



**Kath. Datenschutzzentrum
Frankfurt/M.**

Tätigkeitsbericht 2023

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

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

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen an einigen Stellen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beiderlei Geschlecht.
Bildnachweise: Titel und Rückseite, S.8+9: luftbildagentur euroluftbild.de, S. 8+9: privat, S. 13: LALAKA Adobestock, S. 14: Wei / Adobestock, S. 25+36: Knut / Adobestock, S. 32: Ocskay Mark / Adobestock, S. 38: Olaf J. Lutz, KDSZ Ffm

Inhaltsverzeichnis	3
Vorwort	5
1 Aus der Datenschutzaufsicht	7
1.1 Kontinuität: Zweite Amtszeit für die Diözesandatenschutzbeauftragte Ursula Becker-Rathmair	7
1.2 Wandel: Neuer Standort für das Kath. Datenschutzzentrum Frankfurt/M.	7
2 Entwicklung des Datenschutzes	10
2.1 Staatliche Gesetzgebung	10
2.1.1 Hinweisgeberschutzgesetz	10
2.1.2 Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework	11
2.1.3 Digital Services Act (EU-Verordnung)	13
2.2 Kirchliche Gesetzgebung	14
2.2.1 Erzbistum Freiburg richtet interne Meldestelle nach Hinweisgeberschutzgesetz bei Rechnungshof ein	14
2.2.2 Neues Beschwerdemanagement im Bistum Limburg	15
2.2.3 Bistum Fulda veröffentlicht Datenschutzinfos zu neuem Hinweisgeberschutzgesetz	16
2.2.4 Verpflichtung auf Datengeheimnis – neue Mustertexte und Merkblätter im Bistum Fulda / Vorgehen bei Mitarbeiterexzess	16
2.2.5 Bistum Fulda bündelt Datenschutz im Gesetz zur Regelung von Einsichts- und Auskunftsrechten der Aufarbeitungskommission	18
2.2.6 Bistum Fulda hat jetzt auch ein § 29-KDG-Gesetz	19
2.2.7 Freiburg und Trier erlassen Ordnungen zu Einsichts- und Auskunftsrechten in Sachakten	19
2.3 Ausgewählte Rechtsprechung staatlicher Gerichte	20
2.3.1 Konkrete Empfänger zu benennen	20
2.3.2 Datenverarbeitung im Beschäftigungskontext	21
2.3.3 Kopie als Teil des Auskunftsanspruchs	21
2.3.4 Interne sind keine Empfänger	22
2.3.5 Auskunftsanspruch braucht keine Begründung	23
2.3.6 Exzessive Auskunftserteilung?	25
2.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte	26
2.4.1 Zweckwidriges Zitieren aus einer Personalakte	26
2.4.2 Verarbeitung sensibler Daten zum Schutz lebenswichtiger Interessen	27
2.4.3 Gerichtliche Kassationsbefugnis – deutliche Kritik an KDSGO	28

3	Schwerpunkte der Tätigkeiten im Berichtszeitraum	30
3.1	Datenschutzverletzungen	30
3.1.1	Private Handynummer auf Abwegen	31
3.1.2	Videoüberwachung? – Hier bestimmt nicht!	31
3.1.3	Hinter den Kulissen einer fachgerechten Abfallentsorgung	32
3.1.4	XS, M oder XXL – wer trägt was?	32
3.2	Beschwerden	33
3.2.1	Nachwirkungen von Corona	33
3.2.2	Auch ohne Einwilligung kann die Weitergabe von Gesundheitsdaten rechtmäßig sein	33
3.2.3	Erzieherin ist im Krankenstand auf unbestimmte Zeit – sollten das alle Eltern erfahren?	34
3.2.4	Unschärfe Trennung von Arbeit und Privatem	34
3.3	Anfragen	35
3.4	Gerichtsverfahren	35
3.5	Prüfungen	36
4	Veranstaltungen und Öffentlichkeitsarbeit	37
5	Vernetzung mit anderen Datenschutzaufsichten	38
6	Hinweise des Kath. Datenschutzzentrums Frankfurt/M.	40
6.1	5 Jahre KDG – ein Grund zum Feiern!	40
6.2	Neue Grundlage für den Datentransfer mit den USA	41
7	Ausblick	42
8	Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland	43

2023 – ein Jahr mit Höhepunkten

Die im Tätigkeitsbericht für das Jahr 2022 angedeuteten Veränderungen hinsichtlich des Standorts des Kath. Datenschutzzentrums Frankfurt/M. haben sich ab Beginn des Jahres 2023 konkretisiert: Das Kath. Datenschutzzentrum Frankfurt/M. hat am Roßmarkt mitten im Herzen der Mainmetropole eine neue Bleibe gefunden.

Nach einer Renovierungsphase von circa fünf Monaten, in der durch die komplette Umgestaltung der Innenaufteilung der zu beziehenden Büroetage und den daraus resultierenden Umbauarbeiten quasi „kein Stein auf dem anderen blieb“, erfolgte im Mai 2023 der Umzug. Da nicht nur der Möbelaufbau gut funktionierte, sondern auch die Technik (fast) unmittelbar wieder einsetzbar war, konnten die Tätigkeiten des Kath. Datenschutzzentrums Frankfurt/M. glücklicherweise nahtlos fortgeführt werden.

