Jahresbericht 2023

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Berichtszeitraum
01.01.–31.12.2023

Katholisches Datenschutzzentrum

Herausgegeben vom

Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel.: 0231/13 89 85 – 0
Fax: 0231/13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Hinweis: Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt adäquate andere Formen gleichberechtigt ein.

Bildnachweis Titelmotiv: istockphoto.com | matejmo

8. Jahresbericht

des Diözesandatenschutzbeauftragten für die Erzdiözesen Köln und Paderborn sowie die Diözesen Aachen, Essen und Münster (nordrhein-westfälischer Teil) und des Verbandsdatenschutzbeauftragten des Verbandes der Diözesen Deutschlands (VDD)

für den Zeitraum 01.01.2023–31.12.2023

Redaktionsschluss: 31.10.2024

Inhaltsverzeichnis

Vorwort

Im Mai 2023 konnten wir schon auf fünf Jahre Anwendung der DSGVO und des KDG zurückblicken. Der Start der neuen Regelungen im Jahr 2018 war mit vielen Hoffnungen, aber auch Befürchtungen verbunden. Nicht alle Hoffnungen haben sich in den letzten Jahren der praktischen Anwendung der neuen Regelungen erfüllt, aber auch die mit den neuen Regelungen verbundenen Befürchtungen sind nicht alle eingetreten.

Die Hoffnungen und Befürchtungen spiegeln sich jetzt auch in den Erwartungen an den Evaluierungsprozess des KDG wieder. Der Prozess startete 2021 und dauert noch an. In der täglichen Anwendung des KDG haben sich verschiedene Punkte ergeben, bei denen die kirchlichen Regelungen im Rahmen der Vorgaben der DSGVO noch konkretisiert oder ergänzt werden sollten. Die auf Ebene des Verbandes der Diözesen Deutschlands eingerichtete Arbeitsgruppe zur Evaluierung des KDG wird sicherlich viele der aufgekommenen Punkte diskutieren und mögliche Lösungen aufzeigen.

Die kirchlichen Datenschutzaufsichten haben sich schon frühzeitig mit Anregungen in den Evaluierungsprozess eingebracht. Der Fokus unseres Hauses lag dabei auch auf der Umsetzung der Vorgaben des Art. 91 Abs. 2 DSGVO. Unsere Anregungen zielten hierbei beispielsweise auf eine klarere Formulierung der Aufgaben und Befugnisse der kirchlichen Datenschutzaufsichten. Damit sollten zukünftig Fragen und Missverständnisse zu den Aufgaben und Befugnissen der kirchlichen Aufsichten vermieden werden, die derzeit beim Vergleich der aktuellen Textfassungen von DSGVO und KDG zu diesen Punkten aufkommen könnten. Eine bessere Vergleichbarkeit beider Regelungen in diesem Punkt führt zu mehr Vertrauen in die unabhängige, gesetzeskonforme und interessengerechte Aufgabenwahrnehmung der kirchlichen Aufsichten. Denn ohne Vertrauen in die Wahrnehmung der Aufgabe können die Aufsichten ihre Arbeit nicht wirksam wahrnehmen. Schon der Anschein mangelnder Unabhängigkeit würde die kirchliche Datenschutzaufsicht um das Vertrauen bringen, das sie zur Vermittlung ihrer Entscheidungen benötigt. Nur dann kann der Versuch gelingen, die eigenen Entscheidungen sowohl den Menschen, deren personenbezogene Daten verarbeitet werden, als auch den kirchlichen Stellen und Einrichtungen nachvollziehbar zu erläutern und deren Notwendigkeit zu vermitteln.

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

1 Entwicklungen im Datenschutzrecht

Auf europäischer, nationaler und kirchlicher Ebene entwickeln sich die datenschutzrechtlichen Regelungen im Berichtszeitraum weiter. In diesem Abschnitt werden einige der im Jahr 2023 neuen oder geänderten gesetzlichen und regulatorischen Vorgaben zum Schutz personenbezogener Daten auszugsweise dargestellt. Außerdem wird auf einige wenige Entscheidungen der Gerichte hingewiesen.

1.1 Entwicklungen auf Ebene der Europäischen Union

Auch im Jahr 2023 gab es auf europäischer Ebene wichtige Entwicklungen für den Datenschutz. Neben neuen gesetzlichen Vorgaben sorgt auch die Rechtsprechung des Europäischen Gerichtshofs für die Klärung vieler Rechtsfragen. Einige aus Sicht des Katholischen Datenschutzzentrums datenschutzrechtlich relevante Vorhaben werden in diesem Abschnitt beschrieben.

1.1.1 Privacy by Design wird ISO-Standard

Nach mehreren Entwürfen ist im Februar 2023 die ISO 31700[1] veröffentlicht worden. Unter dem Titel „Consumer Protection – Privacy by design for consumer goods and services" (Verbraucherschutz – Privacy by Design für Konsumgüter und Dienstleistungen) teilt sich die ISO 31700 auf in Teil 1 (ISO 31700-1), der die eigentliche ISO-Norm enthält, und Teil 2 (ISO 31700-2), der drei beispielhafte Anwendungsfälle für den Einsatz der ISO-Norm erörtert.

Teil 1 der ISO-Norm enthält High-Level-Anforderungen an Privacy by Design, um die Privatsphäre während des gesamten Lebenszyklus eines Verbraucherproduktes zu schützen, einschließlich der Verarbeitung von Daten durch den Verbraucher.

Die folgenden drei Leitprinzipien sollen durch die Umsetzung der ISO-Norm dem Produkt und der Organisation zu Privacy by Design verhelfen.

Befähigung und Transparenz:
Die Organisation wird befähigt, durch Implementierung von Maßnahmen, die auf der Perspektive der Verbraucher basieren, sich für den Datenschutz in den eigenen Produkten einzusetzen. Der Verbraucher wird informiert, wie der Datenschutz angegangen und umgesetzt wird.

Institutionalisierung und Verantwortung:
Privacy by Design aus der ISO-Norm konzentriert sich auf die Rechenschaftspflicht und die Verantwortung der Organisation. Aber immer mit dem Fokus auf der Verantwortung dem Verbraucher gegenüber.

[1] ISO 31700-1:2023

Ökosystem und Lebenszyklus:
Die ISO-Norm kann auf das gesamte Informationsökosystem angewendet werden, die Technologie sowie die Organisation. Ebenso aber auch für Daten, die der Verbraucher mit dem Produkt verarbeitet. Dies gilt für den gesamten Lebenszyklus eines Produktes von der Konzeption bis zur Entsorgung.

Teil 2 der ISO-Norm enthält drei konkrete Anwendungsbeispiele. Dabei wird nicht nur der Datenschutz des Produktes oder der Dienstleistung selbst betrachtet, sondern auch der Schutz der Daten, die von dem Produkt verarbeitet werden. Alle Maßnahmen werden technologieneutral beschrieben, um eine möglichst breite Anwendung durch kleinere und größere Organisationen zu ermöglichen.

Hinweis für kirchliche Einrichtungen

Die ISO 31700 kann als standardisierte Anleitung dienen, um Privacy by Design über den kompletten Lebenszyklus eines Produktes oder einer Dienstleistung zu gewährleisten. Zum Thema Privacy by Design gibt es bereits den Standard DIN EN 17529:2022 – Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

1.1.2 EuGH entscheidet über die Frage, ob mündliche Übermittlungen in den Anwendungsbereich der DSGVO fallen

Das Berufungsgericht für Ost-Finnland hat dem EuGH im Rahmen eines Vorabentscheidungsverfahrens u. a. die Frage vorgelegt, ob eine mündliche Übermittlung personenbezogener Daten eine Verarbeitung gem. Art. 2 Abs. 1, Art. 4 Nr. 2 DSGVO darstellt (AZ C-740/22).

Grund für die Vorlage an den EuGH ist das Begehren einer Prozesspartei im Ausgangsverfahren. Sie begehrt mündlich Auskunft über möglicherweise anhängige oder abgeschlossene Strafverfahren gegen eine natürliche Person aus dem Personenregister eines Gerichts, das Informationen über Strafurteile oder Delikte natürlicher Personen enthält. Problematisch ist im vorliegenden Fall, ob der Verarbeitungsvorgang in Form der mündlichen Übermittlung den Anwendungsbereich der DSGVO eröffnet. Der sachliche Anwendungsbereich der DSGVO ist gem. Art. 2 Abs. 1 eröffnet, wenn es sich um eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten handelt sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Begriff der Verarbeitung wird in Art. 4 Abs. 2 DSGVO definiert. Diese Definition legt auch die Offenlegung durch Übermittlung personenbezogener Daten als Verarbeitung fest. In der Definition ist allerdings nicht enthalten, ob die Übermittlung mündlich oder schriftlich geschehen muss. Daher ist fraglich, ob eine mündliche Übermittlung als nicht-automatisierte Verarbeitung mit Speicherung in einem Dateiensystem zu werten ist.

Der Bundes- und auch der kirchliche Gesetzgeber haben sich im Bereich des Beschäftigtendatenschutzes für eine deutlichere Einordnung mündlicher Übermittlungen entschieden (§ 26 BDSG und § 53 KDG). Der Anwendungsbereich des § 53 KDG ist auch eröffnet, wenn personenbezogene Daten verarbeitet werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet oder für die Verarbeitung in einer solchen Datei erhoben werden. Damit fällt im Bereich des Beschäftigtendatenschutzes auch die Verarbeitung von personenbezogenen Daten während eines Gespräches oder Telefonats in den Anwendungsbereich der Norm.

Mittlerweile hat der EuGH am 07.03.2024 sein Urteil in dieser Sache verkündet. Der EuGH hat entschieden, dass Art. 2 Abs. 1 und Art. 4 Nr. 2 DSGVO „dahin auszulegen sind, dass eine mündliche Auskunft über möglicherweise verhängte oder bereits verbüßte Strafen in Bezug auf eine natürliche Person eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 der Verordnung darstellt, die in den sachlichen Anwendungsbereich dieser Verordnung fällt, wenn diese Informationen in einem Dateisystem gespeichert sind oder gespeichert werden sollen."

„Damit fällt im Bereich des Beschäftigtendatenschutzes auch die Verarbeitung von personenbezogenen Daten während eines Gespräches oder Telefonats in den Anwendungsbereich der Norm."

Hinweis für kirchliche Einrichtungen

Die Entscheidung des EuGH kann über Art. 91 DSGVO auch zur Auslegung des sachlichen Anwendungsbereichs des KDG (§ 2 Abs. 1, § 4 Nr. 2 KDG) herangezogen werden, da Art. 2 Abs. 1 DSGVO und § 2 Abs. 1 KDG wortlautgleich sind. Auch katholische Einrichtungen sollten daher ihre Vorgaben zu mündlichen Auskünften über personenbezogene Daten, die bereits elektronisch verarbeitet werden oder elektronisch verarbeitet werden sollen, überprüfen.

1.1.3 Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023 zum Data Privacy Framework

Mit dem Inkrafttreten des Beschlusses der EU-Kommission zur Vereinbarung der EU mit der US-Regierung zum EU-US Data Privacy Framework wird die Übermittlung personenbezogener Daten in die USA wieder erleichtert. Das EU-US Data Privacy Framework ist das Nachfolgeabkommen zu dem 2020 vom Europäischen Gerichtshof für nichtig erklärten Abkommen Privacy Shield[2].

Das kirchliche Datenschutzrecht eröffnet unter den Voraussetzungen des § 40 Abs. 1 KDG auch kirchlichen Stellen die Möglichkeit der Nutzung des neuen EU-US Data Privacy Framework.

Bei der Anwendung der neuen Regelung ist zu beachten, dass die Rahmenbedingungen eingehalten werden müssen, die das neue Abkommen setzt. Dies betrifft vor allem die Notwendigkeit, dass sich US-Unternehmen für die Anwendung des Data Privacy Frameworks bei der

[2] Zum Privacy-Shield-Abkommen siehe Abschnitte 2.1.1 und 3.2 des Jahresberichts 2020, Abschnitt 1.1.2 des Jahresberichts 2021 und Abschnitt 1.1.3 des Jahresberichts 2022.

zuständigen amerikanischen Stelle registriert haben müssen. Dies ist vom kirchlichen Verantwortlichen zu prüfen.[3]

Das Katholische Datenschutzzentrum weist in diesem Zusammenhang auf die grundsätzlich notwendigen Schritte zur Prüfung von Übermittlungen personenbezogener Daten in ein Land außerhalb des Geltungsbereiches der DSGVO durch die Verantwortlichen hin. Hier sind zum einen die üblichen Voraussetzungen der Verarbeitung personenbezogener Daten zu prüfen, die auch bei Übermittlungen ohne Drittlandsbezug zu prüfen wären (z. B. bei einem Vertrag zur Auftragsverarbeitung mit einem Auftragsverarbeiter aus Deutschland). Es müssen also vor allem eine Rechtsgrundlage für die Verarbeitung der Daten vorhanden und die Voraussetzungen des § 29 KDG für eine Auftragsverarbeitung erfüllt sein. Liegen diese Voraussetzungen vor, sind bei der Übermittlung in ein Drittland außerdem die Voraussetzungen der §§ 39 ff. KDG zu prüfen. In diesem zweiten Prüfungsschritt hilft das neue Abkommen (§ 40 Abs. 1 KDG) weiter, da es dem Verantwortlichen die Prüfung eines angemessenen Schutzniveaus für die Daten in dem Drittstaat (hier den USA) abnimmt und dies im Rahmen der Voraussetzungen des Data Privacy Framework feststellt.[4]

Außerdem hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 04.09.2023 Anwendungshinweise zum Angemessenheitsbeschluss zum EU-US Data Privacy Framework veröffentlicht.[5]

Die DSK will mit den umfangreichen Anwendungshinweisen Fragen beantworten, die an die Aufsichten nach dem Erlass des Angemessenheitsbeschlusses herangetragen wurden.

Hinweise für kirchliche Einrichtungen

Die Hinweise der DSK können auch für kirchliche Einrichtungen, unter Beachtung der Regelungen des KDG, hilfreich sein. Das Dokument enthält neben allgemeinen Informationen zum Angemessenheitsbeschluss und Hinweisen für Verantwortliche und Auftragsverarbeiter auch Angaben zu Rechtsschutz und Beschwerdemöglichkeiten.

1.2 Gesetzgeberische Entwicklungen in der Bundesrepublik Deutschland

Neben den Entwicklungen auf europäischer Ebene gab es im Berichtsjahr auch auf nationaler Ebene wieder mehrere, datenschutzrechtlich relevante Gesetzgebungsvorhaben, die hier nur auszugsweise dargestellt werden können.

[3] Der Text des Beschlusses der EU-Kommission kann hier abgerufen werden: https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

[4] Weitere Informationen zum neuen EU-US Data Privacy Framework stellt die EU-Kommission hier zur Verfügung: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[5] Die Anwendungshinweise können hier abgerufen werden: https://datenschutzkonferenz-online.de/media/pm/230904_DSK_PM_Anwendungshinweise_EU_US.pdf

1.2.1 Hinweisgeberschutzgesetz

Am 02.07.2023 trat das Hinweisgeberschutzgesetz (HinSchG) in Kraft. Bundestag und Bundesrat stimmten einem Kompromiss für einen Gesetzesentwurf im Vermittlungsausschuss zu, nachdem der Bundesrat die im Bundestag verabschiedete Version zunächst abgelehnt hatte.

Mit dem Hinweisgeberschutzgesetz hat der Gesetzgeber mit einiger Verspätung die Richtlinie 2019/1937 der EU umgesetzt.

Ziel des Gesetzes ist es u. a. einen gesetzlichen Rechtsschutz für Personen zu schaffen, die Missstände in Behörden oder Unternehmen aufdecken wollen. Dabei soll die Identität der hinweisgebenden Person geschützt und die Person gleichzeitig vor arbeitsrechtlichen Konsequenzen geschützt werden.

Beschäftigungsgebern ab 50 Mitarbeitenden obliegt die Einrichtung einer Meldestelle, an die sich hinweisgebende Personen wenden können. Die Unabhängigkeit dieser Stellen muss gewährleistet werden. Hinzu kommt, dass Behörden und Unternehmen bei der Errichtung der Meldewege auf die Einhaltung der datenschutzrechtlichen Vorschriften achten. Das beinhaltet insbesondere das Vorsehen von geeigneten technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten.

Private Beschäftigungsgeber ab einer Größe von 250 Mitarbeitenden und juristische Personen des öffentlichen Rechts mit mindestens 50 Mitarbeitenden müssen die Anforderungen aus dem Hinweisgeberschutzgesetz bereits umsetzen. Für kleinere private Beschäftigungsgeber zwischen 50 und 249 Mitarbeitenden galt eine Übergangfrist bis zum 17.12.2023.

„Beschäftigungsgebern ab 50 Mitarbeitenden obliegt die Einrichtung einer Meldestelle, an die sich hinweisgebende Personen wenden können."

Hinweis für kirchliche Einrichtungen

Das Hinweisgeberschutzgesetz gilt auch für alle kirchlichen Einrichtungen. Alle (Erz-)Diözesen im Zuständigkeitsbereich des Katholischen Datenschutzzentrums haben eine interne Meldestelle nach Hinweisgeberschutzgesetz eingerichtet.

1.2.2 Gesetzentwurf zur Änderung des BDSG

Im August 2023 legte das Bundesinnenministerium einen Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes vor. Mit dem Entwurf will die Bundesregierung Vorhaben aus dem Koalitionsvertrag und dem Bericht zur Evaluierung des BDSG aus dem Jahr 2021 umsetzen.

Der Entwurf sieht unter anderem vor, die Datenschutzkonferenz als Gremium der unabhängigen Datenschutzaufsichten des Bundes und der Länder zu stärken.

1.3 Gesetzgeberische Entwicklungen in der römisch-katholischen Kirche

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

1.3.1 Neue Grundordnung ist im Januar 2023 in Kraft getreten

Mit dem Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands (VDD) im November 2022 wurde die Grundordnung des kirchlichen Dienstes überarbeitet. Mit entsprechenden Veröffentlichungen in den Amtsblättern der fünf nordrhein-westfälischen (Erz-)Diözesen wurde die Neufassung der Grundordnung zum 01.01.2023 in der jeweiligen (Erz-)Diözese in Kraft gesetzt.

Aus datenschutzrechtlicher Sicht interessant ist, dass die neue Grundordnung – wie die Pressemitteilung[6] der Deutschen Bischofskonferenz betont – nicht mehr den bisherigen überwiegend personenbezogenen Ansatz verfolgt, bei dem der einzelne Mitarbeitende und dessen persönliche Lebensführung im Fokus stand. Was dies bedeutet, führt die Pressemitteilung weiter aus:

> *„Damit einher geht eine weitere wichtige Botschaft der neuen Grundordnung: Der Kernbereich privater Lebensgestaltung unterliegt keinen rechtlichen Bewertungen und entzieht sich dem Zugriff des Dienstgebers. Diese rechtlich unantastbare Zone erfasst insbesondere das Beziehungsleben und die Intimsphäre. Abgesehen von Ausnahmefällen bleibt der Austritt aus der katholischen Kirche wie in der bisherigen Fassung der Grundordnung ein Einstellungshindernis bzw. Kündigungsgrund. Auch eine kirchenfeindliche Betätigung steht einer Einstellung bzw. Weiterbeschäftigung entgegen.*
>
> *Die Religionszugehörigkeit ist nach neuem Recht nur dann ein Kriterium bei der Einstellung, wenn sie für die jeweilige Position erforderlich ist. Das gilt zum einen für pastorale und katechetische Dienste und zum anderen für diejenigen Tätigkeiten, die das katholische Profil der Einrichtung inhaltlich prägen, mitverantworten und nach außen repräsentieren. Von allen Mitarbeitenden wird im Rahmen ihrer Tätigkeit die Identifikation mit den Zielen und Werten der katholischen Einrichtung erwartet."*

Soweit der Kernbereich privater Lebensgestaltung nach der Neufassung der Grundordnung keiner Bewertung mehr unterliegen darf und dem Zugriff des Dienstgebers entzogen ist, besteht damit datenschutzrechtlich auch keine Rechtsgrundlage für eine (weitere) Verarbeitung davon betroffener personenbezogener Daten, soweit die Verarbeitung dieser Daten nicht nach anderen (z. B. steuerlichen) Vorschriften für den Dienstgeber noch notwendig ist.

[6] Deutsche Bischofskonferenz, Pressemitteilung Nr. 188 vom 22.11.2022, https://www.dbk.de/presse/aktuelles/meldung/neufassung-des-kirchlichen-arbeitsrechts.

Hinweise für kirchliche Einrichtungen

Die internen Arbeitsabläufe und Prozesse der Personalgewinnung und der Personalverwaltung sind von den kirchlichen Einrichtungen und Stellen daraufhin zu überprüfen, ob nur die nach der Neufassung der Grundordnung noch notwendigen personenbezogenen Daten verarbeitet werden. Die Arbeitsabläufe und Prozesse sind entsprechend neu aufzustellen.

1.3.2 Einsichtsnormen zur Missbrauchsaufarbeitung

Seit Veröffentlichung der ersten Missbrauchsstudie in der Erzdiözese München und Freising im Jahr 2010 folgten bereits mehrere (Erz-)Diözesen diesem Beispiel und haben (juristische) Gutachten zu der in der jeweiligen (Erz-)Diözese in einem bestimmten Zeitraum der Vergangenheit durch Kleriker und Laien begangenen sexualisierten Gewalt in Auftrag gegeben. Um eine unabhängige Aufarbeitung der Vorfälle zu ermöglichen, werden mit der Erstellung der Gutachten und Untersuchungen externe Rechtsanwaltskanzleien oder Wissenschaftler beauftragt. Auch die Unabhängigen Aufarbeitungskommissionen[7] in den (Erz-)Diözesen widmen sich der Aufklärung der Vorgänge.

