltungszentren und ihren Kitas ein.

Das Bistum teilt auf diesem Wege mit, dass hinsichtlich der Verarbeitung von personenbezogenen Daten mittels „kitaplus“ eine Vereinbarung zwischen ihm, den Gesamtkirchengemeinden, Kirchengemeinden und Zweckverbänden abgeschlossen wurde, die die gemeinsame Verantwortlichkeit im Sinne des § 28 KDG als Träger der Kita-Einrichtungen festlegt.

Gesetzliche Verpflichtung	Zuständiger Verantwortlicher	
Information der betroffenen Personen	**Diözese**	**Träger**
Erfüllung der Informationspflichten nach §§ 14, 15 KDG	(+)	(+)
Erfüllung der Informationspflicht nach § 28 Abs. 2 S. 2 KDG	(+)	(+)
Rechte der Betroffenen		
Auskunftsverlangen nach § 17 KDG	(+)	(+)
Berichtigungsanfrage gemäß § 18 KDG	(+)	(+)
Löschungsanspruch gemäß § 19 KDG	(+)	(+)
Recht auf Einschränkung der Verarbeitung gemäß § 20 KDG	(+)	(+)
Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Sperrung gemäß § 21 KDG	(+)	(+)
Recht auf Datenübertragbarkeit gemäß § 22 KDG	(+)	(+)
Widerspruchsrecht gemäß § 23 KDG, einschließlich Hinweis auf das Widerspruchsrecht	(+)	(+)
Pflichten des Verantwortlichen		
Technische und organisatorische Maßnahmen gemäß § 26 KDG, § 6 KDG-DVO	(+)	(+)
Vertrag zur Auftragsverarbeitung gemäß § 29 KDG, § 15 Abs. 5 KDG-DVO	(+)	
Verzeichnis von Verarbeitungstätigkeiten gemäß § 31 KDG	(+)	(+)
Prüfung und Meldung von Datenpannen gemäß § 33 KDG	(+)	(+)
Prüfung und Benachrichtigung der betroffenen Person gemäß § 34 KDG	(+)	(+)
Datenschutz-Folgenabschätzung gemäß § 35 KDG	(+)	
Maßnahmen des Verantwortlichen gemäß § 15 KDG-DVO, Datenschutzkonzept	(+)	(+)

Es wird in diesem Zusammenhang ausdrücklich darauf hingewiesen, dass die von der Datenverarbeitung Betroffenen über den wesentlichen, die Verarbeitung personenbezogener Daten betreffenden Inhalt gemäß § 28 Abs. 2 S. 2 KDG zu informieren sind. Welche Informationen von jedem der gemeinsam Verantwortlichen zur Verfügung zu stellen sind, hat das Bistum detailliert vorgegeben (s. nebenstehende Tabelle).

2.2.3 Interne Meldestelle gemäß Hinweisgeberschutzgesetz im Bistum Rottenburg-Stuttgart

Des Weiteren hat das Bistum Rottenburg-Stuttgart im Berichtszeitraum unter anderem eine Verordnung zur Einrichtung einer internen Meldestelle gemäß Hinweisgeberschutzgesetz (HinSchG) in Kraft gesetzt: die Meldestellenordnung (MeldeStO).

Die Ordnung gilt für die Diözese, die Dekanate, die (Gesamt-)Kirchengemeinden, die kirchengemeindlichen Zweckverbände und ihre rechtlich unselbstständigen Einrichtungen. Betrieben wird die gemeinsame interne Meldestelle von der Diözese. Diese hat den Referenten für Beschwerdemanagement in der Stabsstelle Entwicklung im bischöflichen Ordinariat mit der Wahrnehmung der Aufgaben einer internen Meldestelle im Sinne des HinSchG betraut. Den Datenschutz bei der Verarbeitung insbesondere von besonderen Kategorien personenbezogener Daten regelt § 7 der Ordnung.

§ 3 Abs. 1 S. 2 MeldeStO weist ausdrücklich darauf hin, dass Rechtsträger mit eigener Website verpflichtet sind, auf ihrer Homepage auf diese Meldestelle hinzuweisen – und sie zu verlinken. Auch die entsprechende URL hierzu ist in dem Ordnungstext aufgeführt: drs.de/hinweisgeberschutz

2.2.4 Hinweis auf Widerspruchsrecht gegen Spendenaufrufe gemäß KDG

Das Bistum Rottenburg-Stuttgart bittet in einem seiner Amtsblätter schließlich noch alle Kirchengemeinden eindringlich, einmal jährlich in ihren Pfarrmitteilungen auf das Widerspruchsrecht gegen Spendenbriefe gemäß dem kirchlichen Datenschutzrecht hinzuweisen. Ein Thema, das gerne auch immer mal wieder das Kath. Datenschutzzentrum Frankfurt/M. beschäftigt.

Das Bistum stellt im Amtsblatt Nr. 8/2024 (S. 237) den Hinweistext zur Verfügung inklusive der rechtlichen Grundlagen und benennt konkret die Stelle im Bischöflichen Ordinariat in Rottenburg, an die der Widerspruch postalisch oder elektronisch zu richten ist.

2.2.5 Neuer Jubiläumserlass im Bistum Mainz

Das Bistum Mainz hat im Frühjahr 2024 im Amtsblatt Nr. 7 ein Ausführungsdekret zum KDG zur Veröffentlichung von Sakramentsspendungen sowie Alters- und Ehejubiläen, Geburten, Weihe-, Priester- und Ordensjubiläen und Sterbefällen erlassen.

Das Dekret findet seine Rechtsgrundlage in § 6 Abs. 1 lit. f) KDG – dem kirchlichen Interesse. Diese doch oft eher wackelige Grundlage bietet vorliegend jedoch ein solides Fundament. Denn gleich in der Präambel des Dekrets hat der Generalvikar diesbezüglich konkret das kirchliche Interesse begründet: „Es gehört zu den Aufgaben der Kirche und liegt zugleich im kirchlichen Interesse, die Gläubigen über die Spendung von Sakramenten, festlich begangene Jahrestage und Jubiläen sowie über freudige und schmerzliche Ereignisse zu informieren, um dadurch einerseits die Gemeinschaft der Gläubigen zu stärken und die Anteilnahme am Leben der Gläubigen in den Pfarreien, Gemeinden und weiteren Orten kirchlichen Lebens zu fördern, andererseits die Dienstgemeinschaft zu stärken und den Dienstnehmern, Priestern und Ordensleuten Wertschätzung entgegen zu bringen.“

Was an personenbezogenen Daten veröffentlicht werden darf, ist in dem Jubiläumserlass für die verschiedenen Personengruppen jeweils festgelegt. Betroffene Personen können gegen die Veröffentlichung von Jubiläen in den kircheneigenen Printmedien und kirchlichen Publikationen, im Kirchlichen Amtsblatt sowie auf den Websites der beteiligten kirchlichen Stellen jederzeit Widerspruch bei der zuständigen Pfarrei oder der Meldestelle im Bischöflichen Ordinariat einlegen.

Der Erlass regelt in § 3 Abs. 2 ausdrücklich, dass auf dieses Widerspruchsrecht mindestens einmal jährlich deutlich in den Publikationsorganen der Pfarreien hinzuweisen ist. Einen passenden Text hierzu liefert § 3 Abs. 3 des Erlasses gleich mit.

2.2.6 Neue datenschutzrechtliche Musterverträge zu den §§ 28 und 29 KDG im Bistum Fulda

Das Bischöfliche Generalvikariat Fulda informiert im Amtsblatt Nr. 11/2024 darüber, dass auf der Datenschutz-Website des Bistums neue Musterverträge zur gemeinsamen Verantwortlichkeit nach § 28 KDG sowie zur Auftragsverarbeitung nach § 29 KDG nebst einem Hinweisblatt für den dienstlichen Gebrauch zur rechtlichen Orientierung bei der Gestaltung von Verträgen hinsichtlich des Umgangs mit personenbezogenen Daten nunmehr zur Verfügung stehen.

Ergänzend weist die Stabsabteilung Recht in diesem Zusammenhang ausdrücklich darauf hin, dass Musterverträge, wie der Name schon sagt, nur allgemeine Regelungen beinhalten und im Falle spezifischer datenschutzrechtlicher Fragen der oder die betriebliche Datenschutzbeauftragte des Bistums oder die betriebliche Datenschutzstelle zur Unterstützung zu kontaktieren sind.

Bezüglich des Mustervertrags zur Auftragsverarbeitung stellt das Hinweisblatt klar, dass sich der Anwendungsbereich lediglich auf vertragliche Beziehungen zwischen dem Bistum Fulda und allen diözesanen Vereinen und Verbänden erstreckt. Für die Kirchengemeinden sowie für sonstige kirchliche öffentlich-rechtliche Einrichtungen im Fuldaer Bistum gelten hingegen die Bestimmungen des § 29-KDG-Gesetzes (das Kath. Datenschutzzentrum Frankfurt/M. berichtete hierüber in seinem Tätigkeitsbericht für das Jahr 2023, S. 19).

2.2.7 Virtuelle Sitzungen der DiAG-MAV Fulda

Die Diözesane Arbeitsgemeinschaft der Mitarbeitervertretungen im Bistum Fulda (DiAG-MAV Fulda) hat eine neue Geschäftsordnung bekommen, die unter der Nr. 81 im Kirchlichen Amtsblatt des Bistums Fulda 2024 veröffentlicht wurde.

Die DiAG-MAV nimmt auf diözesaner Ebene die Aufgaben gemäß § 25 Abs. 2 MAVO wahr. Ihre Organe sind: die Mitgliederversammlung und der Vorstand. Der Vorstand besteht aus fünf Mitgliedern und tritt in regelmäßigen Abständen zusammen. Nach § 6 der neuen Geschäftsordnung können die Sitzungen entweder in Präsenz oder auch als Telefon- bzw. Videokonferenz durchgeführt werden, wenn sichergestellt ist, dass Dritte von den Inhalten der Vorstandssitzung keine Kenntnis erlangen können.

Ausdrücklich geregelt ist auch, dass auf Antrag eines Vorstandsmitglieds die Sitzung in Präsenz durchgeführt werden soll, sofern keine wichtigen Gründe vorliegen, die eine Telefon- oder Videokonferenz erfordern.

Die neue Geschäftsordnung ist zum 1. Juli 2024 in Kraft getreten und ersetzt das bisherige Regelwerk.