Im neuen Domizil können nunmehr zum Teil auch eigene Veranstaltungen stattfinden, ohne dass wie früher regelmäßig auswärtige Örtlichkeiten in Anspruch genommen werden müssen. Der Umzug und die Inbetriebnahme der neuen Räumlichkeiten wurden im September 2023 angemessen gefeiert. Impressionen der Einsegnungsfeier, die nicht nur durch Redebeiträge ergänzt, sondern auch musikalisch von Mitarbeiterinnen und Mitarbeitern der Datenschutzaufsicht mitgestaltet wurde, finden sich im nachfolgenden Kapitel dieses Berichts.

Ebenfalls im Mai 2023 konnte „5 Jahre KDG / 5 Jahre EU-DSGVO“ gefeiert werden. Nachdem sich direkt nach Inkrafttreten der Datenschutzgesetze noch das ein oder andere zurechtrücken musste, haben sich die darin enthaltenen Grundsätze und Maßgaben mittlerweile etabliert und sie werden stetig weiterentwickelt.

Dieses Datum verdeutlicht also noch einmal, dass Datenschutz weder Selbstzweck noch ein überflüssiges bürokratisches Monster ist, sondern dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen dient und den Datentransfer personenbezogener Daten ermöglicht und regelt.

Das Jahr 2023 war zudem das Jahr, in dem „KI“ verstärkt Fahrt aufnahm. Beispielsweise wurden „Large Language Models“ (LLM), also selbstlernende Sprachmodelle, die Texte erzeugen können, durch die im März 2023 erschienene erweiterte Version des Chatbots „ChatGPT“ einer breiten Öffentlichkeit zugänglich. Innerhalb weniger Wochen fand „ChatGPT“ so über 100 Millionen Nutzerinnen und Nutzer.

Auch im kirchlichen Umfeld scheinen Künstliche Intelligenz und ihre Anwendungsmöglichkeiten angekommen zu sein. Die ersten Anfragen in diesem Kontext liegen dem Kath. Datenschutzzentrum Frankfurt/M. bereits seit einiger Zeit vor.

Die Entwicklungen in Bereich der „KI“ werden unbestritten (und vermutlich mit hoher Geschwindigkeit) voranschreiten und deren Auswirkungen auf die zunehmende Digitalisierung, die Gesellschaft und unsere Demokratie bleiben abzuwarten.

A handwritten signature in blue ink, reading "Becker-Rathmair". The signature is written in a cursive, flowing style.

Ursula Becker-Rathmair

Diözesandatenschutzbeauftragte und
Leiterin des Kath. Datenschutzzentrums Frankfurt/M.

1 Aus der Datenschutzaufsicht

1.1 Kontinuität: Zweite Amtszeit für die Diözesandatenschutzbeauftragte Ursula Becker-Rathmair

Am 31. Dezember 2022 ging die fünfjährige Amtszeit der Diözesandatenschutzbeauftragten Ursula Becker-Rathmair zu Ende. Auf Empfehlung des Verwaltungsrates des Katholischen Datenschutzzentrums Frankfurt/M. (KdöR) wurde Frau Becker-Rathmair durch die (Erz-)Bischöfe der sieben zum Katholischen Datenschutzzentrum Frankfurt/M. gehörenden (Erz-)Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier mit Wirkung zum 1. Januar 2023 für weitere fünf Jahre zur Diözesandatenschutzbeauftragten bestellt. Damit nimmt sie weiterhin die datenschutzrechtliche Aufsicht über die katholischen Einrichtungen im Zuständigkeitsgebiet wahr und die Leitung des Kath. Datenschutzzentrums Frankfurt/M. bleibt so unverändert in bewährter Hand.

1.2 Wandel: Neuer Standort für das Kath. Datenschutzzentrum Frankfurt/M.

Verändert hat sich dagegen im Jahr 2023 der Sitz des Kath. Datenschutzzentrums Frankfurt/M. Neue Räumlichkeiten wurden – wie bereits im Ausblick des letzten Tätigkeitsberichts angedeutet – am Ende des Jahres 2022 direkt im Herzen der Mainmetropole gefunden und im Mai 2023 bezogen. Fußläufig von den bislang im Haus am Dom genutzten Büroflächen entfernt, befindet sich die Datenschutzaufsicht der mittel- und südwestdeutschen (Erz-)Bistümer nun am Roßmarkt. Dieser mitten in der Stadt gelegene Platz ist von den neuen Arbeitsplätzen aus gut zu überblicken und das auf dem Platz befindliche Denkmal von Johannes Gutenberg ist nicht nur ein von Touristen häufig fotografisch festgehaltenes Motiv. Vielmehr zeigt es denjenigen, der durch seine Erfindung die manufakturmäßige Herstellung von Büchern und damit die Verbreitung von Daten ermöglichte, also einen neuen Zeitabschnitt der Medienentwicklung einleitete. Ein wichtiges – wenn nicht das wichtigste – Werk Gutenbergs ist und bleibt die Gutenberg-Bibel, die als eines der schönsten Erzeugnisse der Druckkunst gilt. Vor diesem Hintergrund ist die Wahl der neuen Räumlichkeiten des Kath. Datenschutzzentrums Frankfurt/M. nicht nur außerordentlich gelungen, was die Praktikabilität und die Erreichbarkeit der Arbeitsplätze für die Mitarbeiterinnen und Mitarbeiter betrifft, sondern sie scheint auch unter Berücksichtigung der Größe Frankfurts örtlich-thematisch eine Punktlandung zu sein.