In allen diesen Fällen stellt sich die datenschutzrechtliche Frage, auf welcher (datenschutz-)rechtlichen Grundlage diese Externen personenbezogene Daten der besonderen Kategorie gemäß § 11 KDG von der jeweiligen (Erz-)Diözese erhalten und damit verarbeiten dürfen. Insbesondere wird von Seiten der Betroffenen des Missbrauchs, deren Daten im Rahmen der Aufarbeitung auch angeschaut werden, vorgetragen, eine Nutzung der Daten der Betroffenen des Missbrauchs dürfe nur mit deren Einwilligung erfolgen.

Somit ist es aus unserer Sicht grundsätzlich zu begrüßen, dass neben den in den meisten (Erz-)Diözesen mittlerweile bestehenden Personalaktenordnungen für die Kleriker mit der „Musterordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- oder hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien in Bezug auf Sachakten, Verfahrensakten, Registraturakten und vergleichbare Aktenbestände der laufenden Schriftgutverwaltung“[8] (im Folgenden: Musterordnung) eine rechtliche Grundlage geschaffen wurde, die es auch aus datenschutzrechtlicher Sicht ermöglicht, diese Aufarbeitungsarbeit zu gewährleisten. Bei den Regelungen wird jedoch davon ausgegangen, dass jeder vom sexuellen Missbrauch Betroffene zur Förderung der Aufklärung bereit ist, seine persönliche Geschichte durch Weitergabe der entsprechenden Akten (z. B. Interventionsakte oder Akte wegen eines Antrags auf Anerkennung des Leids) an die Kommissionen, Rechtsanwälte oder Wissenschaftler ohne seine vorherige Einwilligung zu offenbaren.

[7] Diese Unabhängigen Aufarbeitungskommissionen bestanden teilweise bereits im Berichtsjahr in einigen (Erz-)Diözesen auf Basis der Vereinbarung zwischen der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) und der Deutschen Bischofskonferenz aus dem Jahr 2020.

[8] Musterordnung auf Ebene des Verbandes der Diözesen Deutschlands. Vgl. beispielsweise die Umsetzung für das Bistum Aachen (Amtsblatt Nr. 11/2023 aus Oktober 2023, https://kirchenrecht-bac.de/document/3470#s00000271).

In § 4 der Musterordnung wird festgelegt, unter welchen Bedingungen die Verarbeitung der personenbezogenen Daten der besonderen Kategorie im Rahmen der Aufarbeitungsarbeit durch die unabhängigen Aufarbeitungskommissionen ohne Einwilligung der betroffenen Person rechtlich möglich sein soll. Dabei wird u. a. als Voraussetzung genannt, dass die Aufarbeitung mit anonymisierten Daten nicht möglich oder der Aufwand der Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden wäre.

Die Musterordnung regelt insgesamt die wichtige Frage, inwiefern Akten, in denen das erlittene Leid der Betroffenen von sexuellem Missbrauch wiedergegeben wird, im Rahmen der Aufarbeitung an Kommissionen, zu Forschungszwecken oder an Rechtsanwaltskanzleien weitergegeben werden dürfen.

Aus datenschutzrechtlicher Sicht erscheinen die gefundenen Vorgaben der Musterordnung aber vor dem Hintergrund der zu beachtenden Vorgaben des KDG nicht unproblematisch, soweit die Musterordnung eine Offenlegung der Daten der Betroffenen des Missbrauchs ohne deren Einwilligung und ohne eine Anonymisierung dieser Daten ermöglicht.[9]

1.4 Aus der Arbeit des Europäischen Datenschutzausschusses und der nationalen Datenschutzaufsichten

Der Europäische Datenschutzausschuss (EDSA; engl. European Data Protection Board – EDPB) trägt als Gremium, in dem sich die Datenschutzaufsichtsbehörden der Mitgliedsländer der EU beraten und u. a. gemeinsame Positionen und Vorgehensweisen beschließen, zur einheitlichen Anwendung der DSGVO bei.

Auf nationaler Ebene beraten sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder in der Datenschutzkonferenz. Hier wird ebenfalls das Ziel verfolgt, eine einheitliche Anwendung des europäischen und auch des nationalen Datenschutzrechts zu erreichen.

Für kirchliche Stellen sind die Themen, mit denen sich der Europäische Datenschutzausschuss und die nationalen Datenschutzaufsichtsbehörden befassen, interessant, da das kirchliche Datenschutzrecht im Einklang mit der DSGVO erlassen wurde. Daher sind die Veröffentlichungen des EDSA beziehungsweise der DSK fast vollständig auf die Rechtslage nach dem KDG übertragbar. Die kirchlichen Datenschutzaufsichten berücksichtigen die Vorgaben des EDSA und der nationalen Datenschutzaufsichtsbehörden und stimmen sich teilweise mit diesen ab[10]. Auf den offiziellen Internetseiten können die Arbeit des EDSA[11] und der DSK[12] verfolgt werden.

[9] Dem KDSZ liegt zu dieser Thematik bereits eine Beschwerde vor, siehe hierzu Abschnitt 2.3.3 dieses Berichts.
[10] Siehe hierzu Abschnitt 3.6 dieses Jahresberichts.
[11] https://edpb.europa.eu/edpb_de
[12] https://www.datenschutzkonferenz-online.de

Der Europäische Datenschutzausschuss und die nationalen Datenschutzaufsichtsbehörden haben sich im Berichtszeitraum mit einer Vielzahl von Themen beschäftigt und z. B. Leitlinien, Stellungnahmen und Entschließungen verabschiedet. Nachfolgend werden einige Punkte aufgegriffen.

1.4.1 EDSA – datenschutzrechtliche Verantwortung für Facebook-Gruppe

Die nationale Aufsichtsbehörde in Estland (Andmekaitse Inspektsioon) hat in einem Prüfverfahren die datenschutzrechtliche Verantwortlichkeit eines Administrators einer Facebook-Gruppe angenommen und gegen diesen ein Bußgeld verhangen.

Die Aufsichtsbehörde wurde aufgrund mehrerer Beschwerden bezüglich der Facebook-Gruppe tätig. In der Facebook-Gruppe wurden Schuldnerdaten von privaten Personen durch Mitglieder der Gruppe veröffentlicht. Eine Rechtsgrundlage aus europäischem oder nationalem Recht gab es laut Entscheidung der estnischen Behörde für die Verarbeitungen in Form der Offenlegungen nicht. Die Behörde versuchte den Administrator der Gruppe zur Schließung dieser zu bewegen, bevor sie das Bußgeld verhing. Die estnische Behörde ging von der Verantwortlichkeit des Gruppenadministrators aus, da dieser, jedenfalls nach eigener Angabe, die Datenverarbeitung einstellen oder Änderungen an den Daten vornehmen könne.[13] Die Entscheidung ist noch nicht rechtskräftig.

1.4.2 EDSA – Bericht der Cookie-Banner-Taskforce

Am 17.01.2023 verabschiedete die Cookie-Banner-Taskforce des Europäischen Datenschutzausschusses ihren Arbeitsbericht[14].

Um die Bearbeitung der Beschwerden zu Cookie-Bannern der Organisation „NYOB“ zu beschleunigen, wurde die Taskforce mit der Untersuchung beauftragt, um den zuständigen Behörden, die mit der Beschwerdebearbeitung befasst sind, eine Hilfestellung zu geben.

Die Taskforce konnte sich in dem Arbeitsbericht auf die folgenden Punkte einigen, die nach ihrer Einschätzung auf die Unzulässigkeit einer Einwilligung bei einem Cookie-Banner hinweisen:

- Ein fehlender Button zum Ablehnen der Cookies auf der gleichen Ebene wie der Button zum Akzeptieren der Cookies

- Vorausgewählte Checkboxen

[13] Die Entscheidung der estnischen Aufsichtsbehörde kann hier abgerufen werden: https://www.aki.ee/sites/default/files/ettekirjutus-hoiatus_isikuandmete_kaitse_asjas_03.01.2022_nr_2.1.-4_21_153_eraisik.pdf ; auch der EDSA hat über die Entscheidung berichtet: https://www.edpb.europa.eu/news/national-news/2023/estonian-sa-private-person-legal-bases-disclosure-data-unidentified-persons_en

[14] Der Bericht wird vom EDSA bislang nur in der englischen Sprachversion veröffentlicht: https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en.

- Kein Button zum Ablehnen von Cookies, nur ein Link im Text des Cookie-Banners als Möglichkeit zum Ablehnen der Cookies
- Ein Link zum Ablehnen von Cookies außerhalb des Cookie-Banners
- Die fehlende Möglichkeit des Widerrufs der Einwilligung

Weiterhin stimmten die Mitglieder der Taskforce überein, dass dem Verantwortlichen nicht auferlegt werden kann, sich an einen allgemeinen Standard in Bezug auf Farbe/Kontrast des Cookie-Banners oder der Schaltflächen zu halten. Als irreführend bezeichnet die Taskforce aber z. B. eine Schaltfläche, bei der der Kontrast zwischen Hintergrund und Text so gering ist, dass der Text für den Nutzer praktisch unlesbar ist. Die Taskforce geht bei der Prüfung von Cookie-Bannern immer von einer Einzelfallprüfung aus. Die Analyse der Cookie-Banner soll zeigen, dass die Erteilung einer Einwilligung rechtlich in Ordnung und genauso einfach zu widerrufen ist.

Der damalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Professor Kelber begrüßte in einer Stellungnahme[15] im Januar 2023 die Arbeit der Taskforce und ergänzte, dass eine gut gemachte und faire Internetseite kein Cookie-Banner benötige, weil sie nur technisch notwendige Cookies verwende. Wenn Internetseitenbetreibende aber unbedingt personenbezogene Daten sammeln wollten, dann dürften sie sich eine Einwilligung dafür nicht mit unfairen oder rechtswidrigen Mitteln holen. Weiter betont der BfDI, dass die Ergebnisse des Abschlussberichts der Cookie-Banner-Taskforce nun zum größten Teil dem entsprechen würden, was die DSK in Deutschland schon in der Orientierungshilfe Telemedien[16] festgehalten habe.

Hinweis für kirchliche Einrichtungen

Das Katholische Datenschutzzentrum schließt sich den Erkenntnissen der Taskforce und der Orientierungshilfe Telemedien an und wird dies bei anstehenden Prüfungen von Internetseiten/Cookie-Bannern mit einfließen lassen. Cookie-Banner müssen der fairen und transparenten Datenverarbeitung dienen. Eine Einzelfallbetrachtung von Cookie-Bannern bei Internetseitenprüfungen ist erforderlich, um die Voraussetzungen an eine rechtswirksame Einwilligung sicherzustellen.

1.4.3 Neues MS Outlook

Microsoft hat mit dem Windows 11-Update auf die Version 23H2 die neue Outlook-App eingeführt. Diese erscheint im Startmenü von Windows 11 als neue App. Im klassischen Outlook wird der Anwender über einen Schalter zum Testen des neuen Outlooks eingeladen. Das

[15] https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2023/02_EDSA-Cookie-Banner-Cloud-Dienste.html
[16] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Orientierungshilfen/OrientierungshilfeAnbieter-innenTelemedien.pdf?__blob=publicationFile&v=6

neue Outlook soll einem Artikel der Microsoft Tech Community[17] zufolge die E-Mail- und Kalender-App in Windows ersetzen. Das neue Outlook ersetzt nicht das Outlook von Microsoft Office.

Mit dem neuen Outlook können nicht nur Microsoft E-Mail-Konten eingebunden werden, sondern auch Yahoo, Google und per IMAP abrufbare Postfächer. Bei der Konfiguration eines Postfachs, das nicht von Microsoft gehostet wird, erscheint ein Hinweis, dass die E-Mails mit der Microsoft-Cloud synchronisiert werden. Es wird auf einen Microsoft Support-Artikel[18] verwiesen, in dem der Leser darauf hingewiesen wird, dass Microsoft dem Anwender die Microsoft-365-Erfahrung auch für Nicht-Microsoft-Postfächer zur Verfügung stellen möchte. E-Mail, Kalender und Kontakte werden zwischen dem E-Mail-Anbieter und dem Microsoft-Rechenzentrum synchronisiert, um die Microsoft-365-Erfahrung mit allen Anwendern teilen zu können.

Diese Synchronisierung funktioniert, weil Benutzername und Passwort durch das neue Outlook an Microsoft übermittelt werden. Durch dieses Vorgehen hat Microsoft den vollen Zugriff auf alle Inhalte der so konfigurierten Postfächer. Microsoft ruft mit den Zugangsdaten die Inhalte beim E-Mail-Anbieter ab und synchronisiert diese in die eigenen Rechenzentren. Dieses Vorgehen wurde von der Zeitschrift c`t des Heise-Verlages[19] veröffentlicht. Bei der Anlage eines neuen IMAP-Kontos im neuen Outlook werden Ziel-Server, Benutzername und Passwort an die Microsoft-Server übertragen. Die Daten werden zwar über eine TLS-verschlüsselte Verbindung[20] übertragen, doch innerhalb der gesicherten Verbindung im Klartext übermittelt.

Microsoft hat sich gegenüber dem Heise-Verlag zu deren Anfrage geäußert und erklärt warum aus Sicht von Microsoft die Übertragung der Zugangsdaten an Microsoft durchgeführt wird.[21]

Wozu Microsoft die Daten nutzt, wird nicht klar dargestellt. Gefällt einem Anwender das neue Outlook nicht, ist laut Microsoft ein Wechsel zurück möglich. Das Passwort und die bereits abgerufenen Informationen sind Microsoft dann allerdings bekannt. Was nach dem Löschen der Konten im neuen Outlook mit den Daten bei Microsoft passiert ist ebenfalls unklar.

In einem Rundschreiben an alle Bundesministerien und obersten Bundesbehörden[22] vom 08.12.2023 schreibt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, dass ein datenschutzkonformer Einsatz der App aktuell nicht möglich sei. Die Nutzer würden zwar vor der Installation darauf hingewiesen, dass E-Mails mit der Microsoft-Cloud synchronisiert würden. Allerdings sei weder aus dem Hinweis, noch aus den weiteren Informationen erkenntlich, dass

[17] https://techcommunity.microsoft.com/t5/outlook-blog/things-to-look-forward-to-in-the-new-outlook-for-windows/ba-p/3975602
[18] https://support.microsoft.com/de-de/office/synchronisieren-ihres-kontos-in-outlook-mit-der-microsoft-cloud-985f9e19-d308-4e85-9d1d-0c6f32f8e981?ui=de-de&rs=de-de&ad=de
[19] https://www.heise.de/news/Microsoft-krallt-sich-Zugangsdaten-Achtung-vorm-neuen-Outlook-9357691.html
[20] Bei Transport Layer Security (TLS, deutsch: Transportschichtsicherheit) handelt es sich um ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
[21] https://www.heise.de/news/Neues-Outlook-Microsoft-bezieht-Stellung-zur-Uebertragung-von-Zugangsdaten-9528869.html
[22] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2023/Das-neue-Outlook-in-der-Cloud.pdf?__blob=publicationFile&v=2

Zugangsdaten in der Cloud gespeichert würden. Laut BfDI handele es sich hierbei nicht um eine wirksame Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO.

Hinweis für kirchliche Einrichtungen

Das KDG stellt mit § 6 Abs. 1 lit. b) KDG und § 8 KDG vergleichbare Anforderungen an eine Einwilligung wie die DSGVO. Deshalb kann im Sinne der Auslegung des BfDI auch im Geltungsbereich des KDG nicht ohne weiteres von einer wirksamen Einwilligung in den Betrieb des neuen Outlooks ausgegangen werden.

1.4.4 Elektronische Patientenakte

Seit 2021 können alle gesetzlich Versicherten auf Wunsch von ihrer Krankenkasse eine elektronische Patientenakte (ePA) zur Verfügung gestellt bekommen. Im Dezember 2023 hat der Bundestag mit dem Digital-Gesetz in 2./3. Lesung beschlossen, dass ab Januar 2025 für alle Versicherten die ePA bereitgestellt wird. Die Nutzung bleibt jedoch weiterhin freiwillig. Wer ab 2025 die ePA nicht nutzen möchte, hat nach der Information zur Einrichtung der ePA durch die jeweilige Krankenkasse die Möglichkeit, per Opt-Out der Anlage einer ePA ganz oder in Teilen zu widersprechen.

Die ePA wird als patientengeführte Akte bereitgestellt. Der Patient kann bestimmen, ob und in welchem Umfang die ePA genutzt wird und welche Daten in der Akte gespeichert und gelöscht werden. Weiterhin kann der Patient entscheiden, welchem Behandler Daten zur Verfügung gestellt werden. Der Patient kann selbständig z. B. eigene medizinische Daten, Gesundheitstagebücher, Notfallkontaktdaten oder auch einen Organspendeausweis in der ePA ablegen. Da die ePA als lebenslange Akte konzipiert ist, gibt es keine Speicherplatzbegrenzung. Der Patient hat die Möglichkeit, einzelne Daten oder die vollständige ePA zu löschen.

Konzipiert ist die ePA, um über eine Smartphone- oder Tablet-App den Zugriff auf die Daten zu bekommen. Wer kein Smartphone oder Tablet zur Verfügung hat oder dieses nicht nutzen kann, kann mit einem eingeschränkten Funktionsumfang auch über einen Desktop-PC oder Laptop auf die ePA zugreifen.

Die Daten werden verschlüsselt bei den jeweiligen Betreibern der ePA-Aktensysteme in der Telematikinfrastruktur gespeichert. Die Server der Telematikinfrastruktur werden bundesweit gehostet, unterliegen der DSGVO und werden durch das Zulassungsverfahren der gematik[23] auf sicherheitstechnische Eignung durch unabhängige Gutachter geprüft. Der Speicherort der Daten der ePA unterscheidet sich je nach Anwendung in der Telematikinfrastruktur. Zum Beispiel werden die Daten des E-Rezepts auf Servern in der Telematikinfrastruktur gespeichert, die von einem durch die gematik ausgewählten Anbieter betrieben werden. Die Telematikinfrastruktur ist nicht der Datenspei-

[23] https://www.gematik.de/ueber-uns/struktur

cher, sondern als „Daten-Autobahn“ zu sehen, die die verschiedenen Anwendungen miteinander verbindet.[24] Die gematik[25] ist der Betreiber der Telematikinfrastruktur. Dieses geschlossene Netzwerk bildet die Plattform für digitale Anwendungen im deutschen Gesundheitssystem.

Verantwortlich für die Datenverarbeitung ist der Anbieter, i. d. R. die jeweilige Krankenkasse. Weder der Anbieter, noch der Betreiber können die Inhalte der ePA einsehen. Für alle Fragen zum Datenschutz der ePA ist gewöhnlich der Datenschutzbeauftragte der jeweiligen Krankenkasse die richtige Anlaufstelle.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit[26] sieht es unter anderem kritisch, dass Menschen, die kein eigenes geeignetes Endgerät besitzen oder benutzen wollen, in ihrer Patientensouveränität eingeschränkt sind. Auch kann die Nutzung mancher Dienste der ePA ab 2025 nicht auf einzelne Behandler beschränkt werden.

„Verantwortlich für die Datenverarbeitung ist der Anbieter, i. d. R. die jeweilige Krankenkasse. Weder der Anbieter, noch der Betreiber können die Inhalte der ePA einsehen.“

1.4.5 Beschluss der DSK: Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 03.02.2023 einen Beschluss zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die nach Art. 28 DSGVO im Wege einer Auftragsverarbeitung im europäischen Wirtschaftsraum (EWR) verarbeitet werden, veröffentlicht. Der Beschluss ist auf der Internetseite der DSK abrufbar.[27]

Der Beschluss setzt sich mit Sachverhaltskonstellationen auseinander, in denen Auftragsverarbeitungen personenbezogener Daten von im EWR ansässigen Tochtergesellschaften durchgeführt werden, deren Muttergesellschaft den Hauptsitz in einem Drittstaat hat. Der Beschluss kann von Verantwortlichen zur Beurteilung von allen Auftragsvereinbarungen über Datenverarbeitungen im EWR herangezogen werden. Dies gilt insbesondere für Sachverhalte, in denen eine Drittlandsübermittlung in die USA aufgrund des CLOUD-Acts möglich erscheint.

Die DSK kommt zunächst zu dem Ergebnis, dass alleine die Gefahr einer Anweisung durch eine Drittlands-Muttergesellschaft an ihre EWR-Tochtergesellschaft, personenbezogene Daten in ein Drittland zu übermitteln, nicht genügt, um eine Übermittlung in ein Drittland i. S. d. Artt. 44 ff. DSGVO anzunehmen. Gleiches gilt für Konstellationen, in denen öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten zu übertragen. Die

[24] https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/gesundheitsdatennutzungsgesetz/faq-gesundheitsdatennutzungsgesetz.html

[25] Gesellschafter der gematik sind das Bundesministerium für Gesundheit (BMG), die Bundesärztekammer (BÄK), die Bundeszahnärztekammer (BZÄK), der Deutsche Apothekerverband (DAV), die Deutsche Krankenhausgesellschaft (DKG), der Spitzenverband der Gesetzlichen Krankenversicherungen (GKV-SV), die Kassenärztliche Bundesvereinigung (KBV), die Kassenzahnärztliche Bundesvereinigung (KZBV) und der Verband der Privaten Krankenversicherung (PKV).

[26] https://www.bfdi.bund.de/DE/Buerger/Inhalte/GesundheitSoziales/eHealth/elektronische Patientenakte.html?nn=252102

[27] https://datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf

DSK führt aber weiter aus, dass eine solche Gefahr dazu führen kann, dass Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, soweit nicht diese – oder auch der Verantwortliche – technische und/oder organisatorische Maßnahmen ergriffen haben, die hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt. Insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen anbelangt, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht. Dabei kann sich ein Verantwortlicher nicht auf bloße, gegebenenfalls vertragliche, Zusicherungen des Auftragsverarbeiters verlassen. Der Verantwortliche muss im Einzelfall prüfen, ob die Zusicherungen eingehalten werden. Eine Aufzählung der insbesondere durch den Verantwortlichen zu prüfenden Punkte kann dem Bescheid der DSK entnommen werden.