2.2.8 Regelung zum Umgang mit Erweiterten Führungszeugnissen im Bistum Speyer aktualisiert

Das Bistum Speyer hat die bisherigen Regelungen zur Vorlagepflicht Erweiterter Führungszeugnisse umfassend erneuert. Das „Gesetz zur Regelung des Umgangs mit Erweiterten Führungszeugnissen für haupt-, neben- und ehrenamtlich Tätige im Bistum Speyer (EFZG)“ basiert auf den bisherigen Regelungen für Ehrenamtliche, nimmt aber auch die bislang nur durch Verwaltungsvorschriften geregelten Pflichten Hauptamtlicher, insbesondere auch der Geistlichen, mit auf. Nach Aussage von Generalvikar Markus Magin wurde mit dem EFZG „eine stringente und leicht nachvollziehbare einheitliche Regelung geschaffen“. Das Gesetz ist am 1. Juni 2024 in Kraft getreten. Wie es in der Präambel heißt, dient die Einforderung von Erweiterten Führungszeugnissen insbesondere der Prävention von sexuellen oder anderen Missbrauchshandlungen gegen Minderjährige oder erwachsene Schutzbefohlene im kirchlichen Raum.

Das neue Gesetz erweitert darüber hinaus die Vorlagepflichten. So sind nun einheitliche Regelungen für alle kirchlichen Rechtsträger in der Diözese geschaffen, auch über die Pfarreien hinaus. Vorlagepflichtig sind neben den Mitarbeitenden der Verwaltung des Bischöflichen Ordinariats, die Mitarbeiterinnen und Mitarbeiter im pastoralen Dienst, alle Priester sowie die von ihnen beschäftigten Personen sowie die Geistlichen aus anderen Bistümern einschließlich der Ruhestandsgeistlichen.

§ 6 EFZG stellt klar, dass das KDG neben dem EFZG natürlich uneingeschränkt gilt und die Verwendung der durch die Vorlage Erweiterter Führungszeugnisse gewonnenen Daten zu anderen Zwecken als der Sicherstellung des Schutzes Minderjähriger und erwachsener Schutzbefohlener nach dem EFZG unzulässig ist. Darüber hinaus weist die genannte Vorschrift in ihrem Absatz 3 ausdrücklich darauf hin, dass die mit der Sichtung dieser Führungszeugnisse beauftragten Beschäftigten im Bischöflichen Ordinariat „in besonderem Maße zur Einhaltung des Datenschutzes verpflichtet“ sind.

Im rheinland-pfälzischen Teil des Bistums Speyer ist alle fünf Jahre ein aktuelles Erweitertes Führungszeugnis vorzulegen und im saarländischen Teil bereits nach drei Jahren.

2.2.9 Neue Dienstordnung für Kita-Beschäftigte im Bistum Speyer

Die neue Dienstordnung regelt deutlich umfassender den Datenschutz und die Verschwiegenheitspflichten gegenüber bekannt gewordenen persönlichen Informationen von Kindern, deren Eltern und den Kita-Beschäftigten. Diese Verpflichtung besteht auch über die Beendigung des Dienstverhältnisses hinaus und ist durch die Unterzeichnung der entsprechenden Verpflichtungserklärung zum Datenschutz zu dokumentieren.

Bezüglich des Datenschutzes wird im Normtext unter der Nr. 28 ausdrücklich aufgeführt, dass die Mitarbeiterinnen und Mitarbeiter mit der Aufnahme der Beschäftigung „zur thematischen Sensibilisierung an der Datenschutz-Grundlagenschulung teilnehmen“ müssen.

Übernommen wurde aus der alten Regelung, dass die in den Kita-Einrichtungen anfallenden personenbezogenen Daten unter Verschluss aufzubewahren sind. Neu ist, dass der Dienstplan nunmehr „unter Berücksichtigung der Bestimmungen des Datenschutzes“ für alle Mitarbeitenden jederzeit einsehbar sein muss (Nr. 12).

Erstaunlich ist auf den ersten Blick, dass explizit ein Produkt in der neuen Dienstordnung erwähnt wird. So hat die Kita-Leitung die Urlaubsabwesenheit von Mitarbeiterinnen und Mitarbeitern zwingend in die Abwesenheitsübersicht in der Kita-Verwaltungssoftware „kitaplus“ aufzunehmen.

Die neue Ordnung gilt für alle Beschäftigten in den katholischen Kindertageseinrichtungen in Trägerschaft der Kirchengemeinden, der katholischen Krankenpflegevereine und der St. Elisabethenvereine auf dem Gebiet der Diözese Speyer. Aus Präventionsgesichtspunkten müssen alle pädagogischen – und nichtpädagogischen – Mitarbeiterinnen und Mitarbeiter entsprechend den gesetzlichen Regelungen ein Erweitertes Führungszeugnis (s. o.) sowie eine Selbstauskunftserklärung vorlegen.

Die neue Dienstordnung ist am 1. Juli 2024 in Kraft getreten und ersetzt die bisherige aus dem Jahr 2000. Sie ist im Amtsblatt für das Bistum Speyer Nr. 7/2024 unter der Nr. 40 veröffentlicht.

2.2.10 Informationen und Anweisungen zum Hinweisgebersystem im Bistum Trier

Das Bistum Trier hat in seinem Amtsblatt vom 1. April 2024 (Nr. 90) wesentliche Informationen zur Umsetzung des im Juli 2023 in Kraft getretenen Hinweisgeberschutzgesetzes bereitgestellt.

Die Infos zeigen auf, wann und unter welchen Voraussetzungen und durch welche Maßnahmen hinweisgebende Personen bei der Meldung geschützt sind. Die Information soll hauptamtliche und ehrenamtliche Mitarbeiterinnen und Mitarbeiter, die einen Hinweis abgeben wollen, ermutigen, Fehlverhalten intern zu melden. Ebenso steht der von der internen Meldestelle betriebene Meldekanal weiteren Personen, wie zum Beispiel Mitarbeitenden von Lieferanten oder Selbstständigen, zur Verfügung.

Das Bistum hat hierzu einen Link auf seiner Homepage implementiert, über den alle Meldenden – auch anonym – Hinweise über rechtswidrige Handlungen abgeben können:
https://bistum-trier.hintbox.de

In der Meldung sollten nach den Angaben in der Bekanntmachung möglichst alle Details der betreffenden Angelegenheit (betroffene Einrichtung, Identität von Beschuldigten, konkrete Schilderung des Schadensereignisses) und jeder verfügbare Beweis (Zeugen, Urkunden, Schriftverkehr) enthalten sein.

Gemeldet werden können begründete Verdachtsmomente oder tatsächliche oder bevorstehende Verstöße und missbräuchliches Verhalten im Rahmen einer beruflichen, dienstlichen oder unternehmerischen Tätigkeit. Die Handreichung benennt neben Verstößen gegen Strafvorschriften ausdrücklich auch solche gegen Regelungen des Datenschutzes und der IT-Sicherheit.

Fristen im Hinweisgeberverfahren werden ebenfalls aufgeführt. So hat die interne Meldestelle der hinweisgebenden Person spätestens nach sieben Tagen den Eingang zu bestätigen und gibt ihr innerhalb von drei Monaten nach der Eingangsbestätigung eine schriftliche Rückmeldung, die auch die Folgemaßnahmen sowie die Gründe für diese, soweit rechtlich möglich, enthält.

Hinweisgebende, die bewusst falsche Auskünfte geben, müssen mit rechtlichen Konsequenzen rechnen.

2.3 Ausgewählte Rechtsprechung staatlicher Gerichte

Der Europäische Gerichtshof (EuGH) hat auch im Berichtsjahr wieder wegweisende Urteile zur Klärung datenschutzrechtlicher Fragen gefällt.

So können sich nach einer Entscheidung des EuGH vom 11. April 2024, in der es erneut um Fragen zum datenschutzrechtlichen Schadensersatzanspruch ging, Arbeitgeber nicht einfach ihrer Verantwortung entziehen, indem sie pauschal auf einen Exzess eines Mitarbeiters verweisen (Az.: C-741/21).

Die Europarichter haben auf eine Vorlagefrage des Landgerichts (LG) Saarbrücken geurteilt, dass es für eine mögliche Befreiung des Verantwortlichen nach Art. 82 Abs. 3 DSGVO von seiner Haftung nicht ausreicht, dass er lediglich nachweist, er habe einer ihm unterstellten Person entsprechende Weisungen erteilt, diese Person habe diese aber nicht befolgt. Vielmehr habe sich der Verantwortliche zu vergewissern, dass seine Anweisungen zum korrekten Umgang mit personenbezogenen Daten eingehalten werden – beispielsweise durch entsprechende TOMs. Begründet wird dies mit dem DSGVO-Ziel eines hohen Schutzniveaus für Personen bei der Verarbeitung ihrer Daten, das im Folgenden noch des Öfteren genannt werden wird.

2.3.1 Anordnung von Datenlöschung ohne Antrag möglich

Im Frühjahr hat das Gericht bereits die Reichweite von Anordnungsbefugnissen von Datenschutzaufsichten aufgezeigt. Nach einem für die Praxis sehr relevanten Urteil vom 14. März 2024 (Az.: C-46/23) kann eine Aufsichtsbehörde eines EU-Mitgliedstaats zum Schutz personenbezogener Daten selbst dann die Löschung unrechtmäßig verarbeiteter Daten anordnen, wenn die betroffene Person zuvor gar keinen entsprechenden Antrag gemäß Art. 17 Abs. 1

DSGVO gestellt hat. Eine solche Löschung könne sich dabei sowohl auf bei der betroffenen Person erhobene als auch auf aus einer anderen Quelle stammende Daten beziehen.

Im zugrunde liegenden Fall beschloss eine ungarische Kommunalverwaltung im Jahr 2020, Personen, die zu einer von der Covid-19-Pandemie gefährdeten Gruppe gehörten, finanziell zu unterstützen. Sie ersuchte deshalb die ungarische Staatskasse und die Regierungsbehörde des IV. Bezirks der Hauptstadt Budapest, ihr die zur Prüfung der Anspruchsvoraussetzungen erforderlichen personenbezogenen Daten zu übermitteln.

Aufgrund eines Hinweises stellte die zuständige ungarische Datenschutzbehörde fest, dass sowohl die Verwaltung als auch die ungarische Staatskasse und die Regierungsbehörde gegen Regelungen der DSGVO verstoßen hatten. Entsprechende Geldbußen wurden verhängt. Die Datenschutzaufsicht stellte fest, dass die Verwaltung die betroffenen Personen innerhalb der dafür geltenden Frist von einem Monat weder über die Verwendung ihrer Daten und den Zweck dieser Verarbeitung noch über ihre Datenschutzrechte informiert hatte. Zudem wies sie die Verwaltung an, die Daten anspruchsberechtigter Personen, die keine Unterstützung beantragt hatten, zu löschen.