Die neuen Räumlichkeiten wurden bezogen, die Arbeitsplätze eingerichtet und eine neue Kaffeemaschine angeschafft, sodass einer feierlichen Einsegnung der Räume des Kath. Datenschutzzentrums Frankfurt/M. im September 2023 nichts mehr im Wege stand. In Anwesenheit des Verwaltungsrats des Kath. Datenschutzzentrums Frankfurt/M., von Vertreterinnen und Vertretern der Bistümer aus dem Zuständigkeitsbereich, vieler weiterer Kolleginnen und Kollegen aus dem kirchlichen und dem staatlichen Datenschutz

sowie von Geschäftspartnern segnete Pfarrer Prof. Wolfgang Beck von der Philosophisch-Theologischen Hochschule Sankt Georgen den neuen Sitz der Datenschutzaufsicht.

Neben Redebeiträgen von Frau Stephanie Rieth, der Bevollmächtigten des Generalvikars des Bistums Mainz, Herrn Dr. Sascha Koller, Vorsitzender des Verwaltungsrats des Kath. Datenschutzzentrums Frankfurt/M. und Frau Ursula Becker-Rathmair wurde die Feierstunde auch musikalisch durch Mitarbeiterinnen und Mitarbeiter umrahmt. Im Anschluss fanden sich die Anwesenden zu angeregten Gesprächen zusammen und für das leibliche Wohl war ebenfalls gesorgt.

” Freiheit ohne Grenzen,
Frieden ohne Bedingungen,
Achtsamkeit ohne
Kompromisse,
Leben ohne Gewalt.
Das wünschen wir uns,
lieber Gott. “

Segensspruch anlässlich der Einsegnung
am 28. September 2023



Neben „Air“ aus der Orchestersuite Nr. 3 von Johann Sebastian Bach erklang auch „Oh, Lady Be Good“ von George Gershwin.



Die bei der Einsegnungsfeier gesungenen Lieder wurden durch professionelle Begleitung am Klavier kreativ unterstützt.

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



**Pfarrer Prof. Wolfgang Beck eröffnete die Feier und
segnete im Anschluss die neuen Räumlichkeiten.**



**Vorsitzender des Verwaltungsrats des überdiözesanen
Kath. Datenschutzzentrums Frankfurt/M.
Dr. Sascha Koller**



**Stephanie Rieth, Bevollmächtigte des
Generalvikars des Bistums Mainz**

2 Entwicklung des Datenschutzes

Ein halbes Jahrzehnt Europäische Datenschutzgrundverordnung (DSGVO) und Gesetz über den Kirchlichen Datenschutz (KDG) – diese „kleinen Geburtstage“ waren im Jahr 2023 zu feiern. Die Zeitspanne von fünf Jahren mag zunächst kurz erscheinen, doch angesichts der rasant fortschreitenden Digitalisierung erhält die informationelle Selbstbestimmung eines jeden Einzelnen immer größere Bedeutung. Denn nicht nur Smartphones, sondern Smartgeräte jeglicher Art sind in allen Lebensbereichen zu finden, wodurch die IT-Sicherheit wachsende Bedeutung erlangt. Dies kann als positiver Nebeneffekt der Datenschutzgesetzgebung gesehen werden, denn umfangreiche Anforderungen an die Ausgestaltung der technischen und organisatorischen Maßnahmen („TOMs“) sind sowohl in der DSGVO als auch im KDG zu finden.

Doch es gibt noch reichlich Entwicklungspotenzial: Vor allem in den Bereichen „Technikgestaltung und Voreinstellungen“, spezifiziert in § 27 KDG bzw. dem korrespondierenden Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ kann und sollte im Laufe der kommenden Jahre der Datenschutz und damit der Schutz der Persönlichkeitsrechte der betroffenen Personen eine deutliche Weiterentwicklung erfahren. So könnte a priori bereits Entscheidendes festgelegt und eine aufwändige Nachbesserung verhindert werden, was vor allem bei der Verarbeitung sensibler Daten, wie zum Beispiel Gesundheitsdaten, von großer Bedeutung ist.

2.1 Staatliche Gesetzgebung

2.1.1 Hinweisgeberschutzgesetz

Der Bundesrat hat im Februar 2023 seine Zustimmung zum vom Bundestag im Dezember 2022 verabschiedeten „Gesetz für einen besseren Schutz hinweisgebender Personen“ (Hinweisgeberschutzgesetz - HinSchG) verweigert und als Folge wurde ein Vermittlungsausschuss eingesetzt. Dem vom Vermittlungsausschuss erarbeiteten Kompromissvorschlag haben der Bundestag und der Bundesrat im Mai 2023 zugestimmt und das Gesetz konnte am 2. Juli 2023 in Deutschland in Kraft treten. Damit erfolgte die längst überfällige Umsetzung der sogenannten „Whistleblower-Richtlinie“ (Richtlinie (EU) 2019/1937), denn diese hätte bereits bis zum 17. Dezember 2021 in deutsches Recht umgesetzt werden müssen.