> **„Dabei kann sich ein Verantwortlicher nicht auf bloße … Zusicherungen des Auftragsverarbeiters verlassen. [Er] muss im Einzelfall prüfen, ob die Zusicherungen eingehalten werden."**

Hinweis für kirchliche Stellen

Die im Beschluss angeführten Überlegungen lassen sich auch auf das KDG übertragen. Katholische Einrichtungen sollten daher überprüfen, ob Auftragsverarbeiter die erforderliche Zuverlässigkeit aus § 29 Abs. 1 KDG gewährleisten können.

1.5 Schwerpunkt Auskunftsrecht (§ 17 KDG)

Das Auskunftsrecht aus § 17 KDG nimmt in der Beratung und bei den Beschwerdeverfahren im Katholischen Datenschutzzentrum einen großen Raum ein. Auch in der Rechtsprechung gibt es immer mehr Entscheidungen zum Auskunftsrecht.

1.5.1 EuGH entscheidet über Umfang des Auskunftsanspruchs

In seiner Entscheidung vom 12.01.2023 (Rs. C-154/21) hat sich der Europäische Gerichtshof dazu geäußert, inwieweit Unternehmen die Identität von Empfängern personenbezogener Daten offenlegen müssen, wenn das Auskunftsrecht nach Art. 15 Abs. 1 lit. c) DSGVO ausgeübt wird.[28]

Ein Betroffener verlangte von der Österreichischen Post Auskunft darüber, wie seine personenbezogenen Daten verarbeitet wurden, insbesondere über die Identität der Empfänger dieser Daten. Die Österreichische Post gab an, dass sie personenbezogene Daten im Rahmen ihrer Tätigkeit als Herausgeberin von Telefonbüchern verwendet und diese Daten Handelspartnern zu Marketingzwecken anbietet. In ihrer Antwort auf die Anfrage nannte die Österreichische Post die Namen dieser Handelspartner nicht.

[28] Die Entscheidung des EuGH kann hier abgerufen werden: https://curia.europa.eu/juris/liste.jsf?language=de&num=C-154/21

Der Betroffene erhob daraufhin Klage und berief sich auf Art. 15 Abs. 1 lit. c) DSGVO. Seiner Ansicht nach gab ihm die Norm ein Recht auf Auskunft über die konkreten Empfänger. Sowohl das Gericht der ersten Instanz als auch das Berufungsgericht wiesen die Klage ab. Der Betroffene legte daraufhin Rechtsmittel ein.

Der Oberste Gerichtshof Österreichs legte in dem Revisionsverfahren dem EuGH die Frage vor, ob das Auskunftsrecht nach Art. 15 Abs. 1 lit. c) DSGVO einen Anspruch auf Nennung der konkreten Empfänger beinhaltet.

Der EuGH entschied, dass Verantwortliche gemäß Art. 15 Abs. 1 lit. c) DSGVO generell verpflichtet sind, die Identität der Empfänger anzugeben. Dies gilt sowohl für Empfänger, denen das Unternehmen die betreffenden personenbezogenen Daten bereits offengelegt hat, als auch für künftige Empfänger der Daten.

Der EuGH sah nur in engen Ausnahmefällen die Möglichkeit, dass der Verantwortliche von der Nennung der konkreten Empfänger absehen und stattdessen nur die Empfängerkategorien angeben kann. Entweder, wenn es dem Verantwortlichen unmöglich ist, die Empfänger zu identifizieren, oder, wenn es sich um offenkundig unbegründete oder exzessive Auskunftsanträge im Sinne von Art. 12 Abs. 5 DSGVO handelt. Der EuGH führte weiter aus, dass der Verantwortliche für diese Umstände beweispflichtig ist.[29]

„Der EuGH sah nur in engen Ausnahmefällen die Möglichkeit, dass der Verantwortliche von der Nennung der konkreten Empfänger absehen … kann."

Der EuGH begründete seine Entscheidung u. a. damit, dass eine andere Auslegung von Art. 15 Abs. 1 lit. c) DSGVO dem Ziel und Zweck des Auskunftsrechts nicht gerecht werden würde. Das Recht auf Auskunft bilde die Grundlage für weitere Betroffenenrechte, darunter das Recht auf Berichtigung und Löschung sowie das Recht auf Widerspruch gegen die Verarbeitung. Nach Ansicht des EuGH stützen die Erwägungsgründe, der Grundsatz der Transparenz und Art. 19 DSGVO diese Auslegung, die den betroffenen Personen hilft, ihr Recht auf Datenschutz zu verwirklichen.[30]

Hinweis für kirchliche Einrichtungen

Auch die kirchlichen Verantwortlichen müssen auf der Grundlage der mit Art. 15 Abs. 1 lit. c) DSGVO deckungsgleichen Regelung des § 17 Abs. 1 lit. c) KDG bei Auskünften unter den vom EuGH genannten Voraussetzungen die Empfänger der Daten konkret benennen. Verantwortliche sollten in Zukunft daher genau prüfen und dokumentieren, wenn und warum sie einem Antragsteller die genauen Empfänger von personenbezogenen Daten nicht nennen.

[29] Siehe Randnummern 48 und 49 der Entscheidung.
[30] Siehe Randnummern 37 ff. der Entscheidung.

1.5.2 EDSA Leitlinien 1/2022 zu den Rechten der betroffenen Person – Auskunftsrecht – Version 2.0

Die „Leitlinien 1/2022 zu den Rechten der betroffenen Person – Auskunftsrecht Version 2.0“[31] des Europäischen Datenschutzausschusses wurden am 28.03.2023 nach öffentlicher Konsultation angenommen, nachdem im Jahr 2022 bereits eine erste Version[32] als Grundlage für das Konsultationsverfahren vorgestellt worden war.

Das Auskunftsrecht ist von Beginn an Teil des europäischen Datenschutzrechtsrahmens und wird in Art. 15 DSGVO (entspricht § 17 KDG) präzisiert.

Die Leitlinien befassen sich mit dem Ziel und der Struktur des Auskunftsrechts, dem Umgang mit Anträgen betroffener Personen sowie dem Umfang und den Grenzen und Einschränkungen des Auskunftsrechts.

Ziel der Leitlinien ist es, durch die ausführlichen Vorgaben und Hilfestellungen eine europaweit einheitliche Handhabung des Art. 15 DSGVO zu erreichen.

Hinweis für kirchliche Stellen

Aufgrund der parallelen Regelung des § 17 KDG ist diese Leitlinie auch für die kirchlichen Einrichtungen hilfreich und beachtenswert.

[31] https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

[32] Siehe Abschnitt 1.5.1 des Jahresberichts 2022. Hier wird der Inhalt der Leitlinien detailliert beschrieben.

2 Aus der Tätigkeit des Datenschutzzentrums

Auch im Berichtsjahr 2023 überstiegen die dem Katholischen Datenschutzzentrum gemeldeten Datenschutzverletzungen zahlenmäßig wieder die eingegangenen Anfragen, Beschwerden und Hinweise. Einige wenige (neue oder immer wieder aktuelle) Themen und Fragestellungen werden in diesem Abschnitt dargestellt.

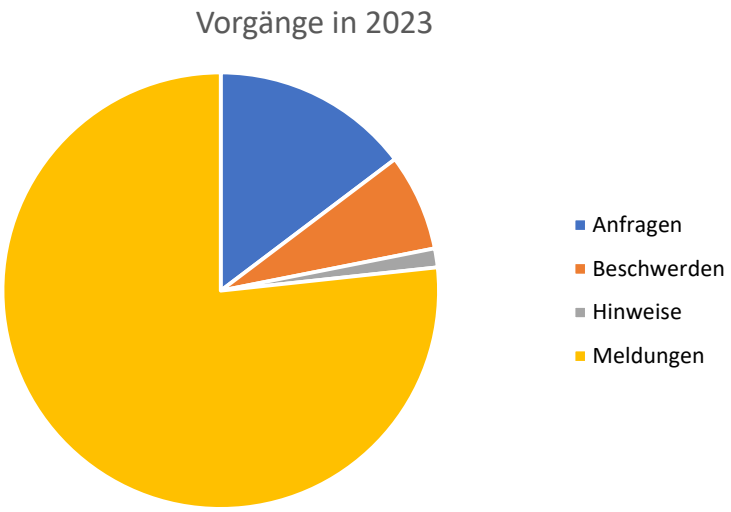


Abb. 1: Vorgänge beim Katholischen Datenschutzzentrum im Jahr 2023.

2.1 Beratungen und Anfragen

Für das Katholische Datenschutzzentrum ist die Bearbeitung von Anfragen und generell die vom KDG mehrfach hervorgehobene Beratungstätigkeit durch die kirchlichen Aufsichten ein wichtiger Bestandteil seiner täglichen Arbeit. Die Themenfelder und Fragestellungen, die von den kirchlichen Stellen an das Katholische Datenschutzzentrum herangetragen werden, sind dabei breit gefächert und können in diesem Abschnitt nur auszugsweise dargestellt werden.

Hinweis für kirchliche Stellen

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

2.1.1 Die Firm-App des Bonifatiuswerks

Im Berichtzeitraum hat das Katholische Datenschutzzentrum eine Prüfung der Firm-App des Bonifatiuswerks durchgeführt.

Auf die Anfrage aus einer kirchlichen Einrichtung hin wurde mit dem Bonifatiuswerk die technische und datenschutzrechtliche Ausgestaltung der Firm-App besprochen. Insbesondere wurden die vertragliche Ausgestaltung hinsichtlich des Verantwortlichkeitsmodells und die Rechtsgrundlagen für die verschiedenen Verarbeitungsvorgänge durch das Katholische Datenschutzzentrum überprüft. Das Bonifatiuswerk hat sich im Verlauf der Prüfung dazu entschlossen, die vertragliche Ausgestaltung zur Nutzung der App zu ändern. Das Vertragswerk der Firm-App wurde dergestalt geändert, dass nunmehr eine gemeinsame Verantwortlichkeit mit den Kirchengemeinden gemäß § 28 KDG vorgesehen ist. Die Datenschutzerklärung und die Nutzungsbedingungen der App wurden ebenfalls überarbeitet.

Durch die vom Bonifatiuswerk vorgenommenen Änderungen bezüglich der Verantwortlichkeit für die Verarbeitung der Daten und soweit sich das Katholische Datenschutzzentrum die technische Gestaltung der App angeschaut hat und entsprechende Anmerkungen durch Bonifatius umgesetzt wurden, konnten die Bedenken des Katholischen Datenschutzzentrums zum Betrieb der Firm-App aus datenschutzrechtlicher Sicht ausgeräumt werden.

2.1.2 Namensschilder der Beschäftigten

Ein kirchliches Krankenhaus bat das Katholische Datenschutzzentrum um Beratung, ob es berechtigt sei, den Vor- und Zunamen der Mitarbeitenden auf dem Namensschild auszuweisen.

Das Tragen eines Namensschildes sei aus Sicht des Krankenhauses erforderlich, um die persönliche und namentliche Ansprechbarkeit zu gewährleisten. Auch für das Beschwerdemanagement sei das Tragen und die Möglichkeit, die Mitarbeitenden zu identifizieren, erforderlich.

Vor- und Zuname sind personenbezogene Daten im Sinne des § 4 Nr. 1 KDG und entsprechend zu schützen. Damit bedarf es für die Verarbeitung dieser Daten durch das Krankenhaus wie stets im Datenschutzrecht einer Rechtsgrundlage.

Als Rechtsgrundlage für das Tragen eines Namensschildes für die genannten Zwecke der Ansprechbarkeit des Personals beziehungsweise der Identifizierung für das Beschwerdemanagement sind § 6 Abs. 1 lit. g) KDG oder § 53 Abs. 1 KDG denkbar. Beide Normen erfordern aber eine Interessenabwägung inklusive einer Erforderlichkeitsprüfung.

In der Interessenabwägung sind die Interessen des Krankenhauses an einer Ansprechbarkeit und Identifizierbarkeit des Personals abzuwägen mit dem Interesse des Personals, beispielsweise nicht privat von Patienten und Patientinnen kontaktiert oder sogar gestalkt zu werden.

Da die vom Krankenhaus genannten Ziele auch mit der Nennung nur des Vor- oder Nachnamens auf dem Namensschild erreicht werden können und andererseits durch die heutigen Informationsmöglichkeiten im Internet Personen sehr viel einfacher gefunden werden können als früher, wird diese Interessenabwägung im Regelfall zugunsten der Beschäftigten ausfallen.

Sofern also keine überwiegenden Gründe für einen vollständigen Aufdruck des Vor- und Zunamens bestehen, darf der Dienstgeber grundsätzlich nur verlangen, dass ein Namensteil auf den Namensschildern angebracht wird. Dies erscheint auch zur Identifikation ausreichend (Aufdruck von Vor- oder Zuname, bei großen Betrieben vielleicht jeweils mit Abkürzung des zweiten Namensteils).

2.1.3 CD von Aufführung der Kita-Kinder

Eine weitere Anfrage im Berichtsjahr war darauf gerichtet, ob eine Aufführung von Kita-Kindern in einer Kindertagesstätte gefilmt, auf CD gebrannt und an die Familien verteilt werden kann, wenn eine Einwilligung von allen Eltern vorliegt.

Grundsätzlich sind die Aufnahme und die Verteilung an die Eltern möglich. Damit die Einwilligungslösung datenschutzkonform umgesetzt werden kann, sind allerdings einige Aspekte zu beachten.

Hervorzuheben ist zunächst, dass es sich bei der Aufnahme und der Veröffentlichung der Aufnahme (in Form durch das Verbreiten/Verteilen an die Eltern) um zwei voneinander zu trennende Verarbeitungsvorgänge handelt. Für jeden der Vorgänge muss eine Rechtsgrundlage, hier etwa in Form der Einwilligung, vorliegen. Auf einem Einwilligungsformular sollte den Erziehungsberechtigten daher die Möglichkeit gegeben werden, zu beiden Verarbeitungsvorgängen zuzustimmen. Eine Einwilligung muss natürlich von den Erziehungsberechtigten aller gefilmten Kinder vorliegen. Daneben sind auch die Transparenz- und Informationspflichten zu beachten.

„Hervorzuheben ist zunächst, dass es sich bei der Aufnahme und der Veröffentlichung der Aufnahme … um zwei voneinander zu trennende Verarbeitungsvorgänge handelt."

Bezogen auf die Verteilung der CDs ist zu beachten, dass eine Einwilligung widerrufen werden kann. Einmal verteilte CDs werden aber wahrscheinlich schwierig wiederzubeschaffen sein. Das Risiko des Widerrufs durch Erziehungsberechtigte liegt im Bereich des Verantwortlichen. Auch kann die Informiertheit einer solchen Einwilligung problematisch sein. Die Einwilligung sollte hier nicht pauschal (z. B. zu Beginn der Kindergartenzeit) eingeholt werden, sondern abgestimmt auf den speziellen Zweck. Daher sollte das Einwilligungsformular das Veröffentlichungsmedium genau bezeichnen und darauf hinweisen, dass die Aufnahmen auf der CD nur für private Zwecke verwendet und nicht über soziale Medien beziehungsweise das Internet weiterverbreitet werden dürfen.[33]

[33] Siehe hierzu auch den Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands aus 2019 zum Umgang mit Bildern von Kindern und Jugendlichen (abzurufen unter www.katholisches-datenschutzzentrum.de in der Infothek).

2.2 Meldungen von Datenschutzverletzungen

Kirchliche Einrichtungen als Verantwortliche im Sinne des KDG sind verpflichtet, bei Kenntnisnahme von einer Datenschutzverletzung innerhalb von 72 Stunden eine entsprechende Meldung bei der zuständigen Datenschutzaufsicht abzugeben.

Die Anzahl der im Jahr 2023 an das Katholische Datenschutzzentrum gerichteten Meldungen von Datenschutzverletzungen nach § 33 KDG war weiterhin sehr hoch. Im Vergleich zum Vorjahr stieg die Zahl nochmals um 17 % an.

Um eine möglichst fallabschließende Bewertung eines gemeldeten Sachverhalts vornehmen zu können, sind regelmäßig Nachfragen durch das Katholische Datenschutzzentrum bei der zuständigen Ansprechperson notwendig. Davon sind gut ein Drittel der Meldungen betroffen. Nachfragen zum Sachverhalt waren zumeist weniger angezeigt, wenn die Meldungen durch oder mit Unterstützung eines internen oder externen betrieblichen Datenschutzbeauftragten erfolgt sind. Zu den im Nachhinein zu klärenden Fragen gehören solche zu konkreten Schutzmaßnahmen, beispielsweise bei einem elektronischen Versand von Daten, zur Notwendigkeit und Umfang eines Versands oder auch zu bestehenden, internen Regelungen dazu. Auch steht immer wieder die Frage im Raum, ob der Pflicht zur Information der Betroffenen von dem Vorfall ausreichend nachgekommen wurde.

Eine grobe thematische Einordnung der gemeldeten Datenschutzverletzungen im Jahr 2023 zeigt die nachfolgende Statistik. Auszugsweise werden einzelne Punkte im Folgenden erläutert.

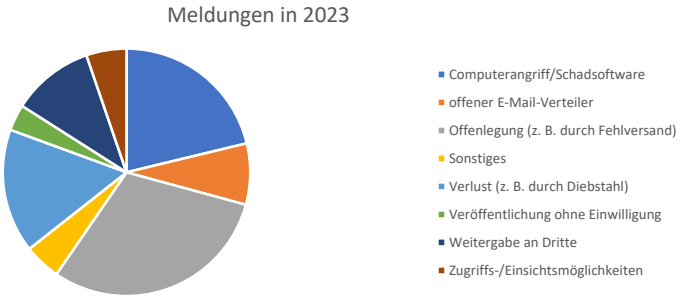


Abb. 2: Meldungen an das Katholische Datenschutzzentrum im Jahr 2023.

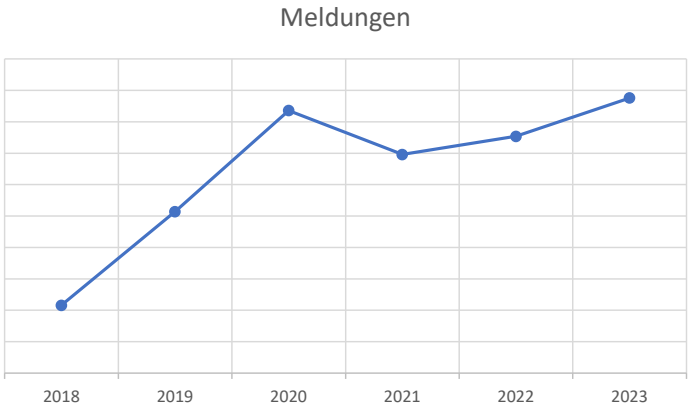


Abb. 3: Meldungen an das KDSZ im Verlauf der Jahre 2018 bis 2023.

2.2.1 Unberechtigte Offenlegung von personenbezogenen Daten durch Fehlversand oder Verlust von Schriftstücken

Eine Vielzahl an Meldungen im Jahr 2023 bezieht sich auf die unberechtigte Offenlegung von personenbezogenen Daten aller Schutzklassen durch Fehlversand oder Verlust von Schriftstücken.

Als Beispiele seien hier der Fehlversand von Arztbriefen, Rechnungen zu Gesundheitsleistungen oder Personalunterlagen genannt. So kommt es z. B. immer wieder bei der Zusammenstellung von Unterlagen einer Patientin oder eines Patienten vor, dass diesem Brief versehentlich auch noch Informationen zu einer anderen Person beigefügt werden, Schreiben für zwei Personen also an eine Person gesendet werden. Oft liegt die Fehlerquelle auch in der Auswahl des Empfängers. Hier gibt es eine Vielzahl von Meldungen, bei denen die automatische Ergänzung von E-Mail-Adressen durch die gängigen E-Mail-Programme zur Auswahl falscher Empfänger führt. Ein geringer Teil der Meldungen zeigte auf, dass der Fehlversand durch einen Ablagefehler in der Vergangenheit begünstigt wurde. Dort waren Daten von unterschiedlichen Patienten in einer Patientenakte gespeichert, was nach Druck und Versand der Akte erst den Empfängern aufgefallen und von diesen der Einrichtung zurückgemeldet worden war.

Zu den bearbeiteten Fällen gehörten im Betrachtungszeitraum ebenfalls Meldungen, bei denen die Offenlegung von Daten nicht durch einen Fehler bei der schriftlichen Kommunikation erfolgte, sondern bei denen die Umstände einer Lebens- oder Arbeitssituation der Beteiligten die Offenlegung begünstigten. So hat beispielsweise in einer Kindertagesstätte ein betreutes Kind die Papierseiten einer auf dem Kopf liegenden und im Raum liegengelassenen Entwicklungsdokumentation für Malpapier gehalten und mit nach Hause genommen. In einem anderen Fall wurde ein Ordner mit Daten von ehrenamtlichen Mitarbeitenden einer Pfarrei vor Antritt der Fahrt auf dem Autodach liegen gelassen und verloren. Auch wenn in diesen beiden Einzelfällen die betroffenen Unterlagen zeitnah wieder vollständig aufgefunden und an die jeweilige Einrichtung zurückgeführt werden konnten, zeigen diese Fälle doch, wie schnell im hektischen Arbeitsalltag Situationen entstehen, aus denen dann Datenschutzverletzungen resultieren können.