Die örtliche Verwaltung hat diese Entscheidung beim zuständigen ungarischen Gericht angefochten und geltend gemacht, die Aufsichtsbehörde sei nicht befugt, die Löschung personenbezogener Daten anzuordnen, wenn die betroffene Person zuvor keinen entsprechenden Antrag gestellt habe. Das ungarische Gericht ersuchte daraufhin den EuGH um Auslegung der DSGVO.

Der Gerichtshof stellt in seiner Antwort im Rahmen des Vorabentscheidungsverfahrens klar, dass die Aufsichtsbehörde eines Mitgliedstaats von Amts wegen die Löschung unrechtmäßig verarbeiteter Daten gemäß Art. 58 Abs. 2 lit. d) und g) DSGVO anordnen darf, also selbst dann, wenn die betroffene Person zuvor keinen entsprechenden Antrag gestellt hat, falls eine solche Maßnahme zur Erfüllung ihrer Aufgabe erforderlich ist, die darin besteht, über die umfassende Einhaltung der DSGVO zu wachen.

Erkennt die Aufsichtsbehörde, dass eine Datenverarbeitung nicht der DSGVO entspricht, so müsse sie dem festgestellten Verstoß abhelfen, und zwar auch dann, wenn die betroffene Person zuvor keinen Antrag gestellt hat. Denn das Erfordernis einer solchen Antragstellung würde bedeuten, dass der Verantwortliche bei fehlendem Antrag die betreffenden personenbezogenen Daten weiterhin speichern und unrechtmäßig verarbeiten dürfte.

Außerdem könne die Aufsichtsbehörde eines Mitgliedstaats die Löschung unrechtmäßig verarbeiteter Daten unabhängig davon anordnen, ob sie unmittelbar bei der betroffenen Person erhoben wurden oder aus einer anderen Quelle stammen.

2.3.2 Datenschutzanforderungen bei Kollektivvereinbarungen als Rechtsgrundlage

Eine weitere Entscheidung mit hoher praktischer Relevanz vor allem für Parteien von Betriebs- bzw. Dienstvereinbarungen hat der EuGH (Urteil vom 19. Dezember 2024, Az.: C-65/23) kurz vor Jahresende getroffen. Darin ging es um die Verarbeitung personenbezogener Daten im Beschäftigungskontext basierend auf einer kollektiven Vereinbarung als Rechtsgrundlage. Das Bundesarbeitsgericht (BAG) hatte dem EuGH diesbezüglich diverse Fragen zur Vorabentscheidung vorgelegt.

Vorliegend wurden Beschäftigtendaten eines Unternehmens in der neu eingeführten cloudbasierten Personalmanagementsoftware „Workday“ auf Grundlage einer Betriebsvereinbarung verarbeitet.

Der EuGH betonte in seiner Grundsatzentscheidung, dass dabei sämtliche Vorgaben der DSGVO zu erfüllen sind, das heißt, neben den spezifischen in Art. 88 Abs. 1 und 2 DSGVO und § 26 Abs. 4 BDSG vor allem auch jene zu den allgemeinen Grundsätzen für die Verarbeitung personenbezogener Daten in Art. 5 DSGVO, zum Erfordernis der Rechtmäßigkeit der Verarbeitung in Art. 6 Abs. 1 DSGVO und zur Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 1 und 2 DSGVO. Zudem stellte das Gericht klar, dass die Erforderlichkeit einer in einer Betriebs- oder Dienstvereinbarung festgelegten Datenverarbeitung voll gerichtlich überprüfbar ist.

Art. 88 DSGVO erlaubt danach also keine wesentlichen Abweichungen vom Schutzstandard der DSGVO. Der EuGH verweist in seiner Entscheidung auf das im Erwägungsgrund 10 genannte Ziel der DSGVO, ein hohes Schutzniveau für die Rechte und Freiheiten der von einer solchen Verarbeitung betroffenen Personen zu gewährleisten.

Die Parteien einer kollektivrechtlichen Vereinbarung verfügen demnach über einen gewissen Gestaltungsspielraum – allerdings nur in den Grenzen der DSGVO.

2.3.3 Gesundheitsdatenbegriff ist weit auszulegen

In einer weiteren Entscheidung aus dem Jahre 2024 hat der EuGH in seiner Begründung ebenfalls das DSGVO-Ziel der Gewährleistung eines hohen Niveaus des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres Privatlebens – bei der Verarbeitung sie betreffender personenbezogener Daten genannt und damit eine weite Auslegung des Begriffs „Gesundheitsdaten“ gemäß Art. 9 Abs. 1 DSGVO begründet.

Es genügt für den EuGH (Urteil vom 4. Oktober 2024, Az.: C-21/23) zur Einstufung von personenbezogenen Daten als Gesundheitsdaten im Sinne der DSGVO, „dass aus diesen Daten mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden kann“.

Konkret ging es im zugrunde liegenden Fall um einen Streit zwischen zwei Apotheken. Die eine verkaufte apothekenpflichtige, aber rezeptfreie Medikamente über die Online-Plattform Amazon, woraufhin die andere als Wettbewerberin dagegen Klage einreichte und diese unter anderem damit begründete, dass die Daten der Kunden nur mit deren ausdrücklicher Einwilligung hätten erhoben werden dürfen, weil es sich um besondere Kategorien personenbezogener Daten, mithin um Gesundheitsdaten gemäß Art. 9 Abs. 1 DSGVO, gehandelt habe.

Um folgende Angaben drehte es sich vor allem: Name, Lieferadresse und für die Individualisierung der Arzneimittel notwendige Informationen. Die EuGH-Richterinnen und -Richter sahen in den Kundendaten ebenfalls besonders schützenswerte Gesundheitsdaten, weil sie Aufschluss über die Gesundheit der Kunden geben können – selbst wenn der Verkauf dieser Arzneimittel keiner ärztlichen Verschreibung bedarf. Es habe folglich einer ordnungsgemäßen Einwilligung in die Verarbeitung der Gesundheitsdaten bedurft.

Es handelt sich hier um einen der eher seltenen Fälle, in denen sich das Gericht nicht einem Schlussantrag des Generalanwalts anschloss. Dieser kam zu dem gegenteiligen Ergebnis, dass die Bestelldaten in dieser Rechtssache keine Gesundheitsdaten im Sinne der DSGVO darstellten. Für ihn boten die vorhandenen Informationen nicht das erforderliche „Mindestmaß an Gewissheit“, um daraus Schlussfolgerungen auf den Gesundheitszustand der betroffenen Person zu ziehen.

„Es genügt für den EuGH zur Einstufung von personenbezogenen Daten als Gesundheitsdaten im Sinne der DSGVO, ‚dass aus diesen Daten mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden kann‘.“

2.3.4 Facebook-Scraping – Schadensersatz schon bei Kontrollverlust über Daten

Der Bundesgerichtshof (Urteil vom 18. November 2024, Az.: VI ZR 10/24) hat in einer Leitentscheidung, die richtungsweisend für tausende Klagen ist, erstmalig geurteilt, dass User nach einem Datendiebstahl auf einer Social Media-Plattform bereits allein aufgrund des Kontrollverlusts über ihre personenbezogenen Daten immateriellen Schadensersatz fordern können.

Hintergrund ist vorliegend ein Fall des sogenannten Web Scrapings. Unbekannte hatten im Frühjahr 2021 Daten des sozialen Netzwerks Facebook von ca. 533 Millionen Nutzerinnen und Nutzern aus 106 Ländern im Internet öffentlich verbreitet. Sie hatten sich zuvor den Umstand zunutze gemacht, dass die Netzwerkbetreiberin es in Abhängigkeit von den Suchbarkeitseinstellungen des jeweiligen Users ermöglicht, dass dessen Facebook-Profil mithilfe seiner Telefonnummer gefunden werden kann. Die Täter ordneten über die Kontakt-Import-Funktion Telefonnummern den zugehörigen Nutzerkonten zu und griffen die zu diesen Konten vorhandenen öffentlichen Daten ab.

Von diesem Scraping-Vorfall waren auch Daten des Klägers (Nutzer-ID, Vor- und Nachname, Arbeitsstätte und Geschlecht) betroffen, die auf diese Weise mit dessen Telefonnummer verknüpft wurden. Der Kläger machte geltend, die Beklagte habe keine ausreichenden Sicherheitsmaßnahmen ergriffen, um eine Ausnutzung des Kontakt-Tools zu verhindern. Ihm stehe wegen des erlittenen Ärgers und des Kontrollverlusts über seine Daten Ersatz für immaterielle Schäden zu. Darüber hinaus begehrte der Kläger unter anderem die Feststellung, dass Facebook verpflichtet sei, ihm in diesem Zusammenhang auch alle künftigen materiellen und immateriellen Schäden zu ersetzen.

Anders als die Vorinstanz gab der BGH dem Kläger in den genannten Punkten Recht. Nach der einschlägigen Rechtsprechung des EuGH könne gemäß Art. 82 Abs. 1 DSGVO auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die DSGVO einen immateriellen Schaden darstellen. Weder müsse insoweit eine konkrete missbräuchliche Verwendung dieser Daten zum Nachteil des Betroffenen erfolgt sein, noch bedürfe es sonstiger zusätzlicher spürbarer negativer Folgen. Das höchste deutsche Zivilgericht sieht vorliegend einen Schadensersatz für den bloßen Kontrollverlust in einer Größenordnung von 100 € als angemessen an, § 287 Zivilprozessordnung (ZPO).

Der BGH hat die Sache zur neuen Verhandlung und Entscheidung an das Berufungsgericht zurückverwiesen – verbunden mit dem Hinweis für die weitere Prüfung, dass die von Facebook vorgenommene Voreinstellung der Suchbarkeitseinstellung auf „alle“ nicht dem Grundsatz der Datenminimierung entsprochen haben dürfte und das Oberlandesgericht (OLG) Köln sich diesbezüglich mit der Frage nach einer wirksamen Einwilligung des Klägers in die Datenverarbeitung zu beschäftigen hat.

Leitsatz des Gerichts:
Immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO kann auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung sein. Weder muss eine konkrete missbräuchliche Verwendung dieser Daten zum Nachteil des Betroffenen erfolgt sein, noch bedarf es sonstiger zusätzlicher spürbarer negativer Folgen.
(BGH, Urteil vom 18. November 2024, Az.: VI ZR 10/24)

2.3.5 Namentliche Nennung des Datenschutzbeauftragten nicht erforderlich

Die Frage nach der Pflicht zur namentlichen Nennung der oder des betrieblichen Datenschutzbeauftragten wird dem Kath. Datenschutzzentrum Frankfurt/M. auch immer wieder gestellt und hat es im Berichtsjahr sogar bis zum BGH (Urteil vom 14. Mai 2024, Az.: VI ZR 370/22) geschafft.