Erhalten Beschäftigte im Rahmen ihrer beruflichen Tätigkeit Kenntnis von Rechtsverstößen, können sie in einen Konflikt geraten, denn die Meldung des Verstoßes und die Loyalitätspflichten als Beschäftigter sind zumeist nicht vereinbar. Die Befürchtung negativer Folgemaßnahmen kann dazu führen, dass mögliche Rechtsverstöße nicht gemeldet werden und somit unentdeckt bleiben. Dem soll das Hinweisgeberschutzgesetz entgegenwirken. Kern dieses Regelwerks ist die Einrichtung von internen Meldestellen in Unternehmen und Behörden, an die sich hinweisgebende Personen wenden können, wenn sie im

Zusammenhang mit ihrer beruflichen Tätigkeit Informationen über Verstöße erlangt haben. Dabei ist neben der Wahrung der Vertraulichkeit der Identität des Hinweisgebers auch sicherzustellen, dass ausschließlich die für die Entgegennahme und Bearbeitung der Meldungen zuständigen Personen Zugriff auf eingehende Meldungen haben.

Ergänzend zu den internen Meldestellen wurde beim Bundesamt für Justiz eine externe Meldestelle des Bundes eingerichtet.

2.1.2 Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework

Rechtssicherer Datentransfer in die USA – war er, ist er, wird er jemals möglich sein? Diese wichtige Frage stellt sich seit Langem im Datenschutz. Es handelt sich dabei um eine grundsätzliche Problemstellung, denn im Falle der EU und den USA treffen aus datenschutzrechtlicher Perspektive zwei Welten aufeinander. Während der Datenschutz in der EU ein Grundrecht ist, mit dem das Recht auf informationelle Selbstbestimmung eines jeden Einzelnen gewahrt werden soll, ist der Datenschutz in den USA ein Bestandteil des Wirtschaftslebens, es gibt kein allgemeines und umfassendes Datenschutzgesetz.

Das aus dem Jahr 2000 stammende Safe-Harbor-Abkommen, das den transatlantischen Datentransfer aus datenschutzrechtlicher Sicht mithilfe eines Abkommens zwischen der EU-Kommission und den USA möglich gemacht hatte, wurde im Oktober 2015 durch den Europäischen Gerichtshof (EuGH) mit dem sogenannten Schrems-I-Urteil gekippt. Das Gericht stellte fest, dass ein gleichwertiges Datenschutzniveau in den USA im Vergleich zur EU durch Safe Harbor nicht gewährleistet werde, denn es mangle in den USA an entsprechenden Rechtsvorschriften und Verpflichtungen.

Im Jahr 2016 trat der sogenannte Privacy Shield in Kraft, bei dem es sich um Zusicherungen der US-amerikanischen Regierung und einen Angemessenheitsbeschluss der EU-Kommission handelte, der festlegte, dass die Vorgaben des Privacy Shields dem Datenschutzniveau der Europäischen Union entsprächen. Auch diese bilaterale Vereinbarung wurde vom EuGH kassiert, und zwar durch das Schrems-II-Urteil im Juli 2020. Von einem auf den anderen Tag gab es keine Rechtsgrundlage mehr für den transatlantischen Datenaustausch.

Das EU-US Data Privacy Framework (DPF), das eine der möglichen Rechtsgrundlagen für die Übermittlung personenbezogener Daten in die USA darstellt, trat am 10. Juli 2023 zusammen mit dem Angemessenheitsbeschluss der EU-Kommission in Kraft. Es handelt sich hierbei um Regelungen mit inhaltlicher Nähe zur DSGVO, was sich an den „EU-US-DPF Principles“ zeigt: Deren Definitionen gleichen denen der DSGVO, Grundsätze wie Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung wurden übernommen, geeignete TOMs sind zu ergreifen und Betroffenenrechte gegenüber Verantwortlichen und Auftragsverarbeitern werden geregelt. Darüber hinaus werden Rechtbehelfsmechanismen

geschaffen, mit denen sowohl unerlaubte Zugriffe überprüft als auch die Rechtsbehelfe der Betroffenen festgelegt werden können.

US-amerikanische Unternehmen, die am DPF teilnehmen wollen, müssen sich selbst zertifizieren und als Datenimporteure in die Liste des Department of Commerce (DOC) aufgenommen werden. Die Zertifizierung muss jährlich erneuert werden.

Unternehmen mit Sitz in der EU, die ihren transatlantischen Datentransfer auf das DPF stützen wollen, müssen prüfen, ob der Datenimporteur auf der Liste des DOC steht.



► Anwendungshinweise der DSK

Vorläufig scheint die Rechtsunsicherheit bezüglich der transatlantischen Datenübermittlung beendet, vermutlich ist es aber nur eine Frage der Zeit, bis eine Klage eingereicht wird und auch das DPF einer gerichtlichen Bewertung ausgesetzt ist. Welche Entscheidung dann getroffen wird, ist völlig unklar.

Darüber hinaus ist hier erwähnenswert, dass der Einsatz von Auftragsverarbeitern, wie zum Beispiel Microsoft, durchaus weitere datenschutzrechtliche Fragen aufwirft, die durch das DPF nicht abgedeckt sind, beispielsweise die Einhaltung der Datenschutzgrundsätze gemäß Art. 5 DSGVO bzw. § 7 KDG oder der Einsatz geeigneter TOMs gemäß Art. 25 DSGVO bzw. § 26 KDG. Diese müssen vom Verantwortlichen nachgewiesen werden.

Katholisches Datenschutzzentrum Frankfurt/M.

Rechtssicherer Datentransfer in die USA – war er, ist er, wird er jemals möglich?