Durch wirksame technische und organisatorische Maßnahmen soll der Schutz von personenbezogenen Daten sichergestellt werden. Diese Maßnahmen müssen dann aber auch auf die konkrete Verarbeitung abgestimmt sein und im Arbeitsalltag der Mitarbeitenden fest verankert sein. So wurden dem Katholischen Datenschutzzentrum z. B. Datenschutzverletzungen gemeldet, bei denen vorhandene E-Mail-Verschlüsselungssysteme ihre Schutzwirkung nicht entfalten konnten, weil Daten der Schutzklasse III gemäß § 13 KDG-DVO als Anhang einer E-Mail irrtümlich an einen Verteiler für allgemeine Informationen gesendet wurden, der nicht in die E-Mail-Verschlüsselung eingebunden war. Daher erfolgte der Versand der Daten trotz vorhandener Schutzmaßnahme unverschlüsselt.

„Durch wirksame technische und organisatorische Maßnahmen soll der Schutz von personenbezogenen Daten sichergestellt werden."

Hinweis für kirchliche Einrichtungen

Die gemeldeten Sachverhalte zeigen auch in diesem Berichtszeitraum, dass beim Versand von personenbezogenen Daten aller Schutzklassen immer eine besondere Sorgfalt anzuwenden ist, da hier viele Fehlerquellen lauern. Gehören die betroffenen Daten zu den Schutzklassen II oder III oder sind eindeutig der besonderen Kategorie personenbezogener Daten zuzuordnen, hilft nur eine obligatorische Endkontrolle vor der Versendung dabei, einen Fehlversand und somit den Schutz der Daten sicherzustellen. Hilfreich bleibt es, die Mitarbeitenden durch regelmäßige Schulungen und Beobachtung der Abläufe hinreichend zu sensibilisieren.

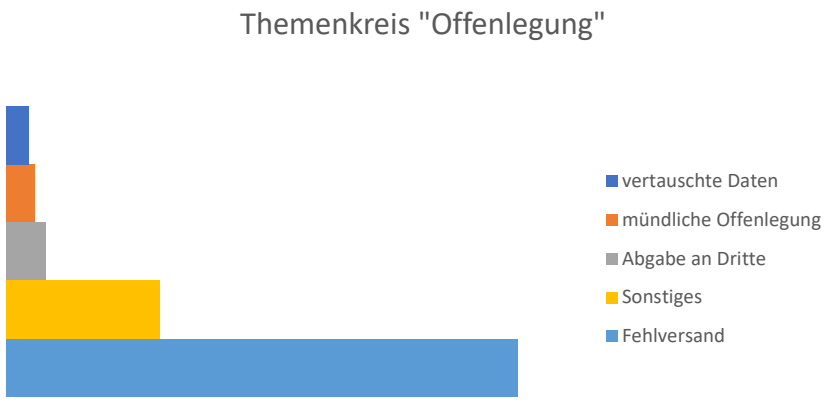


Abb. 4: Meldungen an das KDSZ zum Themenkreis "Offenlegung" im Jahr 2023.

2.2.2 Nutzung offener E-Mail-Verteiler

„Die Verwendung eines offenen E-Mail-Verteilers ist datenschutzrechtlich unzulässig, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben."

Eine häufige und immer wiederkehrende Thematik bei den Meldungen von Datenschutzverletzungen ist die der Nutzung eines offenen E-Mail-Verteilers.[34] Hierbei werden meist allgemeine Informationen, z. B. eine Einladung zu einem Sommerfest einer Kindertageseinrichtung oder Informationen für Erstkommunionkinder, per E-Mail an mehrere Empfänger gesendet, wobei die E-Mail-Adressen für alle Empfänger sichtbar sind, da diese im AN- oder CC-Feld eingetragen werden.[35]

Bei E-Mail-Adressen handelt es sich um personenbezogene Daten gemäß § 4 Nr. 1 KDG. Die Verwendung eines offenen E-Mail-Verteilers ist datenschutzrechtlich unzulässig, wenn die Inhaber der E-Mail-Adressen dazu nicht ihre Einwilligung erklärt haben. Dies ist in der Praxis so gut wie nie der Fall.

Bei Eintragung von E-Mail-Adressen in das AN-Feld oder das CC-Feld sehen alle Empfänger dieser E-Mail, an wen diese sonst noch geschickt wurde. Durch eine unbefugte und nicht notwendige Offenlegung der E-Mail-Adressen werden diese den anderen Adressaten bekannt.

[34] Siehe hierzu auch Abschnitt 3.7.3 des Jahresberichts 2020.
[35] Nicht gemeint sind hier E-Mails, die als Werbung einzustufen sind.

Dadurch wird das Schutzziel der Vertraulichkeit verletzt und eine missbräuchliche Nutzung der Adressen ist nicht auszuschließen, sodass i. d. R. von einem meldepflichtigen Vorgang auszugehen ist. Nur bei Eintragung der E-Mail-Adressen in das BCC-Feld wird die Übertragung der E-Mail-Adressen an die Empfänger unterdrückt.

Im Berichtszeitraum gab es Verteiler mit bis zu 450 betroffenen Empfängern und es wurden berufliche sowie private E-Mail-Adressen offengelegt. Zu erwähnen ist, dass die Schwere einer Datenschutzverletzung sich neben den betroffenen Kategorien personenbezogener Daten auch an der Anzahl der betroffenen Daten (z. B. Anzahl der Empfänger einer E-Mail mit offenem Verteiler) bemisst.

Wie im vorherigen Abschnitt zum Fehlversand[36] ist meist mangelnde Sorgfalt oder Unachtsamkeit der Versender der betroffenen E-Mails ursächlich für die Nutzung eines offenen E-Mail-Verteilers. In den meisten Fällen ist den Mitarbeitenden der Einrichtungen bekannt, dass das BCC-Feld bei mehreren E-Mail-Empfängern zu nutzen ist und dennoch wird dies oft versäumt. Vorgeschlagene Maßnahmen wie (wiederholte) Hinweise zur richtigen Verwendung der Adressfelder bei E-Mail-Versand scheinen deshalb nur bedingt eine Lösung zur Vermeidung von Datenschutzverletzungen aufgrund eines offenen E-Mail-Verteilers zu sein.

„Wie … [beim] Fehlversand ist meist mangelnde Sorgfalt oder Unachtsamkeit der Versender der betroffenen E-Mails ursächlich für die Nutzung eines offenen E-Mail-Verteilers."

2.2.3 Unberechtigte Zugriffe auf den internen Bereich einer Schulhomepage

Gemeldet wurde dem Katholischen Datenschutzzentrum der unberechtigte Zugriff auf den internen Bereich einer Schulhomepage durch Schüler. Ob die Zugangsdaten durch einen Angriff oder durch Passwortweitergabe bekannt wurden, war zum Zeitpunkt der Meldung noch unklar. Der interne Bereich der Schulhomepage wurde umgehend abgeschaltet. Von dem unberechtigten Zugriff waren Adressdaten, interne Bemerkungen des Kollegiums sowie Leistungs- und Gesundheitsdaten betroffen.

Da es sich bei dem Vorfall um Daten der Schutzklasse III gemäß § 13 KDG-DVO handelt, wurde die gesamte Elternschaft von der Datenschutzverletzung informiert. Aufgrund der Benachrichtigung haben einige Schüler weitere Informationen zu der Datenschutzverletzung gemeldet. Den Zugriff auf den internen Bereich der Schulhomepage erlangten Schüler aus verschiedenen Kursen, in denen sich die Lehrkräfte durch unverdeckte Eingabe ihres Passworts an einem Smartboard im internen Bereich der Schulhomepage angemeldet haben. Mit diesen Zugangsdaten haben sich mehrere Schüler angemeldet, Daten ausgelesen und auch weitergegeben. Die Zugriffsmöglichkeit bestand über einen Zeitraum von über einem Jahr.

Aufgrund der neuen Erkenntnisse der Datenschutzverletzung wurden Eltern von Schülern sowie Lehrkräfte, die seit dem Beginn der Datenschutzverletzung die Schule verlassen haben, ebenfalls über den Vorfall informiert.

[36] Abschnitt 2.2.1 dieses Jahresberichts.

Als Konsequenz aus dem Vorfall wurde ein neues internes Schulportal in Betrieb genommen, das über den öffentlichen Teil der Schulhomepage nicht mehr erreichbar ist. Die Lehrkräfte können den internen Bereich über ihre Dienstgeräte erreichen und müssen nicht mehr die Smartboards für den Zugriff nutzen. Um den Zugang zum internen Schulportal weiter abzusichern, wurde für die Anmeldung eine 2-Faktor-Authentisierung implementiert.

Hinweis für kirchliche Stellen

Bei der Eingabe von Zugangsdaten zu geschützten Geräten und Anwendungen oder Systemen ist stets darauf zu achten, dass Nutzernamen und Kennworte nicht mitgelesen werden können. Wo möglich, sollte über die zusätzliche Absicherung sensibler Anwendungen oder Systeme per 2-Faktor-Authentifizierung nachgedacht werden.

2.2.4 Verteilung einer Adressliste mit Gemeindebrief

Bei der Verteilung eines Gemeindebriefes durch ehrenamtlich Mitarbeitende ist die Liste mit Adressen der Haushalte, die einen Gemeindebrief bekommen, zusammen mit einem Gemeindebrief in den Briefkasten eines Haushaltes eingeworfen worden. Da es sich um die Liste einer anderen Straße handelte, wurde der Verlust nicht sofort bemerkt.

Als der Verlust bemerkt wurde, konnte der Kreis der möglichen Empfänger eingegrenzt werden. Durch umgehendes, aktives Nachfragen in den infrage kommenden Haushalten konnte die Liste, die vom Empfängerhaushalt noch nicht bemerkt worden war, wieder an die verteilende Person zurückgegeben werden.

Die ehrenamtlich tätigen Verteiler des Gemeindebriefes sind auf den Datenschutz sowie die Rückgabe oder Vernichtung der Listen verpflichtet worden. Dieser Vorfall wurde zum Anlass genommen, um alle Verteiler nochmals auf die sorgfältige datenschutzkonforme Handhabung der Listen hinzuweisen.

2.3 Beschwerden und Hinweise

Jede Person, die sich durch eine Verarbeitung ihrer personenbezogenen Daten durch eine katholische Einrichtung in ihren Rechten verletzt fühlt, kann bei der Datenschutzaufsicht im Rahmen einer Beschwerde beziehungsweise eines Hinweises (wenn nicht die eigenen Daten betroffen sind) die Verarbeitung der personenbezogenen Daten durch die kirchliche Stelle überprüfen lassen.

Aus der Vielzahl der eingereichten Beschwerden und Hinweise werden nachfolgend ein paar der Sachverhalte aufgegriffen, die nicht schon an anderer Stelle in diesem Bericht erwähnt wurden.

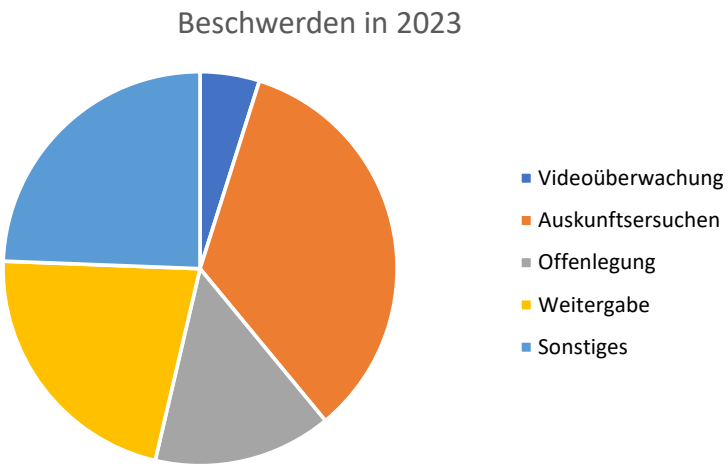


Abb. 5: Beschwerden an das Katholische Datenschutzzentrum Im Jahr 2023.

Bei vielen der eingereichten Beschwerden sind noch Nachfragen bei den Beschwerdeführerinnen oder Beschwerdeführern notwendig, da nicht alle notwendigen Informationen mitgeteilt werden.

Hinweis für kirchliche Einrichtungen

Um diese Nachfragen für die Beschwerdeführerin oder den Beschwerdeführer möglichst in Grenzen zu halten und die (zeitnahe) Bearbeitung der Beschwerde beziehungsweise des Hinweises zu erleichtern, stellt das Katholische Datenschutzzentrum auf seiner Internetseite ein Beschwerdeformular[37] zur Verfügung.

Wird das Formular vollständig ausgefüllt, können viele der sonst regelmäßig zu stellenden Nachfragen entfallen, da die Beschwerdeführerinnen oder der Beschwerdeführer durch die Fragen geführt wird und das Katholische Datenschutzzentrum so die notwendigen Informationen zur Bearbeitung der Beschwerde beziehungsweise des Hinweises erhält.

[37] Link zum Beschwerdeformular auf der Internetseite des KDSZ: https://www.katholisches-datenschutzzentrum.de/beschwerde/

Der Diözesandatenschutzbeauftragte der nordrhein-westfälischen (Erz-)Bistümer und Verbandsdatenschutzbeauftragte des Verbandes der Diözesen Deutschlands (VDD)

Katholisches Datenschutzzentrum

Beschwerde bei der Datenschutzaufsicht
gemäß § 48 des Gesetzes über den Kirchlichen Datenschutz (KDG)

Persönliche Angaben (Beschwerdeführer)

Name, Vorname

Straße und Hausnummer

PLZ und Ort

E-Mail-Adresse

Angaben zum Beschwerdegegner

Name oder Bezeichnung

Straße und Hausnummer

PLZ und Ort

Internetseite (optional)

Informationen zur Vorgangsbearbeitung

Bitte teilen Sie uns mit, auf welchem Weg Sie über den weiteren Verlauf Ihrer Beschwerde informiert werden möchten.

☐ E-Mail verschlüsselt ☐ E-Mail unverschlüsselt

E-MAIL HINWEIS: ein unverschlüsselter Versand von Daten birgt die Gefahr eines unbefugten Zugriffs auf den geführten Schriftwechsel in sich. Wenn verfügbar, werden wir den Informationsaustausch mit Ihnen durch eine S/MIME Verschlüsselung absichern. Ist dies nicht möglich, behalten wir uns den Versand relevanter Daten auf dem Postwege vor.

☐ Post ☐ Keine weiteren Informationen gewünscht

Nennung Ihrer Identität

Im Rahmen der Aufklärung des Beschwerdesachverhaltes ist es unter Umständen erforderlich, Ihre Identität gegenüber der verantwortlichen Stelle des Beschwerdegegners bekannt zu geben. Ohne diese Bekanntgabe kann der Sachverhalt gegebenenfalls nicht geklärt werden. Sofern wir Ihre Identität nicht offenlegen dürfen, weisen wir Sie vorsorglich darauf hin, dass je nach Ausgestaltung des Sachverhaltes bei der Aufklärung des Vorganges trotzdem ein Rückschluss auf Ihre Identität möglich sein kann.

☐ **Ich bin mit der Bekanntgabe meiner Identität einverstanden.**

☐ **Ich widerspreche der Bekanntgabe meiner Identität.**

Wir gehen Ihrer datenschutzrechtlichen Beschwerde nach. Für eine schnelle und effektive Bearbeitung sind wir auf Ihre Hilfe angewiesen.

Bitte füllen Sie deshalb das Formular sorgfältig aus.

Zusammen mit Kopien der für den Sachverhalt relevanten Dokumenten senden Sie es per Post an:

Katholisches Datenschutzzentrum
Brackeler Hellweg 144
44309 Dortmund

Ein Versand des Formulars per E-Mail ist generell möglich, sollte aber nur verschlüsselt erfolgen. Sofern bei Ihnen verfügbar, setzen wir die S/MIME Verschlüsselung ein.

Bei Bedarf stellen wir für Sie einen gesicherten Zugang zur Bereitstellung von relevanten Dokumenten in elektronischer Form zur Verfügung.

Unsere Mailadresse:
info@kdsz.de

Persönlich erreichen Sie uns:

Telefon: 0231/138 985-0

ÖPNV:
U43 der Dortmunder Verkehrsbetriebe, Haltestelle „Brackel Kirche"

Beschwerdeformular Katholisches Datenschutzzentrum / Rev 3.0

Zuständigkeit

Sollte Ihre Beschwerde nicht in unseren Zuständigkeitsbereich fallen, würden wir Ihre Beschwerde an die sachlich zuständige Stelle weiterleiten und Sie darüber informieren. Sofern Sie dies nicht wünschen, werden wir Sie darüber informieren, dass uns eine weitere inhaltliche Bearbeitung Ihrer Beschwerde nicht möglich ist.

☐ **Ich bin mit der Weiterleitung meiner Beschwerde einverstanden.**

☐ **Ich widerspreche einer Weiterleitung meiner Beschwerde.**

Angaben zum Sachverhalt Ihrer Beschwerde

Für eine möglichst präzise Beschreibung hilft die Beantwortung der folgenden Fragen:

		Beispiele
1	Welche persönlichen Daten sind betroffen?	Adressen, Telefonnummern, Bankdaten, Fotos, Gesundheitsdaten
2	Gibt es eine Beziehung (auch ungewollt) zur Stelle oder Person, gegen welche sich Ihre Beschwerde richtet?	Kundenverhältnis, Arbeits- oder Bewerbungsverhältnis, Vertrag, unerwünschte Werbung
3	Wann konkret erfolgte die Datenschutzverletzung?	Bitte geben Sie das entsprechende Datum an.
4	Ist eine Handlung oder Unterlassung Gegenstand der Beschwerde?	Haben Dritte unrechtmäßig Kenntnis von Ihren Daten erhalten? Wurde Ihrem Anspruch auf Auskunft, Berichtigung, Sperrung oder Löschung von Daten nicht nachgekommen?
5	Haben Sie sich zu diesem Sachverhalt bereits an eine andere Stelle gewandt?	andere Datenschutzaufsicht, die Polizei oder Staatsanwaltschaft, ein Gericht

Ihre Beschreibung des Beschwerdesachverhaltes

Beschwerdeformular Katholisches Datenschutzzentrum / Rev 3.0

Abb. 6: Formular zur Abgabe einer Beschwerde an das KDSZ.

2.3.1 Beschwerden aus dem Themenkreis Videoüberwachung

Ein häufiger Gegenstand von Beschwerdeverfahren im Berichtzeitraum war die Videoüberwachung durch und in katholischen Einrichtungen. Beschwerden und Hinweise richteten sich in diesen Fällen meistens gegen eine Videoüberwachung rund um das Gelände einer Kirche, oft auch mit dem Hintergrund, dass nicht nur Bereiche des Gemeindegrundstücks, sondern auch des öffentlichen Raumes mitüberwacht würden.

Neben der Klärung der Frage, ob es für die fallspezifische Videoüberwachung überhaupt beziehungsweise in dem gewählten Umfang eine Rechtsgrundlage gab, wurden formelle Verstöße gegen das KDG untersucht. Verantwortliche verletzten beispielsweise ihre Informationspflichten, indem sie keine oder nur unzureichende Hinweisschilder anbrachten. Auch musste das Katholische Datenschutzzentrum des Öfteren fehlende Verarbeitungsverzeichnisse und Datenschutzfolgenabschätzungen bezüglich der Videoüberwachung feststellen und deren Erstellung anmahnen.

Hinweis für kirchliche Einrichtungen

Verantwortliche sollten sich vor dem Beginn einer Videoüberwachung genau mit den Voraussetzungen, insbesondere den Tatbestandsvoraussetzungen des § 52 KDG beschäftigen. Häufig können Beschwerdeverfahren durch rechtskonforme Hinweisschilder, Verarbeitungsverzeichnisse und Datenschutzfolgenabschätzungen stark verkürzt und bei genügender Transparenz sogar ganz vermieden werden.[38]

2.3.2 Beschwerden zu Auskunftsersuchen (§ 17 KDG)

Wie auch in den letzten Jahren[39] waren nicht oder nicht rechtzeitig oder unvollständig beantwortete Auskunftsersuchen gemäß § 17 KDG eine häufige Thematik bei den im Berichtszeitraum an das Katholische Datenschutzzentrum gerichteten Beschwerden.

Nach Anhörung der Beschwerdeführerinnen und Beschwerdeführer und der kirchlichen Einrichtungen als Beschwerdegegnern konnte das Katholische Datenschutzzentrum in einigen Fällen keine unrichtige oder unvollständige Auskunft feststellen. In anderen Fällen war die Beschwerde (teilweise) begründet und der Beschwerdegegner wurde – je nach Sachverhalt – dazu aufgefordert, innerhalb einer Frist eine vollständige und richtige Auskunft zu erteilen.

Gegenstand der Beschwerden waren u. a. Auskunftsersuchen zu Gesundheitsdaten nach einer ambulanten oder stationären Behandlung, Auskunftsersuchen zu Adressdaten, z. B. im Rahmen der Vorbe-

[38] Für eine ausführliche Darstellung der Voraussetzungen an eine Videoüberwachung siehe Abschnitt 2.8 des Jahresberichts 2021.
[39] Siehe Abschnitt 2.5.1 des Jahresberichts 2021 und Abschnitt 2.3.1 des Jahresberichts 2022.

reitung der Erstkommunion, oder Auskunftsersuchen zu den eigenen Daten in Missbrauchsfällen.

Bei der Aufklärung der Beschwerdefälle war häufig erkennbar, dass falsche oder unvollständige Antworten auf die Auskunftsersuchen auf unzureichende interne Prozesse zur Beantwortung der Ersuchen zurückgeführt werden können. Oft ist der Einrichtung unklar, welche Daten über eine Person an welcher Stelle in einer Einrichtung vorliegen können, wenn die anfragende Person beispielsweise als Mitarbeitender und/oder Nutzender der Einrichtung und/oder aktives Mitglied der örtlichen Kirchengemeinde und/oder Empfänger eines Newsletters und/oder in anderen Funktionen der kirchlichen Einrichtung gegenübertritt. Dabei ist auch zu beachten, dass nicht nur die Daten an sich, sondern auch eventuelle Empfänger der Daten[40] zu beauskunften sind.