Das höchste deutsche Zivilgericht hat dazu eindeutig entschieden. Der amtliche Leitsatz lautet diesbezüglich:

„Bei Mitteilung der Kontaktdaten des Datenschutzbeauftragten nach Art. 13 Abs. 1 lit. b) DSGVO ist die Nennung des Namens nicht zwingend. Entscheidend und zugleich ausreichend für den Betroffenen ist die Mitteilung der Informationen, die für die Erreichbarkeit der zuständigen Stelle erforderlich sind. Ist die Erreichbarkeit ohne Nennung des Namens gewährleistet, muss dieser nicht mitgeteilt werden."

Zur Begründung führt das Gericht aus, dass bereits nach dem Wortlaut des Art. 13 Abs. 1 lit. b) DSGVO keine Pflicht des Verantwortlichen zur namentlichen Nennung des Datenschutzbeauftragten besteht, sondern nur zur Mitteilung der Kontaktdaten. Der BGH schließt sich damit der überwiegenden Meinung in der einschlägigen Kommentarliteratur an.

> **„Auch nach Sinn und Zweck der Vorschrift bedürfe es einer Nennung des Namens nicht zwingend. Denn es komme nicht auf die Person, sondern auf deren Funktion an."**

Dafür spreche ebenfalls die Systematik des Gesetzes, das in unterschiedlichen Zusammenhängen die Mitteilung eines Namens ausdrücklich verlange, zum Beispiel in Art. 13 Abs. 1 lit. a) DSGVO und insoweit ersichtlich bewusst differenziere.

Auch nach Sinn und Zweck der Vorschrift bedürfe es einer Nennung des Namens nicht zwingend. Denn es komme nicht auf die Person, sondern auf deren Funktion an.

Entscheidend und zugleich ausreichend für den Betroffenen sei die Mitteilung von Informationen, wie die zuständige Stelle erreichbar ist. Ist die Erreichbarkeit ohne Nennung des Namens gewährleistet, müsse dieser nicht genannt werden. Im Übrigen habe die Information nach Art. 13 Abs. 1 lit. b) DSGVO zum Zeitpunkt der Erhebung der Daten zu erfolgen. In der Folgezeit könne es zu personellen Veränderungen kommen, weshalb eine namentliche Nennung die spätere Erreichbarkeit sogar erschweren könne.

Im Ausgangsverfahren hatte die Klägerin die beklagte Bank auf Auskunft über personenbezogene Daten in Anspruch genommen und in diesem Zusammenhang auch die namentliche Nennung ihres betrieblichen Datenschutzbeauftragten gefordert.

2.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte

2.4.1 Kirchlicher Datenschutz vs. Teufelsaustreibungen

Teufelsaustreibungen sind laut Wikipedia wieder en vogue, wenn auch Deutschland bei diesem Thema noch hinterherhinke. Ein Fall hat es im Berichtszeitraum sogar bis zum Interdiözesanen Datenschutzgericht (IDSG), geschafft (Beschluss vom 12. August 2024, Az.: IDSG 15/2023). Entsprechend spektakulär beginnt auch die Sachverhaltsdarstellung des Gerichts bei dieser Thematik:

„Der Beteiligte, ein ehemaliger Pfarrer im Erzbistum des Antragstellers, und XX führten eine Gruppe von Gläubigen an, die unter anderem mittels physischer und psychischer Gewalt bei anderen Gläubigen ‚Teufelsaustreibungen' vornahmen. Dies führten sie auch bei der Schwiegertochter von XX XX , XX XX XX , durch, die zusammen mit ihrem Ehemann und ihrem behinderten Sohn im Haus von XX XX wohnte. Der Beteiligte und XX XX waren der Auffassung, XX XX sei ‚vom Teufel besessen', möglicherweise auch deshalb, weil sie Mutter eines behinderten Sohnes ist. XX XX war verängstigt sowie in Sorge um ihren eigenen Leib und ihr eigenes Leben. Unter Zurücklassung ihres Sohnes floh sie ‚bei Nacht und Nebel' aus dem gemeinsam mit den Schwiegereltern bewohnten Haus. Wegen des Umgangs mit dem Sohn kam es in der Folgezeit zu Verfahren vor dem Jugendamt und dem Familiengericht. Im Rahmen der familienrechtlichen Auseinandersetzungen wandte sich der Beteiligte mit einem Schreiben an das Jugendamt, das er mit dem Titel ‚Pfarrer' unterschrieb. XX XX war inzwischen auch in Sorge um Leib und Leben ihres Sohnes, den sie bei XX XX zurücklassen musste."

Neben diesem beeindruckenden Fresko eines Exorzismus in der Kirche San Francesco in Montefalco bietet das pittoreske umbrische Hügelstädtchen hervorragende, gehaltvolle Rotweine, die auch schon erfolgreich für Teufelsaustreibungen genutzt worden sein sollen.

Jacopo Zabolino di Vinciolo, Fresko (Ausschnitt), 15. Jahrhundert, Nische des Heiligen Antonius von Padua, Kirche San Francesco, Montefalco, Italien

Daraufhin leitete das zuständige Erzbistum gegen diesen Beteiligten ein Verfahren ein. Ein beauftragter Weihbischof suchte das Gespräch mit der Betroffenen und teilte ihr bei dieser Gelegenheit den aktuellen Stand sowie die bereits ergriffenen Maßnahmen gegen den Exorzisten mit. Das hierzu angefertigte Protokoll fand im weiteren Verlauf Eingang in das familienrechtliche Verfahren.

Das Auskunftsersuchen des Beteiligten ließ nicht lange auf sich warten und damit der Schwenk vom Teufel zum Datenschutz – vom Dunkel ins Licht.

Das Erzbistum verlängerte die Frist gemäß § 14 Abs. 3 S. 2 KDG unter pauschaler Berufung auf die Komplexität des Antrags auf insgesamt drei Monate. Gegen die Fristverlängerung und später gegen die Weitergabe des Protokolls reichte der Beteiligte bei der zuständigen Datenschutzaufsicht Beschwerde ein. Diese gab ihm in diesen beiden Punkten auch Recht.

Die dagegen gerichtete Klage des Verantwortlichen hatte nur bezüglich der Fristverlängerung Erfolg. Das IDSG hat in dieser Entscheidung klargestellt, dass § 14 Abs. 3 S. 2 KDG dies nur zulässt, „wenn die Komplexität und die Anzahl kumulativ dies erfordern“. Auf die Voraussetzung der gleichzeitigen „Anzahl von Anträgen“ sei das Erzbistum in seiner Fristverlängerungsbegründung aber gar nicht näher eingegangen. Die Fristverlängerung sei lediglich eine Ausnahme von der Monatsregel. Ein Verantwortlicher müsse eben im Hinblick auf die zügige Bearbeitung von Auskunftsbegehren für eine „vorbereitende Organisation“ sorgen.

Die Weitergabe der personenbezogenen Daten des Beteiligten im überlassenen Protokoll stelle hingegen keine Datenschutzverletzung dar. Diese sei „insbesondere durch § 6 Abs. 2 lit. j) KDG gedeckt“. Die Verarbeitung für einen anderen Zweck, vorliegend also im Rahmen des familienrechtlichen Verfahrens, erforderten der Auftrag der Kirche und die Glaubwürdigkeit ihres Dienstes. Dies ergebe eine Abwägung des kirchlichen Interesses mit den Interessen der betroffenen Person. Bei der genannten Vorschrift handele es sich um einen Auffangtatbestand, der die kirchlichen Sonderinteressen berücksichtige und „noch innerhalb des durch Art. 91 Abs. 1 DSGVO eingeräumten Gestaltungsspielraums des kirchlichen Gesetzgebers liegt“.

Die Kirche müsse dem gravierenden Fehlverhalten des beteiligten Priesters im Rahmen der „Teufelsaustreibung“ entschieden entgegentreten und sich um die Opfer bemühen. Dies habe für „die Glaubwürdigkeit ihres Dienstes zentrale Bedeutung“ – vor allem in einer Zeit, „in der die Glaubwürdigkeit der Kirche massiv beschädigt ist“.

Aus der Begründung des Gerichts:
Der durch das Evangelium geprägte Auftrag der Kirche (vgl. can. 747 § 1 CIC) verlangt einen konsequenten Einsatz für den Opferschutz, der auch die Einbeziehung staatlicher Stellen umfassen kann.
(Quelle: IDSG, Beschluss vom 12. August 2024, Az.: IDSG 15/2023, Rn. 62)

2.4.2 Rechtswidrige Weiterleitung eines Attests an Gesundheitsamt

In einem anderen Fall hatte sich das IDSG (Beschluss vom 17. Juli 2024, Az.: IDSG 04/2021) mit der Weitergabe eines Attests einer Schülerin ohne deren Kenntnis bzw. die der Eltern an das zuständige Gesundheitsamt zu beschäftigen. Das Attest befreite die Schülerin vom Tragen eines Mund-Nasen-Schutzes in der Schule – ohne die erforderliche Nennung von Gründen. Die Schule hatte Zweifel an dem Attest und leitete eine nicht anonymisierte Kopie an das Amt weiter. Die zuständige Datenschutzaufsicht sah in dieser Übermittlung von personenbezogenen Gesundheitsdaten mangels Rechtsgrundlage einen Datenschutzverstoß und erteilte in dem zugrundeliegenden Bescheid an den Schulträger zugleich die Auflage, künftig in Zweifelsfällen über die Richtigkeit ärztlicher Atteste zur Befreiung von der Maskenpflicht diese dem Gesundheitsamt nur noch anonymisiert vorzulegen.

Knapp dreieinhalb Jahre nach Erlass des Bescheids, die Schülerin besuchte diese Schule schon lange nicht mehr, gab das Gericht im ersten Punkt der Aufsichtsbehörde Recht, bezüglich der Auflage jedoch nicht.

„Diese Anordnung ist nicht durch § 47 Abs. 5 Satz1 KDG gedeckt, wonach der Beanstandungsbescheid der Datenschutzaufsicht Anordnungen enthalten kann, um einen rechtmäßigen Zustand wiederherzustellen oder Gefahren für personenbezogene Daten abzuwehren“, so das IDSG in seiner Begründung. Die Anordnung sei zu diesem Zweck nicht geeignet. Zum einen handele es sich im vorliegenden Fall offensichtlich um ein unzureichendes, weil nicht qualifiziertes Attest und somit nicht um einen Zweifelsfall, der die Kontaktaufnahme mit dem Gesundheitsamt erfordert habe. Zum anderen komme eine Einschaltung des Gesundheitsamts in Zweifelsfragen zu Attesten nur in Betracht, wenn eine amtsärztliche Einschätzung nötig erscheine. Ob in diesem Zusammenhang eine Weitergabe von personenbezogenen Daten womöglich gerechtfertigt sei, bedürfe dann einer Prüfung im Einzelfall.