- EU und USA - aus datenschutzrechtlicher Perspektive treffen hier zwei Welten aufeinander
 - Grundrecht versus Element des Wirtschaftslebens
 - unabhängige Datenschutzaufsichtsbehörden: die *Federal Trade Commission (FTC)*, die *Department of Justice*
 - gesetzlich klar geregelte Möglichkeiten für den Datentransfer
 - Zugriffe auf Daten ohne richterliche Anordnung
- unser Thema heute: *Angemessenheitsbeschluss der EU-Kommission*

© Katholisches Datenschutzzentrum Frankfurt/M. Austauschtreffen bDSB Ordinarate • 21.11.2023

Katholisches Datenschutzzentrum Frankfurt/M.

5. Ausblick (1)

VORLÄUFIG
scheint der Zustand der Rechtsunsicherheit beim Drittlandstransfer in die USA beendet.

UNTERNEHMEN oder ORGANISATIONEN
müssen aber handeln, um die Möglichkeiten des *Data Privacy Frameworks* nutzen zu können.

FRAGLICH BLEIBT
ob das mittlerweile dritte Abkommen zum transatlantischen Datentransfer Bestand haben wird.

© Katholisches Datenschutzzentrum Frankfurt/M. Austauschtreffen bDSB Ordinarate • 21.11.2023

Katholisches Datenschutzzentrum Frankfurt/M.

5. Ausblick (2)

Rechtssicherer Datentransfer in die USA?
⇒ Es bleibt beim „Jein“!

„Denn am Horizont ist [...] schon die Mastspitze von „Schrems III“ zu sehen.“
(Zitat aus dem Tätigkeitsbericht 2022 des Kath. Datenschutzzentrums Frankfurt/M.)

⇒ **WICHTIG:**
Das *Data Privacy Framework* regelt einzig den **Datentransfer in die USA**, jegliche andere Fragestellungen bezüglich der rechtmäßigen Verarbeitung der pb-Daten bleiben durch das DPF unbeantwortet und müssen separat geprüft werden!

© Katholisches Datenschutzzentrum Frankfurt/M. Austauschtreffen bDSB Ordinarate • 21.11.2023

Auszüge aus der Präsentation des Kath. Datenschutzzentrums Frankfurt/M. zum Thema DPF

Es bleibt also festzuhalten, dass das DPF einzig den Datentransfer in die USA regelt, jegliche andere Fragestellungen bezüglich der rechtmäßigen Verarbeitung personenbezogener Daten bleiben durch das DPF unbeantwortet und müssen weiterhin vom Verantwortlichen hierzulande separat geprüft werden.

2.1.3 Digital Services Act (EU-Verordnung)

Der Digital Services Act (DSA) soll gemeinsam mit dem Digital Markets Act (DMA) zu einer Art Grundgesetz für das Internet werden. Als EU-Verordnung gilt der DSA zwar erst ab Februar 2024 unmittelbar in allen Mitgliedstaaten, bereits seit 25. August 2023 müssen aber sehr große Plattformen und Suchmaschinen erste Vorgaben umsetzen, zum Beispiel die Einhaltung neuer Transparenzregeln und die Bereitstellung von Beschwerdemöglichkeiten.

Durch diese EU-Verordnung sollen Grundregeln für das Verhalten digitaler Diensteanbieter geschaffen werden, um gleiche Wettbewerbsbedingungen für die Förderung von Innovation, Wachstum und Wettbewerbsfähigkeit zu gewährleisten. Für die Nutzerinnen und Nutzer der digitalen Dienste soll ein sicherer digitaler Raum entstehen, in dem ihre Grundrechte geschützt und Rechtsschutzmöglichkeiten eröffnet werden.



▶ European Commission:
The Digital Services Act



Der DSA enthält Vorschriften für Online-Dienste, die täglich von Millionen von Menschen in Europa genutzt werden. Die Pflichten der einzelnen Online-Unternehmen variieren je nach Rolle, Größe und Auswirkung im Online-Umfeld.

Das Risiko der Verbreitung illegaler Inhalte und daraus resultierender Schäden in der Gesellschaft ist auf sehr großen Online-Plattformen und Suchmaschinen besonders hoch. Deshalb sind für Plattformen, die mehr als 10 % der 450 Millionen Verbraucherinnen und Verbraucher in Europa erreichen, besondere Vorschriften vorgesehen.

2.2 Kirchliche Gesetzgebung

2.2.1 Erzbistum Freiburg richtet interne Meldestelle nach Hinweisgeberschutzgesetz bei Rechnungshof ein

Nach dem Inkrafttreten des HinSchG im Jahr 2023 stellt sich auch in den sieben Bistümern im Zuständigkeitsbereich des Kath. Datenschutzzentrums Frankfurt/M. die Frage, wo die jeweils dafür vorgesehene Meldestelle anzusiedeln ist. Das Erzbistum Freiburg hat sich dafür entschieden, die interne Meldestelle beim Rechnungshof anzudocken. Hierfür wurde § 8 des Statuts des Rechnungshofs geändert. In der genannten Vorschrift heißt es nun unter der Überschrift „Hinweisgebersystem, Ombudsmann“:

„Bei dem Rechnungshof wird eine interne Meldestelle eingerichtet, deren Aufgabe es ist, Hinweise von internen und externen Personen über Complianceverstöße bei den der Prüfungszuständigkeit des Rechnungshofs unterliegenden Rechtsträgern, Dienststellen und Einrichtungen entgegenzunehmen, diese in Bezug auf ihre Stichhaltigkeit zu prüfen und angemessene Folgemaßnahmen zu ergreifen.“ Diese nimmt die Aufgaben der internen Meldestelle nach dem HinSchG wahr.