Nicht zuletzt im Hinblick auf mögliche Schadenersatzansprüche Betroffener weißt das KDSZ erneut auf die Beachtung der gesetzlichen Grundlagen im Rahmen der Beantwortung von Auskunftsersuchen von Betroffenen gemäß § 17 KDG hin.

„Nicht zuletzt im Hinblick auf mögliche Schadenersatzansprüche Betroffener weißt das KDSZ erneut auf die Beachtung der gesetzlichen Grundlagen im Rahmen der Beantwortung von Auskunftsersuchen von Betroffenen gemäß § 17 KDG hin."

Hinweis für kirchliche Einrichtungen

Den kirchlichen Einrichtungen kann nur erneut empfohlen werden, sich eine Übersicht darüber zu verschaffen, bei welchen internen Prozessen und Arbeitsabläufen welche personenbezogenen Daten der verschiedenen möglichen Personengruppen verarbeitet werden, um im Falle eines Auskunftsersuchens eine richtige und vor allem vollständige Auskunft geben zu können. Ein guter Ausgangspunkt für diese Überlegungen ist das in der Einrichtung vorhandene Verzeichnis von Verarbeitungstätigkeiten.[41]

2.3.3 Datenschutzverletzung durch Missbrauchsstudie

Nach Veröffentlichung der Missbrauchsstudie im Bistum Münster durch die Universität Münster wandte sich ein vom sexuellen Missbrauch Betroffener mit einer Beschwerde an das Katholische Datenschutzzentrum und führte an, dass er durch die Schilderung „seines Falles" innerhalb der veröffentlichten Studie eine Retraumatisierung erlitten habe.[42] Als zuständige Datenschutzaufsicht hat das KDSZ den Beschwerdesachverhalt in dem Rahmen aufgeklärt, dass betrachtet wurde, ob die Offenlegung der personenbezogenen Daten der besonderen Kategorie gemäß § 11 KDG gegenüber den Wissenschaftlern der Universität Münster datenschutzrechtlich als rechtmäßig einzustufen war. Dabei wurde insbesondere betrachtet, inwiefern es sich um eine datenschutzkonforme Anonymisierung dieses Falles handelte.[43]

[40] Siehe hierzu auch Abschnitt 1.5.1 dieses Jahresberichts.
[41] Zu Auskunftsersuchen siehe auch Abschnitt 2.5.1 im Jahresbericht 2021 und Abschnitt 2.3.1 des Jahresberichts 2022.
[42] Siehe hierzu auch die Mitteilung des Bistums Münster vom 21.06.2023 „Von Missbrauch betroffene Person rügt erfolgreich Datenschutzverletzung" (https://www.bistum-muenster.de/startseite_aktuelles/newsuebersicht/news_detail/von_missbrauch_betroffene_person_ruegt_erfolgreich_datenschutzverletzung).
[43] Siehe hierzu auch Abschnitt 1.3.2 dieses Berichts.

Das Beschwerdeverfahren wurde damit abgeschlossen, dass die Beschwerde begründet ist und die nicht ausreichend anonymisierten Aktenbestandteile (die Tatschilderungen des Beschwerdeführers) nicht in dieser Art und Weise ohne Einwilligung an die Wissenschaftler hätten weitergegeben werden dürfen. Aufgrund der Unzuständigkeit des KDSZ für die Universität Münster wurde der Umstand der Veröffentlichung nicht näher betrachtet.

Dieser Beschwerdefall zeigt, dass bei der notwendigen umfassenden Aufarbeitung des Missbrauchs die Rechte der vom Missbrauch betroffenen Personen mit betrachtet werden müssen. Ohne eine Einwilligung der betroffenen Personen wird in so gut wie allen Fällen eine datenschutzkonforme Anonymisierung unerlässlich sein, gerade wenn es um die Veröffentlichung der Ergebnisse der Gutachten geht und hierbei umfangreiche Tatschilderungen wiedergegeben werden. Dabei reicht die alleinige Auslassung des Namens der Betroffenen für eine ausreichende Anonymisierung nicht aus, wenn sich aus den geschilderten Orts- und Zeitangaben sowie weiteren Details der veröffentlichten Schilderung ein Bezug zu einer bestimmten Person herstellen lässt.

2.4 Prüfungen

Im Rahmen seiner Aufgaben führt der Diözesandatenschutzbeauftragte anlassbezogen (aufgrund der bei ihm eingehenden Beschwerden und Hinweise) oder ohne Anlass (im Rahmen regelmäßiger Kontrollen) Prüfungen zur Verbesserung des Datenschutzes durch. Die Prüfungen können vor Ort oder im schriftlichen Verfahren erfolgen.

Im Berichtsjahr 2023 fanden verschiedene (vor Ort) Prüfungen statt oder konnten zum Abschluss gebracht werden. Das Katholische Datenschutzzentrum informiert auf seiner Internetseite über eine Auswahl von Prüfungen.[44]

2.4.1 Prüfung einer Kirchengemeinde

Im Rahmen einer anlasslosen Prüfung[45] wurde eine Kirchengemeinde geprüft. Prüfungsschwerpunkt war die Verarbeitung personenbezogener Daten im Bereich der Jugendarbeit der Kirchengemeinde. Im Fokus stand insbesondere der Umgang mit den personenbezogenen Daten der Minderjährigen von deren Eintritt in die Kirchengemeinde über ihre Beteiligung am Leben in der Kirchengemeinde bis hin zum Ausscheiden aus der Kirchengemeinde. In diesem Rahmen wurden vereinzelt auch weitere Aspekte herausgegriffen.

Die Zusammenarbeit mit der Kirchengemeinde im oben bezeichneten Fall gestaltete sich sehr kooperativ. Angeforderte Dokumente wurden stets fristgerecht eingereicht und auf Nachfragen wurde unverzüglich

[44] https://www.katholisches-datenschutzzentrum.de/themen/pruefungen/

[45] Bei anlasslosen Prüfungen wird durch ein Zufallsprinzip eine Einrichtung beziehungsweise Kirchengemeinde ausgewählt, deren Prozesse nicht vollständig, sondern themenbezogen datenschutzrechtlich vom Katholischen Datenschutzzentrum überprüft werden. Die Prüfungen werden dabei prozessbezogen aufgebaut.

reagiert. Im Rahmen der Prüfung wurden keine größeren Feststellungen zu Verstößen gegen datenschutzrechtliche Vorgaben getroffen. Auch bei einem Vor-Ort-Termin in den Räumen der Kirchengemeinde Ende des Jahres 2022 konnten alle für die Prüfung relevanten Fragen geklärt werden. Die Prüfung wurde im Laufe des Jahres 2023 abgeschlossen.[46] Alle im Prüfbericht erfassten Feststellungen wurden nachweislich behoben.

2.4.2 Prüfung der Transportverschlüsselung von Internetseiten kirchlicher Einrichtungen

Das Katholische Datenschutzzentrum hat im Berichtszeitraum eine Prüfung der TLS-Verschlüsselung ausgewählter Internetseiten kirchlicher Einrichtungen durchgeführt. Die Transportverschlüsselung der Daten durch TLS stellt eine wichtige technische Schutzmaßnahme nach § 26 KDG zum Schutz der übertragenen personenbezogenen Daten dar.

Als Ergebnis der Prüfung konnte bei gut 80 % der überprüften Seiten eine datenschutzkonforme Absicherung per TLS-Verschlüsselung festgestellt werden. Von den Verantwortlichen der anderen geprüften Internetseiten wurden mittlerweile Maßnahmen zur Sicherstellung eines ausreichenden datenschutzkonformen Einsatzes der Transportverschlüsselung ergriffen.

Hintergrund:

> **„… müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet."**

Eine Internetseite kann nicht nur Informationen bereitstellen, sondern dient je nach Inhalt der Seite auch dem Informationsaustausch zwischen Nutzer und Seitenbetreiber. Auf Internetseiten ist es z. B. möglich, Fragen zu stellen, einen Kommentar zu hinterlassen, einen Newsletter zu bestellen, einen Online-Shop zu nutzen oder auch die eigenen Kontaktdaten für den Betreiber zu hinterlassen. Gemäß § 7 Abs. 1 lit. f) KDG in Verbindung mit § 26 Abs. 1 Satz 1 KDG müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. § 26 Abs. 1 Satz 2 lit. a) KDG nennt hierfür neben der Pseudonymisierung und Anonymisierung auch die Verschlüsselung als mögliche Maßnahme.

Hinweis für kirchliche Einrichtungen

Um die Datenschutzziele der Vertraulichkeit und Integrität der übermittelten personenbezogenen Daten von Webservern an den Browser des Internetseitenbesuchers sicherzustellen, ist eine Verschlüsselung der Verbindung mit einer dem Stand der Technik entsprechenden Transportverschlüsselung sehr wichtig. Bei sensiblen Daten kann sie sogar unerlässlich sein.

Der für den Betrieb der Internetseite Verantwortliche hat auch für die elektronische Übertragung der personenbezogenen Daten Schutz-

[46] Zur Prüfung siehe auch Abschnitt 2.4.2 im Jahresbericht 2022.

maßnahmen zu treffen (vgl. § 6 Abs. 2 lit. d) KDG-DVO). Diese Schutzmaßnahmen sind gemäß § 26 Abs. 1 KDG unter Berücksichtigung des Stands der Technik umzusetzen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seiner technischen Richtlinie TR-02102-2[47] Empfehlungen für die Verwendung von TLS als Transportverschlüsselung veröffentlicht. TLS ist nach der Empfehlung des BSI nur in der Version TLS 1.2 und TLS 1.3 als sicher einzustufen.

Unter Rückgriff auf die technische Richtlinie des BSI hat das Katholische Datenschutzzentrum in der Prüfung die vom BSI als unsicher eingestuften TLS-Versionen nicht mehr als dem Stand der Technik im Sinne des § 26 Abs. 1 KDG entsprechend angesehen. Sie können daher keine ausreichenden Schutzmaßnahmen im Sinne des § 26 KDG mehr sein.

Überprüfung:

Basierend auf einer zufälligen Auswahl wurden im Rahmen der Prüfung Internetseiten von Einrichtungen aus dem Zuständigkeitsbereich des Katholischen Datenschutzzentrums auf die vorhandene TLS-Verschlüsselung geprüft. Neben der Überprüfung der eingesetzten Transportverschlüsselung wurde eine Schwachstellenanalyse der TLS-Konfiguration durchgeführt. Die Schwachstellenanalyse wurde nicht invasiv, also ohne Ausnutzung etwaiger gefundener Schwachstellen, durchgeführt.

Bei rund 80 % der geprüften Internetseiten waren die vom BSI als sicher eingestuften TLS-Versionen 1.2 und 1.3 im Einsatz. Die Schwachstellenanalyse dieser Internetseiten konnte keine bekannte Schwachstelle aufdecken.

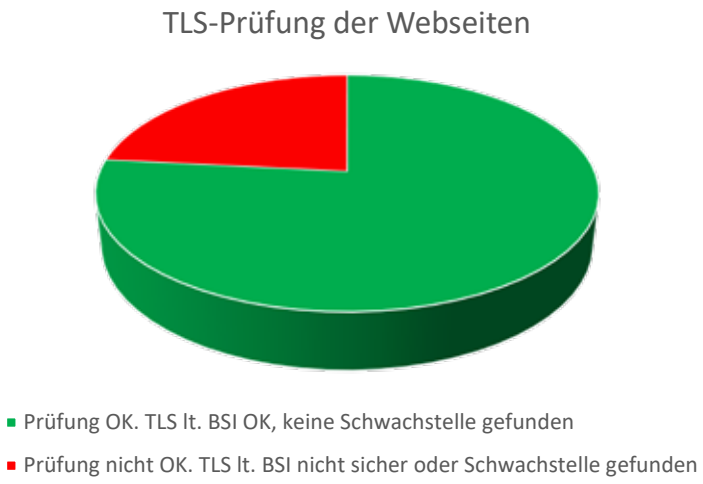


Abb. 7: Gesamtergebnis der geprüften Internetseiten.

Bei den verbleibenden 20 % der geprüften Internetseiten konnten durch die Prüfung zwei verschiedene Problemfelder aufgezeigt werden.

[47] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7

Ein Teil der Internetseiten verwendete die vom BSI als nicht sicher eingestuften TLS-Versionen 1.0 oder 1.1. Diese Internetseiten waren dadurch mit den Schwachstellen behaftet, die durch die Verwendung dieser alten TLS-Versionen einhergehen. Beispielsweise die als „BEAST" bekannte TLS-Schwachstelle kann nur durch eine neuere TLS-Version mitigiert werden und nicht durch Konfigurationsänderungen beseitigt werden (CVE-2011-3389).

Der kleinere Teil der Internetseiten, die bei der Überprüfung des Katholischen Datenschutzzentrums aufgefallen sind, verwendet zwar eine vom BSI als sicher eingestufte TLS-Version, durch eine nicht optimale Konfiguration der Webserver sind diese Internetseiten aber dennoch mit Schwachstellen behaftet und angreifbar. Bei der Verwendung von TLS 1.3 kann beispielsweise die als „Sweet32" bekannte TLS-Schwachstelle (CVE-2016-2183) auf einem nicht optimal konfigurierten Webserver für einen Angriff genutzt werden.

Abb. 8: Aufteilung der auffälligen Internetseiten.

„Keine der geprüften Internetseiten wurde ohne Verschlüsselung vorgefunden."

Keine der geprüften Internetseiten wurde ohne Verschlüsselung vorgefunden. Auch ältere Verschlüsselungen wie z. B. SSL v2/v3 waren nicht mehr in Betrieb.

Hinweise für kirchliche Einrichtungen (1)

Überprüfen Sie Ihre eigenen Internetseiten daraufhin, ob die von Ihnen eingesetzten Verschlüsselungsverfahren noch den Empfehlungen des BSI entsprechen und passen Sie diese ansonsten an.

Hinweis für kirchliche Einrichtungen (2)

Gerade technische Schutzmaßnahmen müssen regelmäßig vom Verantwortlichen daraufhin überprüft werden, ob sie noch den festgelegten und erwarteten Schutzzweck erfüllen können. Entsprechen die eingesetzten Schutzmaßnahmen nicht mehr den für die konkrete Verarbeitung personenbezogener Daten notwendigen Schutzvorgaben, sind die Maßnahmen weiterzuentwickeln.

2.4.3 Prüfung der Absicherung von E-Mail-Accounts

Im Berichtszeitraum konnte das Katholische Datenschutzzentrum bei den eingehenden Meldungen von Datenschutzverletzungen ein erhöhtes Aufkommen von Angriffen auf E-Mail-Accounts feststellen. Dabei scheint die Absicht hinter diesen Angriffen in den meisten Fällen nicht nur die Erbeutung von Zugangsdaten von E-Mail-Kontakten zu sein, sondern auch durch den Versand von Phishingmails über das kompromittierte Postfach die Glaubwürdigkeit dieser E-Mails im Kreis der Empfänger zu erhöhen. Durch Anklicken von Links oder Anhängen in diesen E-Mails wird oft kompromittierte Software aus dem Internet nachgeladen, die weitreichende Schäden verursacht oder Zugriffe auf ganze IT-Landschaften ermöglicht.

Das Katholische Datenschutzzentrum hat diese Entwicklung zum Anlass genommen, im Berichtszeitraum eine Querschnittsprüfung in Form eines Online-Fragebogens durchzuführen, um mit dieser Prüfung den Stand der E-Mail-Sicherheit in kirchlichen Einrichtungen im Zuständigkeitsbereich zu prüfen. Alle Teilnehmenden wurden zufällig aus den kirchlichen Einrichtungen im Zuständigkeitsbereich ausgewählt.

Die Online-Prüfung wurde in fünf Themenbereiche aufgeteilt:

1. Schulung zur Bedrohungslage, Angriffsarten (insbesondere Phishing und Social-Engineering) und präventives Verhalten.

2. Sichere Authentisierung, Rollen und Berechtigungen sowie Nutzerverwaltung.

3. Strukturierte Verwaltung der Postfächer, sicherer Zugang zum Postfach (z. B. über eine Internetseite oder aus dem Homeoffice).

4. Protokollierung der Aktivitäten am Internetübergangspunkt, Blockierung, Protokollierung und Alarmierung, Protokollierungs- und Analysekonzept.

5. Inventarisierung, Patch-Management, Backup-Konzept.

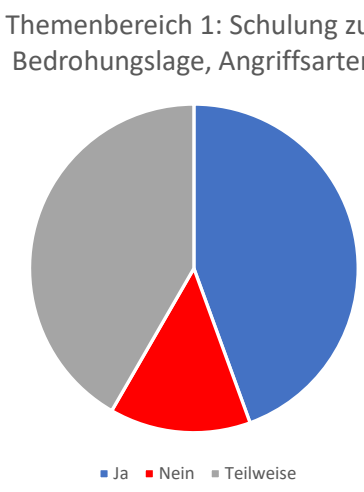


Abb. 9: Aufteilung der Antworten zum Themenbereich "Schulung".

Beim Thema Schulungen gaben rund 44 % der befragten Einrichtungen an, Schulungen würden in der Einrichtung durchgeführt und die in der Umfrage abgefragten Inhalte würden vermittelt, während rund 42 % der Befragten meldeten, dass zwar Schulungen durchgeführt würden, diese aber nicht alle in der Umfrage abgefragten Inhalte einschließen würden. Gut 14 % der Einrichtungen gaben an, keine Schulungen zum Thema durchgeführt zu haben.

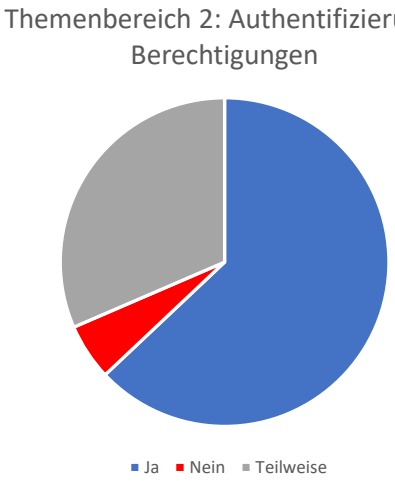


Abb. 10: Antworten der Befragten Einrichtungen zum Themenbereich „Authentifizierung und Berechtigungen".

Bei diesem Themenbereich gaben 63 % der Befragten an, eine Auswahl von sicheren Authentifizierungsmaßnahmen (z. B. komplexe Passwörter, mehrstufige Authentifizierung) einzusetzen. Außerdem existiere ein Rollen- und Berechtigungskonzept und Nutzerkonten würden regelmäßig überprüft. Demgegenüber gaben 31,5 % der Stellen an, mehrstufige Authentifizierung sowie Rollen- und Berechtigungskonzepte nicht implementiert zu haben. Bei 5,5 % der Einrichtungen steht angabegemäß kein Fachpersonal zur Verfügung oder der beauftragte Dienstleister setzt die Maßnahmen nicht um.

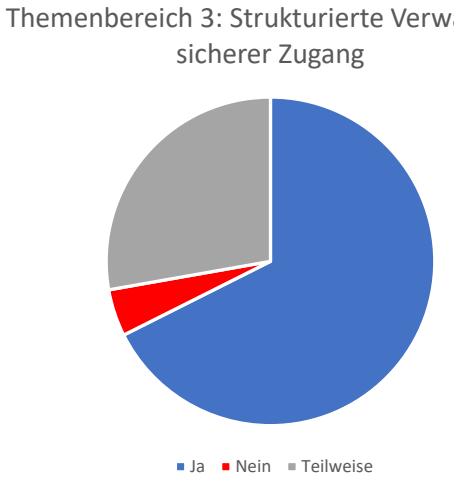


Abb. 11: Antwortaufteilung zum Themenbereich "Strukturierte Verwaltung und sicherer Zugang".

Zur Frage der Verwaltung und des sicheren Zugangs zu den Postfächern gaben fast 68 % der Befragten an, die Verwaltung der Postfächer erfolge strukturiert durch eine Fachabteilung, Clients würden gezielt konfiguriert und die Zugänge zum Postfach über z. B. eine Internetseite,

das Smartphone oder aus dem Homeoffice seien sicher ausgestaltet. Bei gut 28 % der befragten Einrichtungen erfolgte angabegemäß keine gezielte Konfiguration der verwendeten Clients und es wurde nur teilweise eine sichere Ausgestaltung der Zugänge zum Postfach eingerichtet. In 4 % der befragten Einrichtungen fehlten entsprechende Maßnahmen oder Vorgaben mangels Geldes oder Zeit oder die Administration der IT war an einen externen Dienstleister ausgelagert, der die notwendigen Maßnahmen nicht ergriffen hat.

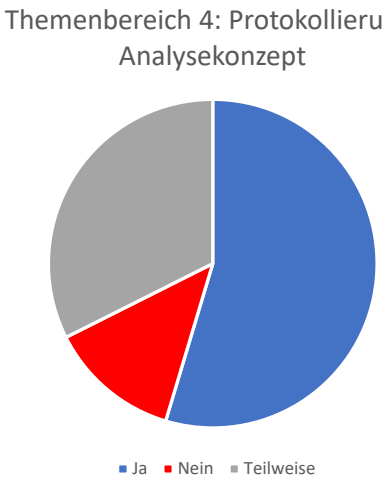


Abb. 12: Aufteilung der Antworten zum Themenbereich „Protokollierung und Analysekonzept".