2.4.3 Erhebliches Interesse an Missbrauchsaufarbeitung

Auch mit Datenschutzfragen im Rahmen der kirchlichen Missbrauchsaufarbeitung hatte sich das IDSG (Beschluss vom 24. Februar 2024, Az.: IDSG 16/2021) im Berichtszeitraum auseinanderzusetzen. Geklagt hatte ein Priester, gegen den Missbrauchsvorwürfe erhoben wurden, die auch Eingang in ein veröffentlichtes Gutachten fanden, wegen der Nutzung seiner Daten in diesem Zusammenhang.

Seine personenbezogenen Daten wurden in dem von einer Anwaltskanzlei erstellten Gutachten zwar anonymisiert. Seiner Ansicht nach konnten aber „Insider“ ohne Weiteres aus den Angaben auf ihn schließen. Die hiergegen gerichtete Beschwerde blieb jedoch ebenso erfolglos wie die Klage beim IDSG. Der Priester legte gegen die Entscheidung zwar Rechtsmittel ein (Az.: DSG-DBK 03/2024), über die aber bis zum jetzigen Zeitpunkt noch nicht entschieden wurde. Dennoch soll wegen der grundlegenden Argumentation des Gerichts zum kirchlichen Interesse bei der Aufarbeitung des sexuellen Missbrauchs an dieser Stelle in aller Kürze auf diesen zentralen Punkt eingegangen werden.

Daneben beschäftigte sich das IDSG in seinem immerhin 32 Seiten umfassenden Beschluss noch mit zahlreichen weiteren datenschutzrechtlichen Fragen – beispielsweise zur Drittlandübermittlung von personenbezogenen Daten in den Vatikan.

Die Richter stellten mit deutlichen Worten dar, dass die Missbrauchsaufarbeitung ein erhebliches kirchliches Interesse darstellt, hinter dem Datenschutzrechte von Beschuldigten unter Umständen zurücktreten müssen.

Das Gericht sieht eine Rechtsgrundlage in der Verarbeitung der Daten des Priesters im Rahmen der Aufarbeitung in § 11 Abs. 2 lit. g) KDG, der insbesondere auf ein erhebliches kirchliches Interesse an der Verarbeitung abstellt. Nach dieser wenig genutzten Vorschrift ist eine – eigentlich gemäß § 11 Abs. 1 KDG untersagte – Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise erlaubt, wenn sie auf der Grundlage kirchlichen Rechts aus Gründen eines erheblichen kirchlichen Interesses erforderlich ist. Dieses kirchliche Recht hat nach der genannten Vorschrift in angemessenem Verhältnis zu dem verfolgten Ziel zu stehen, den Wesensgehalt des Rechts auf Datenschutz zu wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen.

Die Erforderlichkeit ergibt sich vorliegend für das Gericht aus der Pflicht der katholischen Kirche an der Missbrauchsaufarbeitung und der Wiederherstellung ihrer Glaubwürdigkeit: „Es entspricht einem erheblichen kirchlichen Interesse auf der Grundlage kirchlichen Rechts, neben der durch kirchliches und weltliches Strafrecht jeweils gebotenen Untersuchung eines Verdachts auf von einem Kleriker begangenen sexuellen Missbrauch Minderjähriger das Handeln und Unterlassen der Kirche in Bezug auf Verdachtsfälle sexuellen Missbrauchs sorgfältig durch fachlich Unabhängige untersuchen zu lassen und Untersuchungsvorgang wie -ergebnis zu veröffentlichen. Das Gebot der Aufklärung und Aufarbeitung besteht auf der Grundlage der Pflicht des Bischofs nach can. 391 § 1 CIC, seine Leitungsvollmacht nach Maßgabe des Rechts auszuüben und dabei gemäß can. 383 § 1 CIC alle ihm anvertrauten Gläubigen ohne Ansehen der Person gleich zu behandeln, um der Wahrung der Würde von durch Missbrauch und Vertuschung Betroffenen (vgl. can. 208 CIC) willen und aus wohlverstandener Kirchenraison, die auf Erfüllung des von Jesus Christus mit Einsetzung der Kirche gegebenen Auftrags gerichtet ist.“

2.4.4 Rückgriff auf staatliches Verwaltungsrecht geht in Ordnung

Das Datenschutzgericht der Deutschen Bischofskonferenz (DSG-DBK) hat im Berichtsjahr 2024 einen wichtigen Beschluss zur formellen und materiellen Rechtskraft von Entscheidungen der kirchlichen Datenschutzgerichte in zweiter Instanz gefällt (Beschluss vom 16. Januar 2024, Az.: DSG-DBK 02/2023) und auf seiner Website veröffentlicht (Aktenzeichen der ersten Instanz: IDSG 11/2022).

Darin stellen die Richter klar, dass aufgrund der lediglich „rudimentären“ prozessualen Regelungen in der Kirchlichen Datenschutzgerichtsordnung (KDSGO) bei Bedarf subsidiär

auf die staatliche Verwaltungsgerichtsordnung (VwGO) zurückgegriffen werden kann – und nicht etwa auf kirchliches Prozessrecht. Nur so könnten die rechtsstaatlichen Standards des staatlichen Rechts gesichert werden. Andernfalls gehe die kirchliche Gesetzgebung der ihr „durch Art. 91 DSGVO eingeräumten Gestaltungsoption verlustig".

Im Gegensatz dazu nehme das kirchliche Recht materiell mit dem KDG „eine Vollregelung des Datenschutzbereichs" vor.

Im zugrunde liegenden Fall ging es um einen Rechtsstreit anlässlich des Kirchenaustritts des Klägers. Hierzu hat dieser bereits ein früheres Verfahren durch beide Gerichtsinstanzen geführt – war aber jeweils mit seinem Plan, dass sich sein Kirchenaustritt auf das Ausscheiden aus der öffentlich-rechtlichen Körperschaft beschränkt und keine innerkirchlichen Wirkungen hat, gescheitert (s. zum Beschluss des IDSG vom 9. Dezember 2020, Az.: IDSG 05/2019: „Kein teilweiser Kirchenaustritt durch Datenschutz" – Tätigkeitsbericht 2020, S. 17 und zum Beschluss des DSG-DBK vom 16. September 2021, Az.: DSG-DBK 05/2020: „Teilweiser Kirchenaustritt geht nicht" – Tätigkeitsbericht 2021, S. 17). Diesmal ging es wieder um diesen Kirchenaustritt, nur stritten sich die Parteien jetzt über den gebotenen Wortlaut des Taufregistereintrags des erklärten Austritts. Dieser sollte geändert werden und das Gericht feststellen, dass der aktuelle Eintrag ihn in seinen Rechten verletzt.

Der Kläger scheiterte wiederum in beiden Instanzen. Zur Begründung verwies das DSG-DBK darauf, dass aufgrund der materiellen Rechtskraft des von ihm in zweiter Instanz bestätigten Beschlusses des IDSG vom 9. Dezember 2019 im Verfahren IDSG 05/2019 rechtskräftig feststehe, „dass dieser Eintrag im Taufregister im datenschutzrechtlichen Sinne richtig ist". Die materielle Rechtskraft dieses Beschlusses binde auch die Beteiligten in dem vorliegenden Verfahren.

Der Kläger bestritt die Rechtskraft des ersten Verfahrens mit Verweis auf die Möglichkeit, noch außerordentliche Rechtsmittel beim Papst einlegen zu können. Auch das Vorbringen des Klägers, dass das IDSG in seiner Entscheidung mit Normen der staatlichen Verwaltungsgerichtsordnung „völlig verfahrensfremde Vorschriften" angewandt habe, blieb im Ergebnis erfolglos.

Wie eingangs erwähnt, stellten die Richter in zweiter Instanz hierzu fest, dass das IDSG zu Recht die entscheidungserheblichen Fragen zu formeller und materieller Rechtskraft in dem angefochtenen Beschluss anhand der VwGO und der dazu entwickelten Dogmatik beurteilt hat.

Die Möglichkeit der Einlegung eines außerordentlichen Rechtsmittels bleibe dem Kläger im Übrigen unbenommen, ändere aber nichts an der Rechtskraft eines kirchengerichtlichen Urteils, welches wie hier „nicht mehr mit einem ordentlichen Rechtsmittel angefochten werden kann".

3 Schwerpunkte der Tätigkeiten im Berichtszeitraum

3.1 Datenschutzverletzungen

Die Zahl der im Kath. Datenschutzzentrum Frankfurt/M. im Berichtsjahr 2024 eingegangenen Datenschutzverletzungen war im Vergleich zum Vorjahr leicht rückläufig, es war ein Rückgang um knapp 8 Prozent zu verzeichnen.

Fast die Hälfte der Meldungen, nämlich 48 Prozent, stammten von Einrichtungen der Kinder- und Jugend- sowie Alten- und Behindertenhilfe, aus dem Bereich der verfassten Kirche ist der Anteil der gemeldeten Datenschutzverletzungen mit nur 8 Prozent dagegen sehr gering. Die Anzahl der Meldungen aus dem Gesundheitswesen ist nach dem Vorjahresanstieg wieder gesunken.

Bezogen auf die gemeldeten Themengebiete ist sowohl die Anzahl der gemeldeten Cyberattacken relativ konstant geblieben als auch die der durch den Dauerbrenner „offener E-Mail-Verteiler“ entstandenen Datenschutzverletzungen.

Die Bandbreite der Themen war so groß wie in den zurückliegenden Berichtszeiträumen auch: Von Einbrüchen in den verschiedensten Einrichtungen über Verluste von Akten, Mobiltelefonen und Digitalkameras bis hin zum Hochladen von Videos aus dem dienstlichen Kontext auf Snapchat, Instagram und TikTok war alles dabei.

Betrachtet man die Meldungen zum Hochladen von Videos in die eben genannten Portale, so lässt sich feststellen, dass nach wie vor häufig das Bewusstsein der Handelnden für das, was sie mit ihrem Tun anrichten und welchen datenschutzrechtlichen Verstoß sie begehen, völlig fehlt. Umso wichtiger erscheint die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für dieses Thema im Rahmen von Datenschutzschulungen, denn nicht selten werden Verstöße dieser Art auch mit arbeitsrechtlichen Maßnahmen bis hin zur fristlosen Kündigung geahndet.