Weiter ist in Absatz 1 von § 8 des Statuts klar geregelt, dass die Identität von Hinweispersonen nur mit deren Einverständnis oder auf verbindliche Anordnung staatlicher Stellen offenbart werden darf.

Geleitet wird die interne Meldestelle von einer Ombudsperson, die durch den Ordinarius auf Vorschlag der Leitung des Rechnungshofs bestellt wird. Diese nimmt ihre Aufgaben



unabhängig wahr und berichtet direkt an den Ordinarius. Vertreten wird die Ombudsperson durch die Rechnungshofleitung, sofern der Meldestelle „nicht weitere Mitarbeitende zugewiesen sind“.

In den Ausführungsbestimmungen zum Hinweisgebersystem ist zum Datenschutz Folgendes geregelt:

§ 4 Datenschutz

Soweit das HinSchG keine gesonderte Regelung trifft, gilt das Kirchliche Datenschutzgesetz (KDG), wobei § 16 KDG mit der Maßgabe gilt, dass eine Unterrichtung später erfolgen oder unterbleiben kann, wenn dies die ordnungsgemäße Bearbeitung des Hinweises beeinträchtigen würde.

Das Gesetz ist am 2. August 2023 in Kraft getreten und im Amtsblatt der Erzdiözese Freiburg Nr. 14 vom 1. August 2023 ab Seite 276 veröffentlicht.

2.2.2 Neues Beschwerdemanagement im Bistum Limburg

Neben dem digitalen Hinweisgebersystem gibt es seit dem 1. Dezember 2023 ein neues Beschwerdemanagement mitsamt einer Schlichtungsstelle und einen externen, unabhängigen Beschwerdenavigator. Die entsprechende Ordnung wurde im Amtsblatt des Bistums Limburg Nr. 10/2023 ab Seite 217 veröffentlicht und ersetzt die Beschwerdeordnung aus dem Jahr 1997. Damit soll allen mit dem Bistum in Kontakt stehenden Personen eine transparente und niederschwellige Beschwerdemöglichkeit gegeben werden. Das Beschwerdemanagement soll einen Beitrag für die nachhaltige Bearbeitung von Beschwerden und somit einen Beitrag zur Organisations- und Rechtskultur im Bistum leisten und Machtmissbrauch frühzeitig unterbinden. Das Ziel der Beschwerdeordnung ist laut deren Satzung im Sinne der MHG-Studie vor allem die Verhinderung bzw. frühzeitige Erkennung von Machtmissbrauch. Die Studie habe aufgezeigt, dass sexueller Missbrauch durch andere Formen des Machtmissbrauchs angebahnt werden könne. Das Beschwerdemanagement soll als extern vorgeschaltete Stelle fungieren, an die alle Beschwerden gerichtet werden können und die diese Beschwerden zur Bearbeitung an die zuständige interne Stelle weiterleitet.

Die Ordnung gibt vor, dass eine Beschwerde „in jedem Fall registriert“ und der Inhalt „schriftlich“ festgehalten wird. Da dabei mitunter sensible personenbezogene Daten im Spiel sind, weist Absatz 6 von § 1 ausdrücklich darauf hin, dass dies alles nach den einschlägigen datenschutzrechtlichen Vorgaben zu erfolgen hat und entsprechend anzulegen und aufzubewahren ist.

Eine Bearbeitung von anonymen Beschwerden erfolgt nicht. Diese werden lediglich zu statistischen Zwecken registriert und zu den Akten genommen.

Die Schlichtungsstelle nach der Beschwerdeordnung dient der Konfliktbewältigung und soll vorrangig der gütlichen Einigung bei Streitigkeiten dienen. Deren Mitglieder sind zur Verschwiegenheit verpflichtet.

2.2.3 Bistum Fulda veröffentlicht Datenschutzinfos zu neuem Hinweisgeberschutzgesetz

Das Bistum Fulda hat seine Revision mit den Aufgaben einer internen Meldestelle nach dem HinSchG betraut. Die Revision nimmt Meldungen über Regelverstöße auf telefoni-schem und postalischem Wege entgegen und nach Terminvereinbarung auch persönlich. Die Meldestelle ist zuständig für den Rechtsträger Bistum und für diejenigen Kirchengemeinden, die das Bistum mit der Wahrnehmung der Aufgaben einer internen Meldestelle beauftragen.

Die Diözese Fulda hat hierzu ergänzend Datenschutzinformationen gemäß §§ 14, 15 KDG im Rahmen der Umsetzung des HinSchG in seinem Amtsblatt (Stück XIV vom 22. Dezember 2023 ab Seite 433) veröffentlicht. Das Bischöfliche Generalvikariat und die teilnehmenden Kirchengemeinden kommen auf diese Weise den Pflichten einer transparenten Datenverarbeitung im Rahmen der Umsetzung des HinSchG gemäß §§ 14 ff. KDG nach.