Im Themengebiet Protokollierung und Analyse verdächtiger Aktivitäten gaben gut 55 % der Befragten an, dass Aktivitäten am Internetübergangspunkt protokolliert und Aufrufe bekannter verdächtiger Inhalte blockiert, protokolliert und alarmiert würden. Dazu bestünde ein Protokollierungs- und Analysekonzept und die Firewallsysteme würden regelmäßig auf ordnungsgemäße Konfiguration überprüft. Demgegenüber gaben 32 % der Befragten an, es würden keine Protokollierungs- und Analysekonzepte existieren und es fände keine Blockierung, Protokollierung und Alarmierung verdächtiger Inhalte statt. Bei 13 % der befragten Einrichtungen standen keine Zeit, kein Geld oder kein Fachpersonal zur Umsetzung der Maßnahmen zur Verfügung oder ein beauftragter Dienstleister konnte die Maßnahmen nicht umsetzen oder wurde mit der Umsetzung nicht beauftragt.

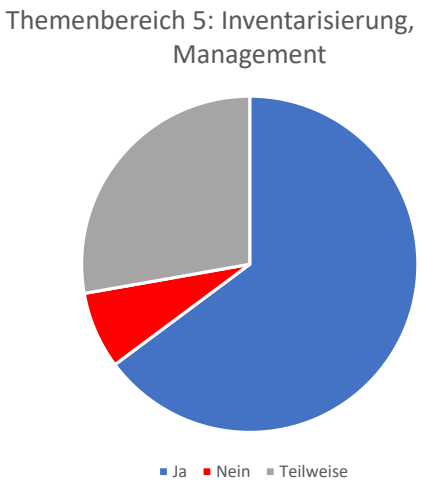


Abb. 13: Antwortaufteilung zum Themenbereich „Inventarisierung und Patchmanagement".

Beim Thema Inventarisierung und Patchmanagement gaben 65 % der Befragten an, eine IT-Inventarisierung sei vorhanden und eine Basiskonfiguration aller Geräte werde durchgeführt. Außerdem seien ein Patchmanagement und Backup-Konzept implementiert. Nur 7 % der befragten Einrichtungen antworteten, es gebe keine Inventarisierung oder es stehe kein Fachpersonal zur Umsetzung der Maßnahmen zur Verfügung und ein Dienstleister wurde mit der Umsetzung nicht beauftragt. Bei 28 % der befragten Einrichtungen standen keine Zeit, kein Geld oder kein Fachpersonal zur Umsetzung der Maßnahmen zur Verfügung oder ein beauftragter Dienstleister konnte die Maßnahmen nicht umsetzen oder wurde mit der Umsetzung nicht beauftragt.

Die Ergebnisse dieser Prüfung zeigen, dass Maßnahmen nicht in allen befragten Einrichtungen in ausreichendem Maße umgesetzt werden. Über die verschiedenen Kategorien und Größen der Einrichtungen sind die Ergebnisse gleichmäßig verteilt. Kleinere Einrichtungen ohne dedizierte IT-Abteilung sind nicht generell schlechter aufgestellt als große Einrichtungen mit eigenem IT-Personal.

„... ist erkennbar, dass durch eine Kombination aus den richtigen technischen und organisatorischen Maßnahmen ein hoher Schutz gegen Angriffe ... erreicht werden kann."

Aus der Analyse der gemeldeten Datenschutzverletzungen im Bereich E-Mail und den Ergebnissen dieser Prüfung ist erkennbar, dass durch eine Kombination aus den richtigen technischen und organisatorischen Maßnahmen ein hoher Schutz gegen Angriffe – wie z. B. durch Phishing – erreicht werden kann. Schulungen und Awareness sind aus Sicht des Katholischen Datenschutzzentrums ein wesentlicher Baustein der Maßnahmen. Mitarbeitende müssen wissen, wie verdächtige E-Mails identifiziert werden können und wie damit umzugehen ist. Technische Maßnahmen – wie z. B. E-Mail-Filter – sind in der Lage, schädliche E-Mails gut zu erkennen und auszufiltern. Da sich der Versand der schädlichen E-Mails ebenfalls weiterentwickelt, müssen die Anwender aber auch in die Lage versetzt werden, zu wissen was zu tun ist, wenn eine verdächtige E-Mail es doch bis in den Posteingang schafft. Die technischen Anforderungen an E-Mail-Server gilt es ebenso im Blick zu behalten: Der Lifecycle der verwendeten Produkte, das eingesetzte Patchlevel des Servers sowie Best Practice zur sicheren Konfiguration der eingesetzten Produkte sind kontinuierlich zu beobachten und die aktuelle Situation unter Risikogesichtspunkten zu bewerten. Dies gilt sowohl für die Server als auch für die auf den Clients eingesetzten Produkte. Die Administration der Server und auch die Kontrolle der Postfächer beziehungsweise Nutzerkonten sollte kontinuierlich erfolgen. Anlegen neuer User, Berechtigungsvergabe nach dem Need-to-Know- und Least-Privilege-Prinzip, aber auch das zeitnahe Deaktivieren von nicht mehr benötigten Postfächern und Nutzkonten erhöht die Sicherheit.

2.4.4 Prüfung der Datenschutzerklärungen von Internetseiten

Im Berichtsjahr wurde eine Prüfung von einzelnen Datenschutzerklärungen auf Internetseiten durchgeführt. Konkreter Prüfungsgegenstand waren die auf den Internetseiten in der Datenschutzerklärung genannten gesetzlichen Grundlagen. Geprüft wurden z. B. die Internetauftritte der (Erz-)Bistümer, der Diözesancaritasverbände sowie des Verbandes der Diözesen Deutschlands und weitere Seiten von Ein-

richtungen aus diesem Bereich, welche der Aufsicht des Katholischen Datenschutzzentrums unterfallen. Die geprüften Einrichtungen wurden ausgewählt, da ihnen aufgrund ihrer Aufgaben und/oder Stellung eine zentrale Funktion zukommt.

Die korrekte Benennung des anzuwendenden Gesetzes dient auch der effektiven Rechtsausübung durch betroffene Personen. Zwar bestehen weitgehende Übereinstimmungen zwischen den Vorgaben des KDG und denen der DSGVO. Jedoch führt eine Verwechslung des anzuwenden Gesetzes aufgrund falscher Angaben des Verantwortlichen teilweise etwa zu Beschwerden bei der unzuständigen Aufsicht. Diese leitet die Beschwerden in diesen Fällen zwar an die zuständige Aufsicht weiter. Allerdings stellt dies eine nicht notwendige Verzögerung dar, die die Wahrnehmung der Betroffenenrechte erschweren kann, da sich etwaige Verstöße nach längerer Zeit möglicherweise nicht mehr vollumfänglich aufklären lassen. Auch ist ein schnelles aufsichtsbehördliches Einschreiten hierdurch nicht möglich.

Im Rahmen der Prüfung zeigte sich, dass die Datenschutzerklärungen von sehr unterschiedlicher Qualität sind. Aus diesem Grund wurde zunächst der Kontakt zu solchen Einrichtungen gesucht, welche gar keine oder jedenfalls eine unzureichende Datenschutzerklärung auf ihren Internetseiten führten. Diesen Einrichtungen wurde sodann Gelegenheit zur Nachbesserung gewährt.

Die Datenschutzerklärungen wurden von allen kontaktierten Einrichtungen verbessert und überarbeitet. Die Prüfung wurde im Laufe des Jahres abgeschlossen. Auch zukünftig wird das Katholische Datenschutzzentrum Einrichtungen anlasslos und anlassbezogen bezüglich ihrer Datenschutzerklärungen überprüfen.

„Auch zukünftig wird das Katholische Datenschutzzentrum Einrichtungen anlasslos und anlassbezogen bezüglich ihrer Datenschutzerklärungen überprüfen."

2.4.5 Prüfung der Organisation des betrieblichen Datenschutzes

Im Berichtzeitraum wurde eine Querschnittsprüfung bezüglich der Tätigkeiten der betrieblichen Datenschutzbeauftragten durchgeführt.

Bei der Umsetzung des Datenschutzes in den (kirchlichen) Einrichtungen nimmt der betriebliche Datenschutzbeauftragte eine zentrale Funktion wahr. Er hat unter anderem die Aufgabe, auf die Einhaltung der Vorschriften über den Datenschutz hinzuwirken und steht dem Verantwortlichen beratend zur Seite.

Aufgrund dieser bedeutenden Position der betrieblichen Datenschutzbeauftragten hat das Katholische Datenschutzzentrum eine Umfrage gestartet, um allgemeine Informationen abzufragen und so einen besseren Überblick über ihre Tätigkeit und Einbindung in den kirchlichen Einrichtungen zu erhalten. Das KDSZ folgt mit seiner Umfrage der vom Europäischen Datenschutzausschuss koordinierten Prüfaktion[48] zu Stellung und Aufgaben des betrieblichen Datenschutzbeauftragten, die die Relevanz der betrieblichen Datenschutzbeauftragten für eine wirksame Umsetzung des Datenschutzes ebenfalls unterstreicht.

[48] https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_de

Zielgruppe der Querschnittsprüfung waren alle Arten kirchlicher Einrichtungen im Zuständigkeitsbereich des Katholisches Datenschutzzentrums, d. h. neben Pfarrgemeinden wurden z. B. auch Krankenhäuser, Alten- und Pflegeheime, Caritasverbände und verschiedene Sozialdienstleister befragt. Insgesamt wurden 100 katholische Einrichtungen per Zufallsprinzip ausgewählt. Die zu der Prüfung gehörende Umfrage wurde ausschließlich online durchgeführt. Vor-Ort- beziehungsweise Betriebsprüfungen waren in dieser Prüfung nicht vorgesehen.

Die Prüfung umfasste Fragen zu Einrichtungsgröße, Qualifikation des Datenschutzbeauftragten, Ressourcen des Datenschutzbeauftragten, weiteren Aufgaben und Pflichten und Interessenkonflikten, der Eingliederung in die Einrichtung, Tätigkeitsberichten und durch den Datenschutzbeauftragten durchgeführten Datenschutzaudits.

Positiv hervorzuheben ist zunächst, dass sich alle 100 ausgewählten Einrichtungen, wie aufgefordert, an der Umfrage beteiligt haben. Aufsichtsbehördliche Maßnahmen oder Bußgeldverfahren wegen unkooperativem Verhalten mussten gegen keine der Einrichtungen eingeleitet werden.

Auffällig war, dass ein Großteil der befragten Einrichtungen angab, dass sie einen externen betrieblichen Datenschutzbeauftragten benannt haben. Sofern sie einen internen betrieblichen Datenschutzbeauftragten benannt haben, übt dieser die Tätigkeit zum überwiegenden Großteil nicht als Vollzeit-, sondern als Teilzeitstelle aus, wobei diese Datenschutzbeauftragten in den meisten Fällen eine weitere Tätigkeit in der Einrichtung ausüben. Beachtlich ist dabei, dass Einrichtungen vereinzelt angegeben haben, dass ihr Datenschutzbeauftragter gleichzeitig die Geschäftsführung wahrnimmt, was gegen das Benennungsverbot aus § 36 Abs. 7 S. 1 KDG verstößt.

Erfreulich ist, dass in den meisten Einrichtungen seit dem Inkrafttreten des KDG ein Datenschutzaudit durch den Datenschutzbeauftragten durchgeführt worden ist.

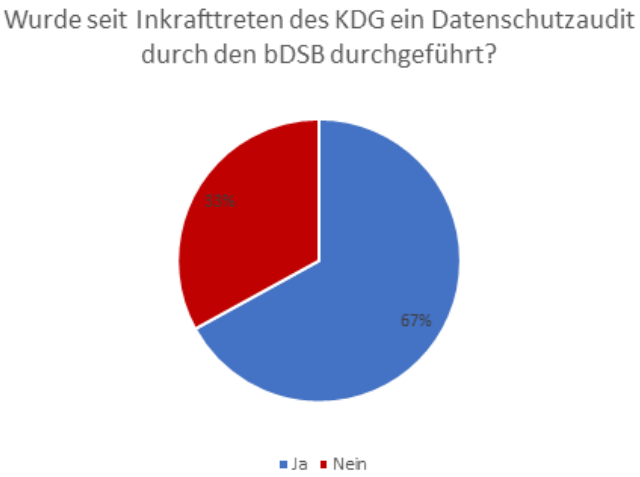


Abb. 14: Antwortverteilung zur Frage nach einem durchgeführten Datenschutzaudit.

Dabei hat nur der geringere Teil der Befragten angegeben, dass der betriebliche Datenschutzbeauftragte schon einmal in ihrer Einrichtung vor Ort war.

Abb. 15: Antwortverteilung zur Frage, ob der bDSB schon einmal in der Einrichtung war.

Der überwiegende Teil der Datenschutzbeauftragten erstellt außerdem einen Tätigkeitsbericht, wobei dies am häufigsten jährlich geschieht.

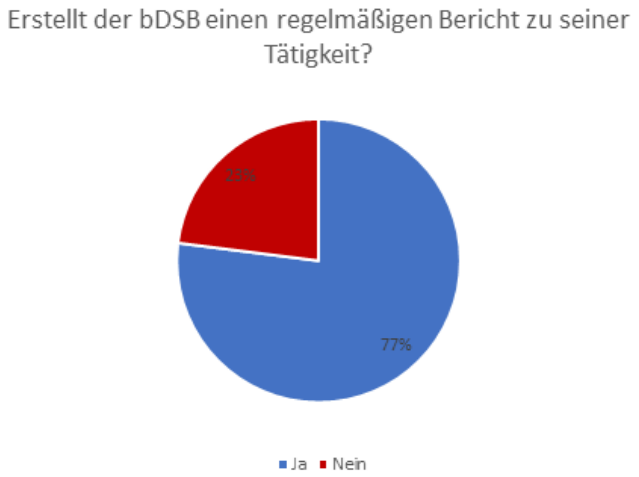


Abb. 16: Antwortverteilung zur Frage nach einem Tätigkeitsbericht des bDSB.

Hinweis für kirchliche Einrichtungen

Nach Auswertung der Umfrage ist den meisten Verantwortlichen zu raten, dass ein noch regelmäßigerer Austausch mit den Datenschutzbeauftragten gesucht beziehungsweise eingerichtet wird, da der sporadische und unregelmäßige Kontakt zu den Datenschutzbeauftragten in den Einrichtungen zu sehr langen Bearbeitungszeiten der Umfrage geführt hat, was auch bei anderen Anfragen problematisch sein könnte. Das gilt insbesondere für die Verantwortlichen, die einen externen Datenschutzbeauftragten benannt haben. Ein positiver Effekt, regelmäßiger mit dem Datenschutzbeauftragten in Kontakt zu treten, könnte darin liegen, das eigene Verständnis vom Aufgabenprofil des Datenschutzbeauftragten zu schärfen und eine erhöhte Wahrnehmung für datenschutzrechtliche Fehlstellungen in den Einrichtungen zu erreichen.

2.5 Wegfall der einrichtungsbezogenen Impfpflicht und Datenlöschung

Mit Änderung des Infektionsschutzgesetzes (IfSG) zum 01.01.2023 ist der § 20a IfSG aufgehoben worden. Damit endete die Pflicht für Mitarbeitende, die z. B. in Krankenhäusern tätig sind, dem Dienstgeber einen Nachweis über eine erfolgte Impfung gegen eine oder die Genesung von einer Covid-19-Erkrankung vorzulegen. Demzufolge endete auf Arbeitgeberseite das Recht auf Aufbewahrung der in diesem Zusammenhang erhobenen und gespeicherten personenbezogenen Daten.[49]

Hinweis für kirchliche Einrichtungen

Datenschutzrechtlich ist somit die Speicherung von personenbezogenen Daten im Zusammenhang mit dem Impf-/Genesungsstatus spätestens nach Ende April 2023 nicht mehr auf der Grundlage des § 20a IfSG zulässig. Auf Basis dieser Rechtsgrundlage erhobene personenbezogene Daten sind zu löschen.

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

Das Katholische Datenschutzzentrum ist regelmäßiger Gast bei den Treffen der betrieblichen Datenschutzbeauftragten der Generalvikariate und der Diözesan-Caritasverbände und steht so in stetem Austausch mit diesen.

Im Berichtsjahr fanden sechs Treffen statt, i. d. R. sind diese in Präsenz, teilweise wurden die Veranstaltungen auch hybrid durchgeführt. Die betrieblichen Datenschutzbeauftragten diskutieren neben aktuellen Themen auch grundlegende Fragestellungen aus ihren Zuständigkeitsbereichen.

„Das Katholische Datenschutzzentrum ist als Gast nicht nur Zuhörer, sondern hat für Fragen ein offenes Ohr und steht beratend zur Verfügung."

Ein wiederkehrendes Thema in der Runde der bDSB sind beispielsweise Fragen rund um die in den Einrichtungen genutzten Anwendungen. Weiterer Diskussionsbedarf bestand z. B. in Bezug auf die Firm-App des Bonifatiuswerks[50], die Nutzung des elektronischen Behördenpostfachs (beBPo) durch Kirchengemeinden und den Umgang mit dem Hinweisgeberschutzgesetz[51], besonders im Hinblick auf die Einführung von Meldestellen nach dem HinSchG.

Das Katholische Datenschutzzentrum ist als Gast nicht nur Zuhörer, sondern hat für Fragen ein offenes Ohr und steht beratend zur Verfügung.

[49] Siehe hierzu auch Abschnitt 2.5 im Jahresbericht 2022.
[50] Siehe hierzu Abschnitt 2.1.1 dieses Berichts.
[51] Siehe Abschnitt 1.2.1 in diesem Jahresbericht.

2.7 Umgang mit Facebook-Fanpages im kirchlichen Bereich

Mit dem Bescheid des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an das Bundespresseamt vom 17.02.2023 hat der Bundesbeauftragte die Konsequenzen aus dem Urteil des Europäischen Gerichtshofs aus dem Jahr 2018 gezogen und eine Untersagung der weiteren Nutzung von Facebook-Fanpages durch das Bundespresseamt ausgesprochen.[52] Dem vorausgegangen waren seit 2018 mehrere Befassungen mit diesem Thema in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und mehrere Schreiben an die Bundesverwaltung.

Auch die Konferenz der Diözesandatenschutzbeauftragten hat schon mit ihren Beschlüssen[53] von Juli 2018 und Oktober 2018 die Thematik gegenüber den kirchlichen Einrichtungen adressiert und die Empfehlung ausgesprochen, auf den Betrieb einer Facebook-Fanpage zu verzichten, da eine datenschutzrechtliche Haftung des Betreibers einer Fanpage nicht wirksam ausgeschlossen werden könne. Dem folgte Mitte 2019 eine Abfrage bei den Generalvikariaten zur Nutzung von Facebook-Fanpages in den (Erz-)Diözesen. Das Thema wurde auch in den Jahresberichten des Katholischen Datenschutzzentrums aufgegriffen.[54]

Das KDSZ hat – ebenso wie die anderen staatlichen und kirchlichen Datenschutzaufsichtsbehörden – in den letzten Jahren viele Stellen und Einrichtungen zu den rechtlichen Rahmenbedingungen des Betriebs einer Facebook-Fanpages beraten. Dies hat in den meisten Fällen aber nicht dazu geführt, dass die kirchlichen Stellen einen aus Sicht der Datenschutzaufsichten datenschutzkonformen Betrieb der Facebook-Fanpages erreicht beziehungsweise die Fanpages deswegen nicht (mehr) unterhalten haben.

Aus diesem Grund hat der Diözesandatenschutzbeauftragte für die bayerischen (Erz-)Diözesen die Nutzung von Facebook-Fanpages für Einrichtungen in seinem Zuständigkeitsbereich untersagt.

Hinweis für kirchliche Einrichtungen

Zwar hat sich das Katholische Datenschutzzentrum einer solchen Allgemeinverfügung nicht angeschlossen, es wird in Zukunft aber bei Prüfungen und Beschwerden verstärkt auf dieses Thema achten und gegebenenfalls handeln.

[52] Im Juli 2023 teilte die Sächsische Datenschutz- und Transparenzbeauftragte mit, dass sie der sächsischen Staatskanzlei ebenfalls den Betrieb einer Facebook-Fanpage untersagt habe; siehe https://www.datenschutz.sachsen.de/staatskanzlei-muss-facebook-fanpage-abschalten-6249.html.

[53] Die Beschlüsse der Konferenz werden auf der Internetseite des KDSZ in der Infothek veröffentlicht: https://www.katholisches-datenschutzzentrum.de/infothek/

[54] Siehe z. B. Abschnitt 2.3.2 des Jahresberichts 2019.

2.8 Das Kirchliche Datenschutzmodell (KDM)

Im Jahr 2023 wurde das Projekt Kirchliches Datenschutzmodell (KDM)[55] – ein gemeinsames Projekt der evangelischen und katholischen Datenschutzaufsichten – erfolgreich abgeschlossen und das Thema in den Regelbetrieb der einzelnen kirchlichen Datenschutzaufsichten übergeben.

Das KDM ist ein Werkzeug zur Auswahl und Bewertung technischer und organisatorischer Schutzmaßnahmen in kirchlichen Einrichtungen. Seit Verabschiedung des KDM im Jahr 2021 hat die ökumenische Arbeitsgruppe unter der Leitung des Beauftragten für den Datenschutz der EKD und des Leiters des Katholischen Datenschutzzentrums das Informationsangebot ständig erweitert.

Auf dem ökumenischen Datenschutztag der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands und der Konferenz der Beauftragten für den Datenschutz in der Evangelischen Kirche in Deutschland am 19.04.2023 wurde das Kirchliche Datenschutzmodell als Projekt abgeschlossen. Die weitere Arbeit wird in einer ständigen Arbeitsgruppe, der sogenannten „KDM-Werkstatt", fortgeführt.

Die Erarbeitung eines fiktiven Praxisbeispiels zur Anwendung des Kirchlichen Datenschutzmodells in Bezug auf eine Bildungs- und Entwicklungsdokumentation eines Kindes in einer Kindertageseinrichtung wurde im Berichtszeitraum abgeschlossen und veröffentlicht.