> **„Hochladen von Videos aus dem dienstlichen Kontext auf Snapchat, Instagram und TikTok – nicht selten werden Verstöße dieser Art auch mit arbeitsrechtlichen Maßnahmen bis hin zur fristlosen Kündigung geahndet.“**

Auch wenn Klebeband preiswerter als Porto und Sparsamkeit am Arbeitsplatz sicherlich eine Tugend ist, so handelt es sich bei der Rückgabe von Bewerbungsunterlagen in einem bereits benutzten und lediglich mit Klebeband verschlossenen Briefumschlag um eine Datenschutzverletzung. Der Umschlag wurde der Bewerberin durch einen unbeteiligten Dritten übergeben, die Einsichtnahme durch Unbefugte in die im Umschlag befindlichen Unterlagen war demzufolge möglich.

Nicht unüblich ist die Mitnahme der ausgehenden Post durch einen Mitarbeiter oder eine Mitarbeiterin nach Dienstschluss und der anschließende Einwurf in einen Briefkasten der Post. Wenn dabei allerdings ein für die Hausbank bestimmter und vollständig ausgefüllter Überweisungsträger ebenfalls in den Briefkasten gerät, so handelt es sich um die uner-

laubte Offenlegung personenbezogener Daten und mithin um eine Datenschutzverletzung. Als Folge dieses Vorfalls soll in der betreffenden Einrichtung zunehmend Online-Banking genutzt werden, weiterhin notwendige papierhafte Überweisungsträger werden zukünftig stets in einem beschrifteten und verschlossenen Umschlag transportiert.

3.1.1 Netzwerkanschluss: Wem gehört er und wie viele Nutzer gibt es eigentlich?

Bei Umbaumaßnahmen in einem von mehreren Einrichtungen genutzten Gebäude wurde ein Router durch einen der Nutzer zurückgesetzt und neu konfiguriert, ohne jedoch zuvor sicherzustellen, wem dieser Router denn eigentlich gehört. Auch die Tatsache, dass niemand über die Zugangs- und Nutzungsdaten für den Router verfügt, hat die Beteiligten von einer Neukonfiguration nicht abgehalten. Nach deren Durchführung war der Router nicht mehr zugriffsgesichert und auf die Daten der Besitzerin des Routers – die im Gebäude ansässige Kindertagesstätte – hätten unberechtigte Zugriffe erfolgen können.

Dieser Umstand ist allerdings erst bei einer Jahre später durchgeführten Netzwerkwartung aufgefallen, durch die sich herausstellte, dass alle Einrichtungen im Gebäude ihren gesamten Datenverkehr lange Zeit über diesen ungesicherten Router abgewickelt hatten. Nach Bekanntwerden des Gesamtszenarios wurden umgehend die notwendigen technisch-organisatorischen Maßnahmen, wie die Aufbewahrung des Routers in einem verschließbaren Netzwerkschrank sowie das Vornehmen der entsprechenden Einstellungen im Router, eingeleitet.

Auch wenn es zu keiner unmittelbaren Datenschutzverletzung gekommen ist, so bleibt doch zu konstatieren, dass die regelmäßige Prüfung von Zutritts-, Zugangs- und Zugriffsmöglichkeiten zu Netzwerkeinrichtungen unerlässlich ist.

3.1.2 Ein alter Brauch: Das Vergraben der Plazenta – aber bitte nur die eigene!

Das Vergraben der Plazenta und anschließend darauf einen Baum zu pflanzen, ist ein bekannter Brauch. Doch soll es sich natürlich um die eigene Plazenta handeln. Im vorliegenden Fall wurde einem jungen Paar im Krankenhaus eine eingefrorene Plazenta mitgegeben, die – wie sich beim Auftauen herausstellte – mit dem Patientinnenaufkleber einer anderen Frau versehen war. Die Recherche ergab aufgrund der Geburtszeit, dass es sich um die richtige Plazenta handelte, die jedoch mit einem falschen Aufkleber versehen worden war.

Durch die auf dem Aufkleber vorhandenen besonderen Kategorien personenbezogener Daten der anderen Mutter, die dem jungen Paar auf diese Weise unberechtigt zur Kenntnis gelangt sind, handelte es sich hier um eine Datenschutzverletzung.

Um zukünftig den Vorgang des Plazentaeinfrierens datenschutzsicher zu gestalten, wurde im betreffenden Krankenhaus der gesamte Prozess in einer Arbeitsanweisung verschriftlicht und die Mitarbeiterinnen und Mitarbeiter im Kreißsaal wurden entsprechend geschult.

3.1.3 Mitteilung einer geänderten Kontoverbindung: Das nächste Gehalt erhält dann ein Betrüger

Gleich von zwei der Zuständigkeit des Kath. Datenschutzzentrums Frankfurt/M. unterliegenden Einrichtungen wurden gleichlautende Datenschutzverletzungen gemeldet. Der Personalabteilung wurde per E-Mail die angebliche Änderung einer Kontoverbindung mitgeteilt, um eine Gehaltszahlung in betrügerischer Absicht umzuleiten. In beiden Fällen wurde von der jeweiligen Personalabteilung die Änderung der Kontoverbindung durchgeführt und die Gehaltszahlungen auf fremde Konten veranlasst. Da die Betrüger nach den erfolgreichen Überweisungen unmittelbar über die Beträge verfügen konnten, waren Rückforderungen nicht möglich.

Bei Kontoverbindungsdaten handelt es sich gemäß KDG-DVO um personenbezogene Daten der Datenschutzklasse III. Zur Vermeidung einer wie hier beschriebenen Datenschutzverletzung, wird dringend geraten, einen Prozess zu etablieren, der bei Änderung von Kontoverbindungsdaten die Identifizierung eines Beschäftigten eindeutig zulässt. Wird die Änderung einer Kontoverbindung per E-Mail mitgeteilt, so genügt dabei als eindeutige Identifizierung nicht, dass es sich bei der Absenderadresse um eine dienstliche E-Mail-Adresse handelt. Auch diese E-Mail-Adresse könnte in krimineller Absicht verändert und zu Betrugszwecken eingesetzt worden sein.

Eine telefonische Nachfrage beim Beschäftigten oder die zwingende postalische Form für die Mitteilung einer geänderten Kontoverbindung stellen dagegen sicherere Identifizierungsprozesse dar, die von der Datenschutzaufsicht empfohlen wurden.

3.2 Beschwerden

Die Zahl der Beschwerden war gegenüber dem Vorjahreszeitraum nahezu konstant. Unzureichend oder gar nicht erteilte Auskunftsersuchen waren auch im Jahr 2024 häufig Gegenstand einer Beschwerde, der Anteil der Beschwerden aus dem Gesundheitsbereich hat sich leicht verringert.

3.2.1 Auf die Endung kommt es an

Dopplungen bei E-Mail-Adressen sind nicht möglich, denn eine bereits vergebene Adresse kann kein zweites Mal angelegt werden. Allerdings gibt es Anbieter, die verschiedene Endungen für E-Mail-Adressen anbieten, so im hier beschriebenen Fall „.com“ und „.net“. Bei Gleichheit von Vor- und Nachnamen der E-Mail-Adressen-Inhaber kann dies zu Verwechslungen führen und damit auch zu einer Beschwerde beim Kath. Datenschutzzentrum Frankfurt/M. Überdies handelte es sich bei der betroffenen E-Mail-Adresse um eine private, die aber überwiegend im dienstlichen, hier auch im seelsorgerischen, Kontext genutzt wurde.

„muster@adresse.net oder muster@adresse.com – ein kleiner, aber wichtiger Unterschied!“

Der Beschwerdeführer erhielt über einen langen Zeitraum hinweg die verschiedensten E-Mails des Namensvetters. Der permanente Erhalt von fremden E-Mails ist nicht nur unschön und nervig, sondern diese enthalten gelegentlich auch Inhalt, der personenbezogene Daten von Dritten offenbart. Neben der Betrachtung der datenschutzrechtlichen Aspekte war die Datenschutzaufsicht in diesem Fall vor allem auch damit befasst, zu klären, warum dem Eigentümer der E-Mail-Adresse nicht daran gelegen war, in dieser seit Langem andauernden und misslichen Situation für Abhilfe zu sorgen. Zum einen hätte dies durch die Information der Absender (bei denen es sich zu einem guten Teil um einen „festen Kreis“ handelte) geschehen können, zum anderen vor allem durch die ausschließliche Nutzung der dienstlichen E-Mail-Adresse im dienstlichen Umfeld.

3.2.2 Datenschutz als Vorwand? Rechtsmissbräuchliches Vorgehen ist manchmal nicht ausgeschlossen

Die Weitergabe personenbezogener Daten ohne Rechtsgrundlage ist gemäß § 6 KDG nicht gestattet. Im vorliegenden Fall reichte ein Vater Beschwerde bei der Datenschutzaufsicht ein, weil im Rahmen eines Sorgerechtsstreits seine personenbezogenen Daten in Form von Protokollen eines Beratungsdienstes an das Amtsgericht weitergegeben wurden, obwohl er dazu keine explizite Einwilligung erteilt habe.

Die Übermittlung der Daten erfolgte jedoch auf Grundlage einer gerichtlichen Vereinbarung. In dieser waren die Modalitäten zum Umgang von Vater und Kind festgelegt, die im Rahmen eines Vergleichs über einen bestimmten Zeitraum hinweg beobachtet und vom Gericht bewertet werden sollten, bevor das Verfahren endgültig als abgeschlossen betrachtet werden konnte.

Das Kath. Datenschutzzentrum Frankfurt/M. sah eine explizite Einwilligung zur Weitergabe der Daten an das Amtsgericht nicht als erforderlich an, da die Regelungen zum Umgang und zur anschließenden Bewertung bereits in der gerichtlichen Vereinbarung festgehalten worden waren. Eine Bewertung durch das Gericht unter Einbeziehung des entsprechenden Beratungsdienstes kann jedoch nur unter Verwendung der Protokolle, die die fraglichen personenbezogenen Daten enthalten, erfolgen, da nur diesen der Sachverhalt im Detail zu entnehmen ist.

Der Beschwerde wurde durch die Aufsichtsbehörde nicht stattgegeben.

3.3 Anfragen

Die Anzahl der im Kath. Datenschutzzentrum Frankfurt/M. im Jahr 2024 eingegangenen Anfragen hat sich gegenüber den Vorjahreszeiträumen leicht verringert. Die Anfragen wurden wieder aus den verschiedensten Aufgabenbereichen der katholischen Datenschutzaufsicht gestellt: Gesundheitswesen, Kinder- und Jugendhilfe, Kirchengemeinden, Schulen und Altenhilfe.