Neben den Rechtsgrundlagen, den Verarbeitungszwecken oder der Speicherdauer weisen die Datenschutzinformationen auch auf die Weitergabe der Hinweise an die im Bistum zuständigen Fachabteilungen hin – sowie auf das Vorgehen, sollten die bereitgestellten Hinweise nicht in den Anwendungsbereich des HinSchG fallen: Die interne Meldestelle wird in diesem Fall den Hinweisgeber hierüber informieren, sofern dessen Kontaktdaten vorliegen, und an die richtige Stelle in der Diözese – wie beispielsweise den betrieblichen Datenschutz oder das Beschwerdemanagement – verweisen. Meldungen, aus denen sich ein Verdacht auf sexuellen Missbrauch ergibt, werden ohne Nennung des Hinweisgebers „auf jeden Fall an den Interventionsbeauftragten der Diözese weitergeleitet“, so steht es ausdrücklich in den Datenschutzinfos. Dieser ist dann bei Vorliegen von Anhaltspunkten für das Vorliegen von Sexualstraftaten seinerseits verpflichtet, die Strafverfolgungsbehörden zu informieren – sofern kein Widerspruch durch den von Missbrauch Betroffenen vorliegt.

2.2.4 Verpflichtung auf Datengeheimnis – neue Mustertexte und Merkblätter im Bistum Fulda / Vorgehen bei Mitarbeiterexzess

Verantwortliche sind nach dem KDG gehalten, haupt- und ehrenamtlich Beschäftigte bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten. Denn Verarbeitung und Nutzung personenbezogener Daten sind vielfach Teil einer haupt- oder ehrenamtlichen Tätigkeit.

Das Bistum Fulda hat deshalb sein Merkblatt zur Verpflichtung auf das Datengeheimnis und die dazugehörigen Mustertexte für die Verpflichtungserklärungen zum Datengeheimnis gemäß § 5 KDG von Beschäftigten und ehrenamtlich Tätigen aktualisiert (Amtsblatt Stück VII vom 30. Juni 2023).

Das überarbeitete Merkblatt stellt wiederum klar, dass eine Verarbeitung personenbezogener Daten nur in dem Umfang und in der Weise gestattet ist, wie es zur Aufgabenerfüllung erforderlich ist. Neu ist der sich anschließende Hinweis, der auch die datenschutzrechtliche Praxis des Kath. Datenschutzzentrums Frankfurt/M. zum sogenannten Mitarbeiterexzess wiedergibt:

„Insbesondere ist es nicht erlaubt, personenbezogene Daten aus einer dienstlichen oder ehrenamtlichen Tätigkeit für eigene private oder geschäftliche Zwecke zu verwenden. In einem solchen Fall würde der/die Mitarbeiter/in selbst Verantwortliche und somit der Datenschutzgrundverordnung einschließlich deren Bußgeldvorschriften unterliegen.“

Kirchliches Amtsblatt Fulda 2023, Stück VII 185

Mustertext für ehrenamtlich Tätige

**Verpflichtungserklärung zum Datengeheimnis gemäß § 5 KDG
(Kirchliches Datenschutzgesetz der Diözese Fulda)**

Vorname, Name _____

Anschrift _____

Ehrenamtliche Tätigkeit bei/für _____

Ich verpflichte mich zur Einhaltung des Datengeheimnisses gemäß § 5 KDG, das kirchliche Datenschutzgesetz einschließlich der jeweils geltenden Fassungen sowie anderer für meine Tätigkeit geltende Datenschutzvorschriften sorgfältig einzuhalten.

Darüber hinaus bestätige ich, dass ich auf die für die Ausübung meiner Tätigkeit spezifisch geltenden Bestimmungen und im Übrigen auf die allgemeinen datenschutzrechtlichen Regelungen in den jeweils geltenden Fassungen hingewiesen wurde und versichere deren Einhaltung. Die Texte wurden mir zur Einsichtnahme ausgehändigt oder werden mir in digitaler Form bereitgestellt. Auf Anforderung wird mir das Gesetz nebst Verordnungen auch in Papierform zur Verfügung gestellt.

Ich bin darüber belehrt worden, dass das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten ist und dass ein Verstoß gegen das KDG oder die anderen für meine Tätigkeit geltenden Datenschutzvorschriften und Verschwiegenheitspflichten rechtliche Folgen haben kann. Dies können disziplinar- oder arbeitsrechtliche Konsequenzen sein, z.B. Abmahnung und Kündigung, ferner Schadenersatzansprüche im Rahmen der Haftung oder Schmerzensgeld, Geldbußen, Geld- und Freiheitsstrafen.

Ein Exemplar der Verpflichtungserklärung wurde mir ausgehändigt.

(Vorname, Name in leserlicher Form)

(Ort, Datum)

Kirchliches Amtsblatt Fulda 2023, Stück VII 184

Mustertext für Beschäftigte

**Verpflichtungserklärung zum Datengeheimnis gemäß § 5 KDG
(Kirchliches Datenschutzgesetz der Diözese Fulda)**

Vorname, Name _____

Dienststelle _____

Personalnummer _____

Geburtsdatum, Anschrift (nur sofern Personalnummer nicht vorhanden) _____

Ich verpflichte mich zur Einhaltung des Datengeheimnisses gemäß § 5 KDG. Ferner verpflichte ich mich, das kirchliche Datenschutzgesetz einschließlich der Durchführungsverordnung sowie anderer für meine Tätigkeit geltende Datenschutzvorschriften in den jeweils geltenden Fassungen sorgfältig einzuhalten.