Dieses und alle weiteren Dokumente und Informationen finden Sie auf der Internetseite zum KDM:

https://www.kirchliches-datenschutzmodell.de

[55] Ausführlich zum Projekt siehe Abschnitt 2.2 des Jahresberichts 2021

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

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

„Niemand darf gemaßregelt oder benachteiligt werden, weil er sich … an die Datenschutzaufsicht gewendet hat."
(§ 48 Abs. 3 KDG)

3.1 Der gemeinsame Diözesandatenschutzbeauftragte

Der Diözesandatenschutzbeauftragte und Leiter des Katholischen Datenschutzzentrums ist als Datenschutzaufsicht im Sinne des Art. 91 Abs. 2 DSGVO und der §§ 42 ff. KDG zuständig für die Erzdiözese Köln, die Erzdiözese Paderborn, die Diözese Aachen, die Diözese Essen und die Diözese Münster (nordrhein-westfälischer Teil). Hinzu kommen noch einzelne Gemeinden oder Teile von Gemeinden in Rheinland-Pfalz, die zur Erzdiözese Köln gehören, und von Niedersachsen und Hessen, die zur Erzdiözese Paderborn gehören. Im Zuständigkeitsgebiet leben fast 6,2 Millionen Menschen römisch-katholischen Glaubens (Stand 2022).

Seit dem 01.01.2018 ist der Diözesandatenschutzbeauftragte zusätzlich als Datenschutzaufsicht für den Verband der Diözesen Deutschlands[56] (Rechtsträger der Deutschen Bischofskonferenz) zuständig. Im VDD sind die 27 rechtlich und wirtschaftlich selbstständigen (Erz-) Diözesen zusammengeschlossen. Neben dem Sekretariat der Deutschen Bischofskonferenz in Bonn gehören damit unter anderem auch die Geschäftsstelle des VDD in Bonn, das Kommissariat der deutschen Bischöfe – Katholisches Büro in Berlin und weitere Einrichtungen des VDD zum Zuständigkeitsbereich des Katholischen Datenschutzzentrums.

Die Aufgaben des Diözesandatenschutzbeauftragten beziehungsweise des Verbandsdatenschutzbeauftragten des VDD als Datenschutzaufsicht sind im KDG beziehungsweise im KDG-VDD beschrieben.[57]

Der Diözesandatenschutzbeauftragte, seine Stellvertreterin und die Mitarbeiterinnen und Mitarbeiter bringen ihre Kenntnisse und Erfahrungen aus der Praxis der Datenschutzaufsichten auch in die Arbeit von kirchlichen Gremien und Arbeitsgruppen ein. Die Beratung der Gremien und Arbeitsgruppen ist Teil des gesetzlichen Auftrags der Datenschutzaufsichten.

[56] Die Datenschutzaufsicht heißt dort „Verbandsdatenschutzbeauftragter".
[57] Für eine ausführliche Darstellung der Aufgaben der Datenschutzaufsicht siehe Abschnitt 3.5 des Jahresberichts 2021.

3.2 Das Katholische Datenschutzzentrum

Das Katholische Datenschutzzentrum bildet als Körperschaft des öffentlichen Rechts den Rahmen für die Arbeit des Diözesandatenschutzbeauftragten und unterstützt diesen bei der Ausübung der Datenschutzaufsicht über die katholischen Einrichtungen in seinem Zuständigkeitsbereich.

Das Katholische Datenschutzzentrum in Dortmund ist als Umsetzung der Rechtsprechung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsichtsbehörden als eigenständige und unabhängige Körperschaft des öffentlichen Rechts gegründet worden.[58] Der Diözesandatenschutzbeauftragte ist zugleich Leiter dieser Körperschaft und vertritt diese nach außen. Das für die Erfüllung der Aufgabe der Datenschutzaufsicht notwendige Personal ist bei dem Katholischen Datenschutzzentrum als Körperschaft direkt angestellt. Mit dieser organisatorischen Trennung und der im Gesetz über den Kirchlichen Datenschutz festgeschriebenen Unabhängigkeit der Funktion des Diözesandatenschutzbeauftragten soll sichergestellt werden, dass die Datenschutzaufsicht die gesetzlich vorgesehene Kontrollfunktion auch unbeeinflusst wahrnehmen kann.[59]

Abb. 17: Das Katholische Datenschutzzentrum hat seinen Sitz in der Kommende Dortmund, dem Standort des Sozialinstituts der Erzdiözese Paderborn.
(Bild: Sozialinstitut Kommende Dortmund)

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

[58] Siehe hierzu auch Marcus Baumann-Gretza, Zur Entstehungsgeschichte und Struktur des Katholischen Datenschutzzentrums in Dortmund, in: Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung (Band 2 der Schriften zum kirchlichen Datenschutz des KDSZ), Dortmund 2021, S. 81–90.

[59] Siehe hierzu auch Burkhard Kämper / Jan Gers, Handlungsbedarf für die katholische Kirche durch das Urteil des EuGH von 2010 zur Unabhängigkeit der Datenschutzaufsichten in Deutschland, in: Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung (Band 2 der Schriften zum kirchlichen Datenschutz des KDSZ), Dortmund 2021, S. 69–80.

Das Katholische Datenschutzzentrum wird von den fünf (Erz-)Diözesen als Mitgliedern der Körperschaft des öffentlichen Rechts getragen. Wie in § 43 Abs. 4 KDG beschrieben, stellen sie die für die Erfüllung der Aufgaben des Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung. Außerdem verfügt der DDSB über einen eigenen jährlichen Haushalt.

Für das Kalenderjahr 2023 sieht der Haushaltsplan für das Katholische Datenschutzzentrum ein Volumen in Höhe von 1.364.000 Euro zur Deckung der notwendigen Personal- und Sachausgaben vor. Für das Folgejahr 2024 sinkt das genehmigte Budget auf 1.264.000 Euro.

3.3 Der hl. Ivo – Schutzpatron des Katholischen Datenschutzzentrums

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

Der hl. Ivo lebte im 13. Jahrhundert in der Bretagne. Der Bischof von Tréguier ernannte den Priester, der auch Rechtswissenschaften studiert hatte, zu seinem Offizial. Dieses kirchliche Richteramt füllte er mit Mut und Unbestechlichkeit aus und setzte sich vor allem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein, was ihm den Ruf eines „Anwalts der Armen“ einbrachte. Sein Gedenktag ist der 19. Mai.[60]

Das Bildnis des hl. Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums, sodass der Schutzpatron in der täglichen Arbeit immer gegenwärtig ist.

Abb. 18: Darstellung des Siegels des KDSZ im Amtsblatt der Erzdiözese Paderborn (Bild: Katholisches Datenschutzzentrum)

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

3.4 Öffentlichkeitsarbeit

Das Katholische Datenschutzzentrum macht auf vielfältige Weise auf den Datenschutz in der katholischen Kirche und seine Arbeit aufmerksam und informiert die kirchlichen Einrichtungen, die betroffenen Personen und die interessierte Öffentlichkeit über den Datenschutz in der katholischen Kirche.

Über die Internetpräsenz ***www.katholisches-datenschutzzentrum.de*** stellt das Katholische Datenschutzzentrum vielfältige Informationen rund um den kirchlichen Datenschutz und die Arbeit der Datenschutzaufsicht zur Verfügung. Diese Informationen sind als Internetseiten online verfügbar oder stehen dort zum Download bereit. Hierbei reicht das Spektrum von einschlägigen Gesetzestexten für die jeweilige (Erz-) Diözese über Hilfestellungen bis hin zu Mustern und Vorlagen.

Das Katholische Datenschutzzentrum ist mit einem eigenen „besonderen elektronischen Behördenpostfach (beBPo)" an den elektronischen Rechtsverkehr angebunden.

Neben den Auskünften auf der Internetseite stellt das Katholische Datenschutzzentrum auch weitergehende Informationen in Form von Informationsblättern, Broschüren, Arbeitshilfen, Mustern oder Checklisten bereit. In diesen Publikationen behandelt das Katholische Datenschutzzentrum grundsätzliche oder aktuelle Themen, auf die es entweder selbst aufmerksam oder durch vermehrte Anfragen zu einem Thema ein erhöhter Informationsbedarf deutlich wird. Das Angebot an Informationen wird stetig ausgebaut.

3.5 Antragsverfahren vor dem Interdiözesanen Datenschutzgericht

Im Berichtszeitraum sind neun Verfahren vor der 1. Instanz (Interdiözesanes Datenschutzgericht, IDSG) und ein Verfahren vor der 2. Instanz (Datenschutzgericht der Deutschen Bischofskonferenz, DSG-DBK) aus dem Jahr 2023 anhängig, bei denen das Katholische Datenschutzzentrum als Antragsgegner oder Beteiligter geführt wird. Ein Verfahren der 1. Instanz wurde im Berichtsjahr abgeschlossen, die restlichen Verfahren laufen noch. Auch die Verfahren aus dem Jahr 2022 sind teilweise noch nicht entschieden.[61]

Inhaltlich betreffen die Verfahren wieder fast ausschließlich Beschwerdeverfahren, welche durch das KDSZ gemäß § 48 KDG bearbeitet wurden. Ein Betroffener hatte sich demnach mit einer datenschutzrechtlichen Eingabe an das Katholische Datenschutzzentrum gewandt und anschließend gegen dessen Bescheid gerichtlichen Rechtsbehelf eingelegt.

[61] Siehe Abschnitt 3.5 im Jahresbericht 2022.

Hinweis für kirchliche Einrichtungen

Die Entscheidungen der 1. und 2. Instanz werden regelmäßig auf der Internetseite der Deutschen Bischofskonferenz veröffentlicht.[62] Die Verfahren vor den kirchlichen Gerichten in Datenschutzangelegenheiten richten sich nach der Kirchlichen Datenschutzgerichtsordnung (KDSGO)[63].

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

Unter dem Vorsitz[64] von Schleswig-Holstein fanden im Jahr 2023 weitere Schritte zur Intensivierung der Zusammenarbeit mit der Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder statt. Eine gute Kooperation wird von allen Beteiligten als wertvoll erachtet.

Unter anderem wurde die Zusammenarbeit mit den kirchlichen Aufsichten (katholisch/evangelisch) durch die Teilnahme von Vertretern der kirchlichen Aufsichten an weiteren Arbeitskreisen der Datenschutzkonferenz[65] intensiviert. Die detaillierte Vorarbeit für Beschlüsse oder Entschließungen der DSK wird auf Ebene der Arbeitskreise erbracht, sodass schon vor einer Veröffentlichung Informationen weitergegeben und die spezifischen Aufsichten an Denkprozessen beteiligt werden.

Zweimal im Jahr findet der „Austausch zwischen Mitgliedern der DSK und spezifischen Datenschutzaufsichtsbehörden" in Präsenz oder als Videokonferenz statt.[66] Im Berichtszeitraum wurde auf einem der Treffen zur Verbesserung der Kooperation ein Adressverteiler der spezifischen Aufsichtsbehörden ins Leben gerufen und gemeinsam konzipiert. Der Adressverteiler stellt nicht nur für die interne Arbeit der Datenschutzaufsichten, sondern auch für die Öffentlichkeit eine große Hilfe dar und ist mittlerweile auf der neugestalteten Internetseite des BfDI veröffentlicht worden.[67] Die Zentrale Anlaufstelle (ZASt)[68] übernimmt die Pflege der Kontaktliste.

Auch unabhängig von geplanten Treffen findet ein reger Austausch untereinander statt. Das Katholische Datenschutzzentrum begrüßt die engere Zusammenarbeit unter den Datenschutzaufsichten und betont, wie positiv diese Zusammenarbeit von allen Seiten empfunden wird.

---

62 https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen und https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/entscheidungen

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

64 https://www.datenschutzkonferenz-online.de/vorsitz.html

65 https://www.datenschutzkonferenz-online.de/ak.html

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

67 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/Adressverteiler-extern-Kirchen.html?nn=302362

68 https://www.bfdi.bund.de/DE/Fachthemen/ZASt/ZASt-node.html

4 Dokumentation

4.1 Die Datenschutzaufsicht in der katholischen Kirche

Die Datenschutzaufsicht für die (Erz-)Diözesen in der katholischen Kirche in Deutschland wird von fünf überdiözesanen Stellen wahrgenommen. Diese fünf Diözesandatenschutzbeauftragten sind jeweils für mehrere (Erz-)Diözesen bestellt. Die Verteilung ist in der nachfolgenden Übersicht dargestellt:

Abb. 19: Struktur der Datenschutzaufsichten der (Erz-)Diözesen in Deutschland

Daneben gibt es noch eine eigene Datenschutzaufsicht für die katholische Militärseelsorge, die in Personalunion vom Diözesandatenschutzbeauftragten für die ostdeutschen (Erz-)Diözesen wahrgenommen wird. Außerdem besteht eine eigenständige Datenschutzaufsicht für den Verband der Diözesen Deutschlands und die nachgeordneten Einrichtungen. Diese Aufsichtsfunktion wird in Personalunion vom Diözesandatenschutzbeauftragten für die nordrhein-westfälischen (Erz-) Diözesen wahrgenommen[69].

Für den Bereich der Ordensgemeinschaften päpstlichen Rechts hat die Deutsche Ordensobernkonferenz, der Zusammenschluss der Höheren Oberen der Orden und Kongregationen in Deutschland, die Einrichtung der Gemeinsamen Ordensdatenschutzbeauftragten der DOK als Datenschutzaufsicht geschaffen.[70]

Zu den Aufgaben der Diözesandatenschutzbeauftragten gehört gemäß §§ 44 Abs. 3 lit. f) und 46 KDG das Hinwirken auf die Zusammenarbeit mit den anderen Diözesandatenschutzbeauftragten. Um eine möglichst einheitliche Praxis bei der Auslegung des Gesetzes und bezogen auf Verfahrensabläufe der kirchlichen Stellen zu erreichen, tauschen sich

[69] Siehe Abschnitt 3.1 des Jahresberichts.
[70] Siehe https://datenschutz.orden.de/.

die Diözesandatenschutzbeauftragten regelmäßig als Konferenz der Diözesandatenschutzbeauftragten aus. Zu den Konferenzen werden auch die Ordensdatenschutzbeauftragten der DOK eingeladen.[71]

Hinweis für kirchliche Einrichtungen

Die Konferenz der Diözesandatenschutzbeauftragten hat zur leichteren Erreichbarkeit eine „Geschäftsstelle" eingerichtet. Diese befindet sich beim Katholischen Datenschutzzentrum in Dortmund.

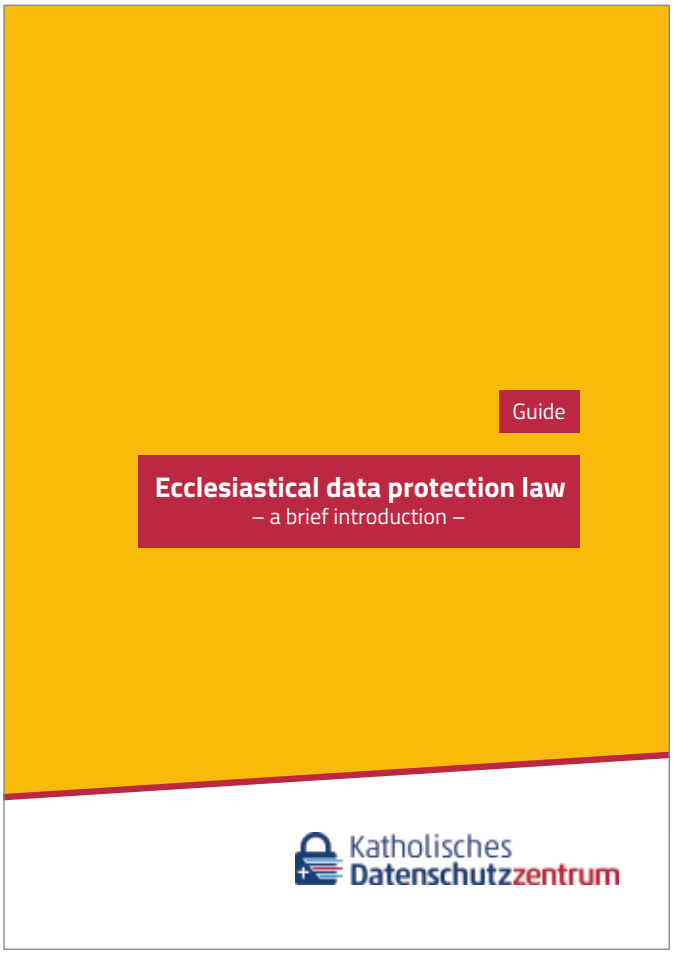
[71] Ausführlich zur Konferenz der Diözesandatenschutzbeauftragten siehe Abschnitt 4.1.3 im Jahresbericht 2021.

4.2 Veröffentlichungen des Katholischen Datenschutzzentrums – Auszug –

Auch im Jahr 2023 hat das Katholische Datenschutzzentrum für die kirchlichen Einrichtungen wieder praktische Hilfestellungen zur Auslegung und Umsetzung datenschutzrechtlicher Vorgaben veröffentlicht.

Kurzinformation zum kirchlichen Datenschutz in englischer Sprache

Das Katholische Datenschutzzentrum hat Informationen zum kirchlichen Datenschutz in einer Broschüre in englischer Sprache zusammengestellt. Damit kommt das Katholische Datenschutzzentrum Bitten aus dem kirchlichen Bereich nach, Grundinformationen zum kirchlichen Datenschutz auch in englischer Sprache bereit zu halten.[72]



[72] Die Veröffentlichung kann hier abgerufen werden: https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2023/03/Guide-ecclesiastical-data-protection-law.pdf

Ecclesiastical data protection law

This guide aims to provide an insight into the implementation of ecclasiastical data protection in the archdioceses and dioceses of the Catholic Church in Germany. The Church can rely on its own ecclasiastical data protection Law. This Law and the own ecclasiastical data protection supervisory authority are made possible by the regulations of Art. 91 GDPR.

Editors: Steffen Pau
Marcel Pfefferkuch

Publisher:

Der Verbandsdatenschutzbeauftragte des Verbandes der Diözesen Deutschlands (VDD)
Steffen Pau

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231/13 89 85 – 0
Fax 0231/13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de

Revision 1.0/February 2023

Ecclesiastical data protection law*

The European General Data Protection Regulation (GDPR) provides for exceptions to its applicability for two constitutionally protected areas – the media, churches or religious communities. Article 85 of the GDPR allows member states to provide for derogations in the areas of freedom of expression and freedom of information for the processing of personal data for journalistic and other privileged purposes mentioned therein. Member States may also provide for separate supervisory structures in these areas. The second area specifically regulated in the GDPR are the data protection regulations of churches and religious communities in Art. 91 GDPR.[1]

Constitutional and primary law foundations

The Grundgesetz (German Basic Law, or short GG[2]) protects freedom of religion in Article 4 GG. The content of this fundamental right has also found its way into the Charter of Fundamental Rights of the European Union (CFR) in Art. 10 (1) CFR.

The protection of religious freedom from Article 4 GG is complemented by Article 140 GG, which transfers the provisions of the regulations of Articles 136 to 139 and 141 of the Weimarer Reichsverfassung (German Constitution of 11 August 1919 – Weimar Constitution, or short WRV) into the Basic Law. This implements public entity status for some religious communities and enshrines a constitutional guarantee of freedom of religion

* This text is a revised and supplemented English version of the article in the journal Datenschutznachrichten (DANA), issue 3/2022, page 158 et seqq. (published by the Deutsche Vereinigung für Datenschutz e. V.).

1 This article looks at the data protection laws enacted by the (arch)dioceses in Germany on the basis of the model draft of the Kirchlichen Datenschutzgesetz (Ecclasiastical Data Protection Act, or short KDG) as amended by the unanimous resolution of the plenary assembly of the Association of German Dioceses of 20 November 2017. This consideration is complemented by references to the Ecclesiastical Data Protection Act of the Protestant Church in Germany (EKD Data Protection Act – DSG-EKD) of 15 November 2017. Data protection regulations of other churches or religious communities in Germany or in other European countries are not considered in this article. References to other ecclesiastical data protection laws (without claiming to be complete) are collected, for example, by *Felix Neumann* in his blog: https://artikel91.eu/rechtssammlung/.

2 The Grundgesetz is the constitutional law in Germany.

in the Basic Law,[3] which, among other things, enables religious communities to organise and administer their affairs independently within the limits of the laws applicable to all (Art. 140 GG in conjunction with Art. 137 (3) WRV).

The General Data Protection Regulation (GDPR) takes up this legal framework on the basis of Art. 17 of the Treaty on the Functioning of the European Union (TFEU) and implements it in Art. 91 GDPR. Article 91 of the GDPR enables the churches to continue to apply their own existing data protection regulations, provided that these are brought into line with the provisions of the GDPR. Likewise, Art. 91 GDPR opens up the possibility of installing their own data protection supervisory authority, which must fulfil the requirements of Chapter VI of the GDPR. Thus, this regulation respects the individual's right to the protection of personal data and the status of religious societies under Art. 140 GG in conjunction with. Art. 137 (3) WRV, equally (corporate religious freedom).[4]

Through the provision of Art. 91 of the GDPR, the European legislator makes it possible for the Church to continue to maintain its leeway under german state-church law despite the central European legal requirement. In this way, the European legislator complies with the requirements laid down in Art. 17 TFEU. According to this provision, the European Union shall respect and not prejudice the status of churches, religious associations or communities under national law in the Member States (Art. 17 (1) TFEU). The provision takes the fact into account, that European law has an increasingly strong impact on churches and can affect them particularly in their „proprium".[5]

Art. 91 GDPR thus provides both the legal framework for the current Kirchliches Datenschutzgesetz (Ecclesiastical Data Protection Act, or short KDG) and for the establishment of the Catholic Church's own data protection supervisory authorities.

[3] See also *Hense*, Art. 91 of the General Data Protection Regulation and the Church's Right to Self-Determination, in Pau (ed.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, p. 35 et seqq. (available online in the Infothek at www.katholisches-datenschutzzentrum.de).