Eine Tendenz zu vorherrschenden Themen bei den eingegangenen Anfragen war nicht festzustellen – vom Einsatz einer Übersetzungs-App über die Ausgestaltung datenschutzrechtlicher Formulare und Fragen verschiedene Aufbewahrungsfristen betreffend bis hin zu konkreten Anfragen zum Einsatz eines Videokonferenz-Tools war alles dabei.

Einmal mehr musste bei verschiedenen Anfragen klargestellt werden, dass seitens der Datenschutzaufsicht keine Produktempfehlungen oder -freigaben erteilt werden.

3.4 Gerichtsverfahren

Im Berichtsjahr sind einige wenige Klagen gegen (Bußgeld-)Bescheide des Kath. Datenschutzzentrums Frankfurt/M. dazugekommen und einige konnten durch Vergleich oder Rücknahme abgeschlossen werden. Bei einer Klage ging es eigentlich um die niedrigere Eingruppierung einer Beschäftigten nach einem Jobwechsel. Angeblich hätten sich der alte und der neue Arbeitgeber hierüber heimlich – und damit datenschutzwidrig – ausgetauscht. Rechtswidrige Anhaltspunkte hierzu konnte die Datenschutzaufsicht jedoch nicht feststellen – was die Petentin naturgemäß ganz anders sah. Ihre daraufhin eingereichte Klage enthielt weder einen Antrag noch eine Begründung oder gar den angefochtenen Bescheid.

Ein weiteres zweitinstanzliches Verfahren konnte nach mehreren Anläufen mit einem Vergleich erledigt werden, ohne dass das Kath. Datenschutzzentrum Frankfurt/M. letztlich inhaltlich substanziell wesentlich von seinem Tenor im streitgegenständlichen Bescheid abgewichen wäre. Vor dem DSG-DBK sind nach wie vor zwei Alt-Verfahren anhängig. In dem einen Verfahren ist von den ursprünglich Beteiligten nur noch die Datenschutzaufsicht übrig, denn sowohl die Geschäftsführung der Einrichtung und deren betrieblicher Datenschutzbeauftragter als auch der Petent, der dort einmal beschäftigt war, haben bzw. mussten den Betrieb zwischenzeitlich verlassen.

In dem anderen älteren Verfahren, das mittlerweile zahlreiche Aktenordner umfasst, hat das IDSG den Antrag der Petentin gleich an der Antragsbefugnis scheitern lassen. Ob zu Recht, wird sich irgendwann in der zweiten Instanz zeigen.

3.5 Prüfungen

Die Überprüfungs- und Kontrollaktivitäten wurden auch im Jahr 2024 wieder wie vom Gesetz ausdrücklich vorgesehen fortgesetzt. Bereits laufende Prüfungen konnten im Berichtsjahr abgeschlossen und neue, teils sehr umfangreiche Prüfungen, beispielsweise von 240 Schul-Websites oder von Pflegeheimen, durchgeführt werden. Die letztgenannten Außenprüfungen bestanden aus ganztägigen Besuchen vor Ort in den Einrichtungen, denen eine Begutachtung der zuvor eingereichten Unterlagen voranging und sich eine Gesamtbetrachtung und -bewertung anschloss. Da den Mitarbeiterinnen und Mitarbeitern des Kath. Datenschutzzentrums Frankfurt/M. im Rahmen solcher Überprüfungen immer wieder die Frage gestellt wird, weshalb man „gerade“ auf diese oder jene Einrichtung gekommen ist, sei an dieser Stelle gesagt, dass bei anlasslosen Prüfungen der Zufall entscheidet, in welcher Einrichtung zwischen Bodensee und Kassel nach dem Rechten geschaut wird.

Anders verhielt es sich beispielsweise bei einem großen Krankenhaus, welches aus gegebenem Anlass geprüft wurde. Dessen Website wies aus Datenschutzsicht erhebliche Mängel auf und bedurfte einer dringenden Überarbeitung. Diese Aktualisierung des „elektronischen Aushängeschilds“ des Klinikums wurde vom Verantwortlichen in enger Absprache mit der Datenschutzaufsicht angegangen, damit der Internetauftritt samt Datenschutzerklärung künftig den datenschutzrechtlichen Maßgaben entspricht.

3.6 Umfragen

▶ Pressemitteilung des KDSZ Frankfurt/M.

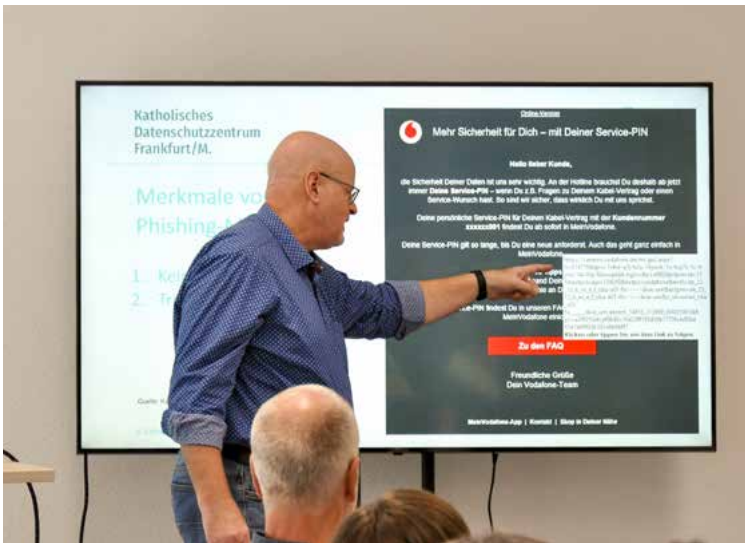
Die Katholische Datenschutzaufsicht Nord und das Kath. Datenschutzzentrum Frankfurt/M. haben im Juli 2024 gemeinsam eine Sensibilisierungskampagne unter den kirchlichen Einrichtungen gestartet. Da sich in Prüfungen und Beschwerdeverfahren gezeigt hat, dass einige Einrichtungen noch immer kein geregeltes Verfahren zum Umgang mit Datenschutzverletzungen haben, werden im Rahmen dieser Maßnahme über 100 Verantwortliche aus allen thematischen Gebieten der Zuständigkeitsbereiche aufgefordert, an einer Online-Umfrage hierzu teilzunehmen.

Primär sollen durch diese Umfrage die Einrichtungen und ihre Mitarbeitenden sensibilisiert werden, darüber hinaus können die gegebenenfalls festgestellten Defizite Hinweise für künftige Tiefenprüfungen geben.

Der Gesamtzeitraum der Kampagne wird sich über ein Jahr erstrecken, über Ergebnisse und daraus resultierende Schritte der Aufsichtsbehörden wird im nächsten Tätigkeitsbericht zu lesen sein.

4 Veranstaltungen und Öffentlichkeitsarbeit

Im Berichtszeitraum wurden wieder Schulungs- und Fortbildungsveranstaltungen angeboten, die sich großer Nachfrage erfreuten. So konnte beispielsweise das regelmäßig im Jahresrhythmus stattfindende Treffen mit den betrieblichen Datenschutzbeauftragten der Bischöflichen Ordinariate inhouse in den neuen Räumlichkeiten am Frankfurter Roßmarkt stattfinden. Für das Treffen mit den betrieblichen Datenschutzbeauftragten aus dem Caritas-Bereich musste jedoch aus Platzgründen ins nicht weit entfernte Dominikanerkloster ausgewichen werden. Thematisch drehte es sich bei diesen beiden Austauschtreffen im Frühherbst 2024 vor allem um das Kirchliche Datenschutzmodell (KDM) und um das Erkennen bzw. Vermeiden der bereits seit einiger Zeit verstärkt auftretenden Phishing-Attacken für kleine und große Einrichtungen im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. Vorab wurden erfreulicherweise wieder zahlreiche Themen für einen angeregten fachlichen Austausch untereinander eingereicht. Die Anregungen zeigten dabei einmal mehr eine sehr große thematische Bandbreite und reichten von der Jubiläumsordnung über den Umgang mit KI- und Übersetzungs-Tools und dem Einsatz von Sprachassistenten wie beispielsweise „Alexa“ im Pflegebereich bis hin zu möglichen immateriellen Schadensersatzansprüchen bei nicht fristgerecht beantworteten Auskunftsersuchen.



Referentinnen und Referenten des KDSZ Frankfurt/M. informierten auch im Berichtsjahr die interessierte Zuhörerschaft auf verschiedenen Veranstaltungen beispielsweise über die Verhinderung von Phishing-Attacken und den Umgang mit Auskunftsersuchen.

Gerne beteiligte sich das Kath. Datenschutzzentrum Frankfurt/M. auch wieder am Austauschforum Datenschutz des DiCV Rottenburg-Stuttgart im ersten Quartal 2024. Dieses Mal gaben die Referentinnen und Referenten der Datenschutzaufsicht einen umfassenden Überblick zum allgegenwärtigen datenschutzrechtlichen Auskunftsrecht unter besonderer Berücksichtigung der aktuellen kirchlichen und staatlichen Rechtsprechung und zum Begriff der Verfahrensbeteiligten in aufsichtlichen und in sich anschließenden gerichtlichen Datenschutzangelegenheiten.

Die Mitarbeiterinnen und Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. nahmen im Berichtsjahr Fortbildungsmöglichkeiten im Datenschutz wahr und folgten auch gerne Einladungen zu Veranstaltungen wie zum Beispiel dem feierlichen Festakt zum 50. Jubiläum des rheinland-pfälzischen Landesdatenschutzgesetzes.

5 Vernetzung mit anderen Datenschutzaufsichten

Der intensive Austausch unter den fünf katholischen Datenschutzaufsichten wurde auch im Berichtszeitraum fortgesetzt. Sprecherin der Konferenz der Diözesandatenschutzbeauftragten war Frau Becker-Rathmair vom Kath. Datenschutzzentrum in Frankfurt am Main. So fand denn auch die Herbstkonferenz in den Frankfurter Räumlichkeiten statt – mit anschließender Stadtführung und Verkostung des Frankfurter Nationalgetränks „Ebbelwoi".

Gleich zu Beginn des Jahres besuchten die Juristinnen und Juristen aus Frankfurt die Kollegen vom Kath. Datenschutzzentrum Bayern in ihren neuen Räumlichkeiten in der pittoresken Nürnberger Altstadt und die Kolleginnen und Kollegen von der Katholischen Datenschutzaufsicht Nord aus Bremen kamen kurze Zeit später zur fachlichen Diskussion für zwei intensive Tage in Frankfurt am Main vorbei.

Der Austausch mit den staatlichen Datenschutzaufsichten der Bundesländer Baden-Württemberg, Hessen, Rheinland-Pfalz und Saarland setzte sich wie gewohnt und fruchtbar fort, wobei es sich Herr Prof. Kugelmann, der rheinland-pfälzische Landesdatenschutzbeauftragte, erfreulicherweise nicht nehmen ließ, einmal vor Ort in Frankfurt/M. vorbeizuschauen und sich die neuen Räumlichkeiten anzusehen.