[4] *Hense* in Sydow, Europäische Datenschutzgrundverordnung, 2nd ed. 2018, Art. 91, marginal no. 1 with further explanations.

[5] Cf. *Streinz* in Streinz, EUV/AEUV, 3rd ed. 2018, Art. 17 TFEU, para. 7 et seq. and 12.

Article 91 GDPR as the starting point of today's ecclesiastical data protection

Art. 91 (1) GDPR provides that a church or a religious association or community which applies comprehensive rules in a Member State for the protection of individuals with regard to the processing of their data at the time of the entry into force of the GDPR may continue to apply those rules, provided that those rules are brought in line with the GDPR.

These conditions are fulfilled by the data protection regulations of the Catholic Church in Germany.[6]

The German (arch)dioceses had already created their own ecclesiastical data protection laws at the end of the 1970s with the Anordnung über den kirchlichen Datenschutz (Directive about the ecclesiastical data protection, or short KDO).[7] As a result, they can look back on a comparably long application of data protection regulations, equal to the legislator of the Federal Data Protection Act.

The data protection laws of both the Catholic Church and the Protestant Church in Germany (EKD) have been repeatedly adapted in response to the developments of the Federal Data Protection Act over the years. Therefore, the Catholic Church and the EKD were able to draw on comprehensive data protection regulations when the GDPR came into force in May 2016.[8]

[6] This also applies to the regulations of the Protestant Church in Germany (EKD) on data protection.

[7] On the development of ecclesiastical data protection law, cf. *Pau*, Kirchlicher Datenschutz von den Anfängen bis zum KDG, in Pau (ed.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, p. 51 et seqq. (available online in the Infothek at www.katholisches-datenschutzzentrum.de). The data protection law of the EKD has taken a comparable development.

[8] *Hense* in Sydow, Europäische Datenschutzgrundverordnung, 2nd ed. 2018, Art. 91, marginal no. 19; *Jacob* in Auernhammer, DSGVO BDSG, 7th ed. 2020, Art. 91, marginal no. 12.

Before May 2018, both the Catholic Church and the Protestant Church recognized the need to adapt their own existing data protection regulations, so that the requirement of Article 91 (1) of the GDPR, which necessitates that the regulations must be brought into line with the GDPR, was also met.[9]

The Ecclesiastical Data Protection Act (KDG)

In the Catholic Church, the legislative power for ecclesiastical laws lies with the individual (arch)bishops for their respective (arch)dioceses.[10] For regulations that are applied to the Church internationally, legislative power lies with the Holy See in Rome.

The Ecclesiastical Data Protection Act (KDG) was therefore enacted as a law by the 27 diocesan bishops for their respective (arch)diocese and published in the corresponding official church journal. This was done on the basis of a model version drawn up by the Association of German Dioceses – the legal body of the German Bishops' Conference – in order to achieve uniform implementation of the data protection regulations.[11] In addition to the KDG, an ordinance regulating the implementation of the KDG (KDG-DVO) was also issued by the individual (arch)dioceses, which contains specific explanations for the provisions of the KDG.[12]

A look at the table of contents of the KDG (as well as the DSG-EKD) shows that the law is somewhat shorter than the GDPR. The ecclesiastical legislator has not adopted the parts of the GDPR that were not relevant to its area of regulation. For example, the chapter on the European Data Protection Board and the cooperation of data protection supervisory authorities at the European level is missing, as this was not to be regulated by the church legislator – not even in the sense of bringing the regulation in line with the GDPR.

[9] *Herbst* in Kühling/Buchner, DS-GVO BDSG, 3rd ed. 2020, Art. 91, marginal no. 15a; *Jacob* in Auernhammer, DSGVO BDSG, 7th ed. 2020, Art. 91 marginal no. 13.

[10] Some special features – e.g. for religious congregations under papal law – will not be discussed in detail here.

[11] The model version can be downloaded as part of Working Aid No. 320 on the website https://www.dbk.de/themen/kirche-staat-und-recht/datenschutz-faq of the German Bishops' Conference.

[12] The sample text of the KDG-DVO is also included in the German Bishops' Conference's working aid no. 320 (see fn. 11).

A second look at the ecclesiastical law shows that the structure of the law is similar to the GDPR and that many provisions have been adopted from the GDPR with identical content. This is where the advantages of the consistency of the Church's regulations with the GDPR become apparent for the legal user. The legal user finds many familiar regulations and can, therefore, also use the commentary literature on the GDPR in many places.[13] A look at the law also reveals that the ecclesiastical legislator has also taken the implementation of the European provisions of the GDPR which were adapted in national data protection law, namely the new version of the Federal Data Protection Act, into account. Therefore, fragments of regulations of the new Federal Data Protection Act can also be found in the ecclesiastical law.

However, since Art. 91 of the GDPR doesn't require a complete adoption of the GDPR, there are also differences to the GDPR which were inserted due to specific church peculiarities.

There are provisions where the reason for the church-specific regulation is immediately obvious, such as the regulation in § 2 (3) KDG, which reminds us that the preservation of the secrecy of confession and pastoral care and other duties of confidentiality mentioned there remain unaffected, or § 14 KDG-DVO, which additionally regulates the handling of personal data that are subject to the secrecy of confession or pastoral care. The definition of „special categories of personal data" in § 4 no. 2 KDG also shows a difference. Membership of a church or religious community does not fall into the group of special categories of personal data in the Ecclesiastical Data Protection Act (cf. § 4 no. 2 sentence 2 KDG), as this is a datum that inevitably arises in many processing operations of personal data in the ecclesiastical sphere (e.g. entry into the baptismal register).

In the case of other regulations, the special ecclesiastical feature that necessitates a deviation from the wording of the GDPR may not always be immediately apparent. In some cases, the content of the regulations was taken over from the preceding law, the Anordnung über den kirchlichen Datenschutz (KDO), or an attempt was made – within the bounds of Art. 91 GDPR – to emphasize ecclesiastical features or to make linguistic adjustments.

[13] There is also a separate commentary for the KDG: Sydow, Kirchliches Datenschutzrecht, Baden-Baden 2021. A commentary on the DSG-EKD is in preparation.

The KDG, with its written form requirement in § 8 (2) KDG, appears stricter than the GDPR, which stipulates in Art. 7 (1) GDPR that the controller must be able to prove consent. It is questionable, to which extent this provides for major differences in the day to day handling of consent. On one hand, § 8 (2) KDG itself provides for „another form" of consent due to special circumstances. On the other hand, the obligation to provide proof in Art. 7 (1) GDPR also leads to a textual or written version of consent in many cases.

Scope of application of the KDG

Section 3 of the KDG includes all ecclesiastical bodies in the scope of the KDG, regardless of whether they are public institutions (e.g. dioceses or parishes) or Caritas institutions. Other bodies of the Church, foundations, establishments, workshops, institutions and other church legal entities regardless of their legal form are also included in the scope of application. This makes it clear that all ecclesiastical institutions, not only the ecclesiastical „core area" of the constitutionally guaranteed church, fall within the scope of the KDG. Therefore, ecclesiastical hospitals, ecclesiastical care facilities, ecclesiastical schools or ecclesiastical day-care centres are also among the institutions that apply the KDG.

Data protection officers

For the area of the constitutional church (i.e. the (arch)dioceses and the parishes or their associations at the middle administrative level), the KDG requires the appointment of data protection officers (cf. § 36 (1) KDG). The other ecclesiastical bodies must appoint one pursuant to § 36 (2) KDG if either at least ten persons[14] are permanently engaged in the processing of personal data, or the core activity of the controller consists in the performance of processing operations which require extensive regular and systematic monitoring of the data subjects, or the core activity consists in the extensive processing of special categories of personal data, or of data relating to criminal convictions and offences pursuant to § 12 KDG.

[14] The ecclesiastical legislator has not yet implemented the amendment to § 38 (1) BDSG which raises the threshold for the mandatory appointment of a company data protection officer to 20 persons. It is not yet known whether this will be considered as part of the current evaluation of the church law.

The company data protection officers support the management of the institutions in fulfilling their duties to adhere with data protection regulations and work towards their compliance. In order for the data protection officers to be able to fulfil their duties, they must be integrated into the operational processes and information flows. The data protection officer shall enjoy protection against dismissal in accordance with § 37 (4) KDG, unless extraordinary dismissal is considered.

Data subject rights

The KDG regulates the rights of data subjects to obtain information about their own data in more detail than before. The right to information in § 17 KDG enables the person to obtain detailed information about the data processed about him or her. The right to information is complemented by the right to rectification of the data stored about one's person by the data controller, § 18 KDG.

The data subject can assert his or her right to have data deleted in accordance with § 19 KDG. However, the conditions and exceptions to this right must be observed. The right to data portability under § 22 KDG is intended to ensure that a data subject has the possibility to transfer his or her data, which he or she has provided to the controller, to another controller. To also bear in mind is the right of the data subject to object to the processing of his or her data under certain conditions, § 23 KDG.

The rights of the data subject are further complemented by the obligation of the data controller to inform the data subject of the contents set out in §§ 15 and 16 KDG at the time of collection of personal data.

Ecclesiastical data protection supervisory authorities

Due to the comprehensive data protection regulations of the KDG and the DSG-EKD in accordance with Art. 91 (1) DSGVO, both churches also have the possibility to establish their own ecclesiastical data protection supervisory authorities in accordance with Art. 91 (2) GDPR. On the Catholic side, the Diocesan Data Protection Commissioners have been appointed in the individual (arch)dioceses as heads of the data protection supervisory authorities (§§ 42 KDG et seqq.). Several (arch)dioceses have made use of

the possibility to appoint a joint diocesan data protection commissioner as data protection supervisory authority for their respective (arch)dioceses. For example, the (arch)dioceses of North Rhine-Westphalia have appointed a joint data protection commissioner who is the head of the Catholic Data Protection Centre, which was created as a public institution.[15]

Just as ecclesiastical data protection law precedes over the GDPR under the conditions of Art. 91 (1) GDPR, the ecclesiastical data protection commissioners take the place of the state data protection commissioners for the ecclesiastical institutions subject to ecclesiastical data protection under the conditions of Art. 91 (2) GDPR. In doing so, they perform – just like the state data protection commissioners – the broad range of tasks of a data protection supervisory authority. Since all German (arch)dioceses have taken advantage of the opportunity to install their own data protection supervisory authorities, the diocesan data protection commissioners are the responsible authorities when it comes to data protection complaints against ecclesiastical institutions, for example.

In order to achieve the most uniform possible interpretation of the ecclesiastical regulations on data protection by the ecclesiastical supervisory authorities, the diocesan data protection commissioners agree on central issues, pass joint resolutions, and formulate common positions in the Conference of Diocesan Data Protection Commissioners.[16] In addition, there is a close exchange with the data protection supervisory authorities of the Protestant Church and the state data protection supervisory authorities.

[15] The 27 (arch)dioceses have appointed five joint data protection commissioners with offices in Bremen, Schönebeck, Dortmund, Frankfurt am Main and Munich. In addition, there is a joint data protection supervisory authority for the religious congregations under papal law in Germany. The EKD has established a data protection supervisory authority in the form of the Commissioner for Data Protection with its headquarters in Hanover and four branch offices, which the vast majority of the regional churches and diaconal organisations have joined.

[16] The resolutions are available on the websites of the ecclesiastical data protection supervisory authorities, e.g. at www.katholisches-datenschutzzentrum.de under the heading Infothek.

Ecclesiastical data protection courts

The GDPR provides that effective legal remedies must exist against decisions of the data protection supervisory authority as well as against the data controllers or processors directly (cf. Art. 78, 79 GDPR). This requirement has been transposed into church law in § 49 KDG and § 47 DSG-EKD.[17]

In the non-ecclesiastical area, the administrative courts are responsible for these legal remedies according to the GDPR. Within the scope of the DSG-EKD, these disputes are assigned to the ecclesiastical administrative courts of the EKD (cf. § 47 DSG-EKD).

Since there is no ecclesiastical administrative jurisdiction in the area of the German Bishops' Conference, the Conference has, parallel to the entry into force of the KDG, created an ecclesiastical court which is specifically assigned to handle the aforementioned disputes.

The Kirchliche Datenschutzgerichtsordnung (Ecclesiastical Data Protection Court Rules, or short KDSGO) regulate the establishment of ecclesiastical courts specifically for disputes arising from § 49 KDG. The KDSGO provides for an original and appellate court. The Interdiözesane Datenschutzgericht (Interdiocesan Data Protection Court, or short IDSG) has the original jurisdiction. An appeal against the decisions of the IDSG can then be made to the Datenschutzgericht der Deutschen Bischofskonferenz (Data Protection Court of the German Bishops' Conference, or short DSG-DBK).

[17] While § 47 DSG-EKD still requires a preliminary procedure, at least in part, the KDG does not require a preliminary procedure.

Professors, judges and other experts with many years of experience in data protection have been recruited as judges for both courts, ensuring a high quality of the courts' work. Decisions of the courts are partly published on the website of the German Bishops' Conference.[18]

Conclusion

The Catholic Church in Germany – just like the Protestant Church in Germany – has fulfilled the requirements of Art. 91 GDPR with the update of the Ecclesiastical Data Protection Act before 25 May 2018 and has established its own data protection supervisory authorities for this purpose, which fullfill the conditions laid down in Chapter VI of the GDPR. Judicial review is carried out by the data protection courts specifically established for this purpose at the level of the German Bishops' Conference.

[18] Further information on both courts, including the decisions, can be found at https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/. An initial look at the work of the court is contained in *Sydow*, Die Datenschutzgerichte der katholischen Kirche – erste Erfahrungen und Perspektiven, in Pau (ed.), Ein Jahr Gesetz über den Kirchlichen Datenschutz (KDG) – Rückblick und Ausblick, Katholisches Datenschutzzentrum, Dortmund 2020, p. 53 et seqq. (available online in the Infothek at www.katholisches-datenschutzzentrum.de). An overview of the first published decisions is contained in the article by *Joachimski/Melzow*, Die kirchliche Datenschutzgerichtsbarkeit, in Pau (ed.), Kirchlicher Datenschutz – gewachsener Baustein kirchlicher Selbstverwaltung, Katholisches Datenschutzzentrum, Dortmund 2021, p. 91 et seqq. (available online in the Infothek at www.katholisches-datenschutzzentrum.de).

Appendix

The ecclasiastical data protection supervisory authorities of the (arch)dioceses in Germany

Ecclesiastical Data Protection Act (KDG): Sources in official journals[19]

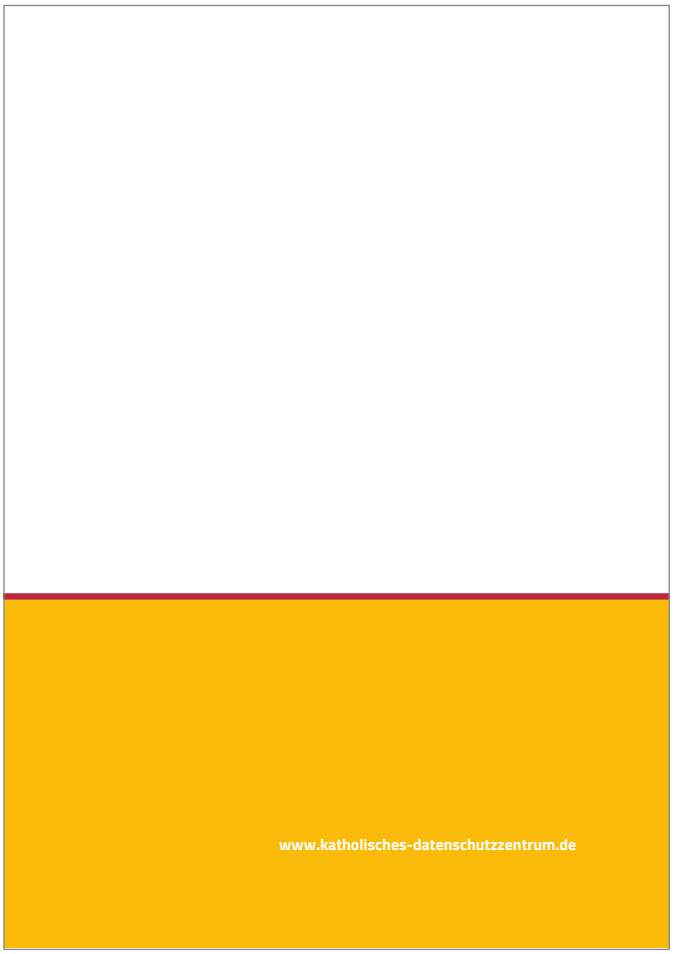
(Arch-)Diocese	Official Journal of	page
Aachen	1 March 2018	78
Augsburg	9 April 2018	378
Bamberg	15 March 2018	162
Berlin	1 March 2018	24
Dresden-Meißen	9 March 2018	103
Eichstätt	17 April 2018	193
Erfurt	20 March 2018	2
Essen	19 January 2018	33
Freiburg	23 March 2018	185
Fulda	8 May 2018	49
Görlitz	8 May 2018	1
Hamburg	23 January 2018	2
Hildesheim	23 April 2018	98
Köln	31 January 2018	13
Limburg	15 January 2018	295

[19] Content taken from Working Aid No. 320 of the German Bishops´ Conference; Appendix I pages 187–188 (https://www.dbk-shop.de/de/publikationen/arbeitshilfen/kirchliches-datenschutzrecht.html)

(Arch-)Diocese	Official Journal of	page
Magdeburg	1 February 2018	Appendix
Mainz	26 February 2018	21
München und Freising	30 April 2018	
Münster	1 February 2018	56
Offizialat Vechta	15 May 2018	166
Osnabrück	19 April 2018	100
Paderborn	6 February 2018	48
Passau	16 April 2018	99
Regensburg	30 January 2018[20]	17
Rottenburg-Stuttgart	5 March 2018	69
Speyer	22 March 2018	746
Trier	1 April 2018	118
Würzburg	28 March 2018	255
VDD Official Journal of München und Freising	31 May 2018	434

The KDG was put into force in all (arch)dioceses on 24.05.2018.

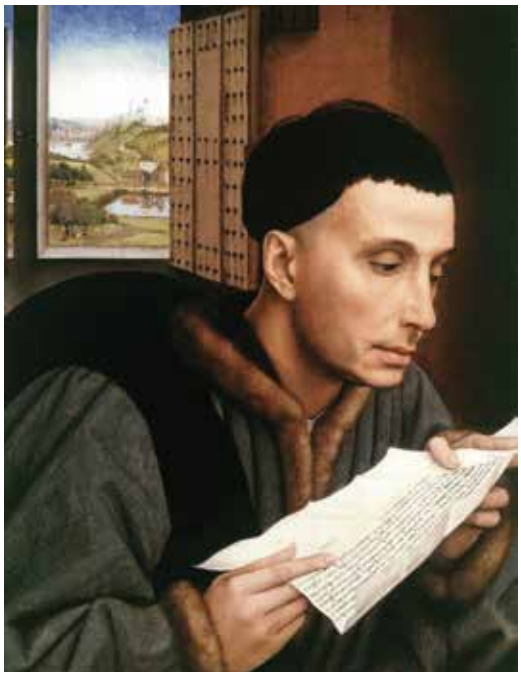
[20] Supplemented by the official journal of 10 May 2019, p. 58 and entered into fore 1 July 2019.


www.katholisches-datenschutzzentrum.de

Abkürzungsverzeichnis

BÄK	Bundesärztekammer
beBPo	besonderes elektronisches Behördenpostfach
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer; Arbeitsgemeinschaft der deutschen Zahnärztekammern e. V.
DAV	Deutscher Apothekerverband e. V.
DDSB	Diözesandatenschutzbeauftragte/r
DKG	Deutsche Krankenhausgesellschaft e. V.
DOK	Deutsche Ordensobernkonferenz
DSG-DBK	Datenschutzgericht der Deutschen Bischofskonferenz – 2. Instanz
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichten des Bundes und der Länder
EDSA	Europäischer Datenschutzausschuss
EKD	Evangelische Kirche in Deutschland
ePA	elektronische Patientenakte
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
GKV-SV	Spitzenverband der Gesetzlichen Krankenversicherungen
HinSchG	Hinweisgeberschutzgesetz
IDSG	Interdiözesanes Datenschutzgericht – 1. Instanz
IfSG	Infektionsschutzgesetz
ISO	Internationale Organisation für Normung
KBV	Kassenärztliche Bundesvereinigung
KDG	Gesetz über den Kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum KDG
KDG-VDD	KDG für den Verband der Diözesen Deutschlands
KDM	Kirchliches Datenschutzmodell

KDSGO	Kirchliche Datenschutzgerichtsordnung
KDSZ	Katholisches Datenschutzzentrum
KZBV	Kassenzahnärztliche Bundesvereinigung
NYOB	none of your business (Nichtregierungsorganisation, Europäisches Zentrum für digitale Rechte)
PKV	Verband der Privaten Krankenversicherung e.V.
TLS	Transportschichtsicherheit (Transport Layer Security)
UBSKM	Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs
USA	Vereinigte Staaten von Amerika (United States of America)
VDD	Verband der Diözesen Deutschlands
ZASt	Zentrale Anlaufstelle



Hl. Ivo

Der heilige Ivo ist der Schutzpatron des Katholischen Datenschutzzentrums.
Er lebte im 13. Jahrhundert im heutigen Frankreich und setzte sich dort unter anderem für Arme und Bedrängte vor weltlichen und kirchlichen Gerichten ein.
Das Bildnis des heiligen Ivo ziert auch das Siegel des Katholischen Datenschutzzentrums. Sein Gedenktag ist der 19. Mai.

Bild: Joachim Schäfer – www.heiligenlexikon.de

Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund

Tel.: 0231/13 89 85 – 0
Fax: 0231/13 89 85 – 22
E-Mail: info@kdsz.de
www.katholisches-datenschutzzentrum.de