Weitere Austausche fanden beispielsweise mit Herrn Prof. Meckel von der Philosophisch-Theologischen Hochschule Sankt Georgen in deren Räumen im Süden Frankfurts statt.

Der regelmäßige Austausch mit den evangelischen Kolleginnen und Kollegen fand im Jahr 2024 unter anderem auf dem Ökumenischen Datenschutztag statt, zu dem der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland, Herr Jacob, nach Erfurt ins Augustinerkloster eingeladen hatte. Ein Thema war dort der Einsatz von Künstlicher Intelligenz (KI) in kirchlichen und caritativen bzw. diakonischen Einrichtungen. Es bestand Einigkeit, dass diese wichtige Thematik weiter gemeinsam bearbeitet werden soll.

Weiterhin nahmen Mitarbeiterinnen und Mitarbeiter der katholischen Datenschutzaufsichten an Sitzungen der Arbeitskreise der Datenschutzkonferenz teil. Im Rahmen des Arbeitskreises (AK) Technik trafen sich beispielsweise IT'ler der staatlichen und kirchlichen Aufsichten zu mehrtägigen intensiven Austauschveranstaltungen, unter anderem zur Prüfung von Android-Apps oder IoT-Geräten, an denen auch IT-Referenten aus Frankfurt/M. teilgenommen haben.

6 Hinweise und Arbeitshilfen des Kath. Datenschutzzentrums Frankfurt/M.

Im Berichtsjahr 2024 hat das Kath. Datenschutzzentrum Frankfurt/M. seinen Einrichtungen im Zuständigkeitsbereich auch wieder praktische Hinweise zu aktuellen Datenschutzthemen auf Veranstaltungen und der Homepage gegeben.

6.1 Steht Datenschutz im Grundgesetz? Sicher! 23. Mai 2024 – Das Grundgesetz wird 75

Am 23. Mai 1949 wurde das Grundgesetz der Bundesrepublik Deutschland verkündet und trat einen Tag später in Kraft. Seit diesem Tag ist dessen Artikel 1 Absatz 1 das Maß allen staatlichen Handelns und ist und bleibt die Nummer 1 in unserer Verfassung: die Unantastbarkeit der Menschenwürde. Aus diesem Grundsatz leiten sich die weiteren Grundrechte ab – so auch das auf Datenschutz.

Dies hat das Bundesverfassungsgericht erstmals im Volkszählungsurteil aus dem Jahr 1983 festgestellt. Das höchste deutsche Gericht entwickelte aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 Grundgesetz, in Verbindung mit Art. 1 Abs. 1 Grundgesetz das Grundrecht auf informationelle Selbstbestimmung. Jeder und jede darf demnach grundsätzlich selbst über die Preisgabe und Verwendung der persönlichen Daten entscheiden. Der Datenschutz in Deutschland erfuhr durch diesen Grundsatz eine deutliche Bedeutungssteigerung und hat den Datenschutz maßgeblich geprägt. Datenschutzgesetze sowohl auf nationaler als auch auf EU-Ebene wurden erarbeitet, damit jeder vor unbefugter Erhebung, Verarbeitung und Speicherung seiner persönlichen Daten geschützt ist.

Datenschutz ist seitdem unerlässlicher Bestandteil des Rechts auf freie Entfaltung der Persönlichkeit und auf Schutz der individuellen Freiheit – und ist insofern konsequenterweise im Grundgesetz zu finden.

6.2 Entschließung der DSK vom 15. Mai 2024 „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern“

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf die notwendige Auseinandersetzung mit den datenschutzrechtlich relevanten Auswirkungen der für die Zukunft zu befürchtenden weiteren Krankenhausschließungen hin.

Details finden sich in der Entschließung der DSK vom 15.05.2024 „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern“.

▶ Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern

6.3 Sicherheitslücke bei der KiTa-App „Stay Informed“

Bereits im März 2024 hielt das Kath. Datenschutzzentrum Frankfurt/M. seine Einrichtungen über die Homepage zu der Datenpanne beim Anbieter der KiTa-Verwaltungs-App „Stay Informed“ auf dem Laufenden (Stand: April 2024):

Wie zumeist durch verschiedene Presseveröffentlichungen bekannt, wurde in der vergangenen Woche eine Sicherheitslücke bei der KiTa-App Stay Informed (vormals: KiTa-Info- und Schul-Info-App) aufgedeckt. Diese App findet auch in kirchlich-katholischen Kindertageseinrichtungen weite Verbreitung. Die betroffenen Einrichtungen sollen über den Vorfall in zwei Schreiben von der Stay Informed GmbH informiert worden sein, insbesondere auch über die möglicherweise notwendige Meldepflicht gegenüber der zuständigen Datenschutzaufsicht gemäß § 33 Kirchliches Datenschutzgesetz (KDG) und die gegebenenfalls erforderliche Benachrichtigung der betroffenen Personen gemäß § 34 KDG.

Aktuelle Hinweise hierzu stellt der App-Anbieter Stay Informed auf einer eigenen Internetseite bereit: *https://www.stayinformed.de/informationen-zur-datenpanne*

Um eine Fülle von Einzelmeldungen aus den KiTa-Einrichtungen zu vermeiden, wenden Sie sich bitte zunächst an die betrieblichen Datenschutzbeauftragten, mit denen die Aufsicht zum Teil diesbezüglich bereits in einem engen Austausch steht, oder an die übergeordnete Verwaltungseinheit (KiTa-Geschäftsträger, Verrechnungsstelle, Verwaltungszentrum u. a.).

Es laufen derzeit intensive Bemühungen, um zu einer Klärung der mit der Datenschutzverletzung verbundenen Fragen zu gelangen. Weitere Informationen zu der Datenpanne bei Stay Informed finden sich beispielsweise auf folgenden Webseiten:

- Datenleck bei beliebter KiTa-App Stay Informed (heise online vom 22.03.2024): *https://www.heise.de/news/Datenleck-bei-beliebter-KiTa-App-Stay-Informed-9662578.html*
- Sicherheitsversagen bei Stay Informed – Persönliche Daten aus beliebter Kita-App standen offen im Netz (SPIEGEL Netzwelt vom 22.03.2024): *https://www.spiegel.de/netzwelt/web/stay-informed-techmagazin-berichtet-von-sicherheitsluecke-bei-beliebter-kita-app-a-5074d96c-2db3-4b04-8eeb-4dca1f931aa7*
- Nach Datenleck bei Kita-App: Stay Informed richtet Informationsseite und FAQ ein (heise Security vom 26.03.2024): *https://www.heise.de/news/Nach-Datenleck-bei-Kita-App-Stay-Informed-richtet-Informationsseite-und-FAQ-ein-9667323.html*
- Sicherheitslücke bei der KiTa-App Stay Informed aufgedeckt (Der Beauftragte für den Datenschutz der EKD am 26.03.2024): *https://datenschutz.ekd.de/2024/03/26/sicherheitsluecke-bei-der-kita-app-stay-informed-aufgedeckt/*

7 Aus der Konferenz der Diözesandatenschutzbeauftragten

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Gemeinsame Stellungnahme
der Konferenz der Diözesandatenschutzbeauftragten
der Katholischen Kirche Deutschlands

zu den Unabhängigen Aufarbeitungskommissionen:

Anwendbarkeit des Kirchlichen Datenschutzrechts, datenschutzrechtliche Verantwortlichkeit und Gewährleistung der Datensicherheit

vom 12.11.2024

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

I. Anwendbarkeit des Kirchlichen Datenschutzrechts

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

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

II. Datenschutzrechtliche Verantwortlichkeit

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

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

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

[...]

▶ Gemeinsame Stellungnahme der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands zu den Unabhängigen Aufarbeitungskommissionen (6 Seiten)

8 Ausblick

Da nichts so beständig ist wie der Wandel, lässt auch der Ausblick in die nähere Zukunft der Datenschutzthemen einiges an Veränderungen erwarten: Die Novellierung des KDG, deren erster Entwurf im November 2024 veröffentlicht wurde, scheint in nicht allzu weite Ferne gerückt – vielleicht lässt sich im nächsten Tätigkeitsbericht bereits Konkretes dazu berichten.

Und auch die DSGVO soll möglicherweise eine Anpassung erfahren: Erleichterungen für KMU sind im Gespräch und Bürokratieabbau ist ein vielzitiertes Stichwort, doch noch gibt es keine Beschlüsse aus Brüssel.

AI-Act, CRA, NIS2-Richtlinie – alle diese im vorliegenden Bericht beschriebenen Verordnungen bzw. Gesetze des staatlichen Datenschutzes stehen entweder noch vor ihrer Umsetzung in nationales Recht oder die Regelungen sind zum Teil schon in Kraft und werden in bereits festgelegten Prozessen in den kommenden Jahren schrittweise umgesetzt. In jedem Fall werden sie den Datenschutz und alle an diesem Thema Beteiligten weiterhin begleiten.

Und für KDG und DSGVO gilt gleichermaßen, dass besonders die Vernetzung der Themenbereiche eine bedeutende Rolle spielen wird: KI, Datennutzung und Datenschutzrecht sind kaum mehr zu trennen und werden in zukünftigen Prozessen und Entwicklungen zunehmend jeweils immer „mitgedacht“ werden müssen.

Seien wir ehrlich: KI ist eines der allgegenwärtigsten Themen, wenn nicht DAS aktuelle Thema schlechthin – und wird es vermutlich auch im kommenden Jahr bleiben. Könnte es sein, dass dieser Ausblick KI-generiert ist? Urteilen Sie selbst …

9 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland

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

Unser Lieben Frauen Kirchhof 20
28195 Bremen
Diözesandatenschutzbeauftragter:
Andreas Bloms

Katholisches Datenschutzzentrum (KdöR)

Brackeler Hellweg 144
44309 Dortmund
Diözesandatenschutzbeauftragter:
Steffen Pau

Kath. Datenschutzzentrum Frankfurt/M. KdöR

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

Diözesandatenschutzbeauftragter der ostdeutschen Bistümer und des Katholischen Militärbischofs

Im Badepark 4
39218 Schönebeck
Diözesandatenschutzbeauftragter:
Matthias Ullrich

Datenschutzbeauftragter der Bayerischen (Erz-)Diözesen

Vordere Sterngasse 1
90402 Nürnberg
Diözesandatenschutzbeauftragter:
Dominikus Zettl

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

Kath. Datenschutzzentrum
Frankfurt/M.
Tätigkeitsbericht 2024