Darüber hinaus bestätige ich, dass ich auf die für die Ausübung meiner Tätigkeit spezifisch geltenden Bestimmungen und im Übrigen auf die allgemeinen datenschutzrechtlichen Regelungen in den jeweils geltenden Fassungen hingewiesen wurde und versichere deren Einhaltung. Die Texte wurden mir zur Einsichtnahme ausgehändigt oder werden mir in digitaler Form bereitgestellt. Auf Anforderung wird mir das Gesetz nebst Verordnungen auch in Papierform zur Verfügung gestellt.

Ich bin darüber belehrt worden, dass das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten ist und dass ein Verstoß gegen das KDG oder die anderen für meine Tätigkeit geltenden Datenschutzvorschriften und Verschwiegenheitspflichten rechtliche Folgen haben kann. Dies können disziplinar- oder arbeitsrechtliche Konsequenzen sein, z.B. Abmahnung und Kündigung, ferner Schadenersatzansprüche im Rahmen der Haftung oder Schmerzensgeld, Geldbußen, Geld- und Freiheitsstrafen.

Ein Exemplar der Verpflichtungserklärung wurde mir ausgehändigt.

(Vorname, Name in leserlicher Form)

(Ort, Datum) _____

(Unterschrift)

Das Bistum Fulda hat sein Merkblatt zur Verpflichtung auf das Datengeheimnis und die dazugehörigen Mustertexte für die Verpflichtungserklärungen von Beschäftigten und Ehrenamtlichen aktualisiert.

2.2.5 *Bistum Fulda bündelt Datenschutz im Gesetz zur Regelung von Einsichts- und Auskunftsrechten der Aufarbeitungskommission*

Das Bistum Fulda hat aus datenschutzrechtlicher Sicht relevante Änderungen an dem erst 2022 verabschiedeten Gesetz zur Regelung von Einsichts- und Auskunftsrechten der Kommission zur Aufarbeitung des sexuellen Missbrauchs Minderjähriger und schutz- und hilfebedürftiger Erwachsener vorgenommen. Zum 1. August 2023 wurden die in dem Regelwerk verstreuten Datenschutzregelungen vor allem zur Pseudonymisierung nunmehr in § 9 des Gesetzes gebündelt. Der eigentliche Text des § 9 findet sich leicht versteckt im 4. Absatz der Neufassung unverändert wieder.

Neufassung § 9 Gesetz zur Regelung von Einsichts- und Auskunftsrechten der Kommission zur Aufarbeitung des sexuellen Missbrauchs Minderjähriger und schutz- und hilfebedürftiger Erwachsener:

Artikel 1

Änderung des Gesetzes

...

3. § 9 wird wie folgt gefasst:

„§ 9

Datenschutz

(1) Vor der Weitergabe von Dokumenten und Informationen an die Kommission nach den Normen dieses Gesetzes sind die Identitäten der durch die Taten im Sinne von § 1 Nr. 4 Betroffenen zu pseudonymisieren und Hinweise, die eindeutige Rückschlüsse auf ihre Identität ermöglichen würden, zu schwärzen oder anderweitig unkenntlich zu machen. Besteht nach dem Urteil der Interventionsbeauftragten der Diözese oder aufgrund eines ausdrücklichen Wunsches eines Betroffenen ein erhöhter Schutzbedarf, gilt dies auch für alle Daten, die Rückschlüsse auf die Identität eines Betroffenen erleichtern würden.

(2) Die Gewährung von Akteneinsicht nach § 10 Abs. 2 geschieht in der Weise, dass Einsicht in Aktenkopien zu gewähren ist, in denen besonders schutzwürdige personenbezogene Daten geschwärzt oder anderweitig unkenntlich gemacht worden sind. Dies gilt nicht, soweit sich die Daten auf Personen beziehen, in deren Personalakten nach den §§ 2 bis 4 Einsicht zu gewähren ist und, soweit nach den Normen dieses Gesetzes erforderlich, ein entsprechendes rechtskräftiges Dekret zur Gewährung von Akteneinsicht vorliegt.

(3) Veröffentlichungen nach § 11 dürfen keine besonders schutzwürdigen personenbezogenen Daten enthalten. § 11 Abs. 2 bleibt unberührt.

(4) Der Kommission nach den Normen dieses Gesetzes überlassene Dokumente sind datenschutzkonform und gegen unbefugte Kenntnisnahme geschützt aufzubewahren.“

2.2.6 Bistum Fulda hat jetzt auch ein § 29-KDG-Gesetz

In datenschutzrechtlicher Hinsicht hat sich einiges im letzten Jahr im Bistum Fulda getan, wie auch in diesem Bericht deutlich wird. Der Bischof hat wie zuvor schon seine Amtskollegen im Erzbistum Freiburg und in den Diözesen Mainz und Rottenburg-Stuttgart (das Kath. Datenschutzzentrum Frankfurt/M. berichtete hierüber in den letzten Tätigkeitsberichten) ein Gesetz zur Regelung des Rechtsinstruments nach § 29 KDG über die Verarbeitung personenbezogener Daten im Auftrag zum 1. November 2023 erlassen.

Damit gestaltet sich die Auftragsverarbeitung zwischen kirchlichen Stellen im Bistum Fulda nunmehr ebenfalls einfacher, da die Verarbeitung auf Grundlage dieses Rechtsinstruments erfolgen kann.

Näheres regelt die ausführliche Durchführungsverordnung (DVO) zum § 29-KDG-Gesetz, die neben den erforderlichen TOMs unter anderem auch den Auftragsinhalt konkretisiert, indem sie Art, Zweck und Gegenstand der Datenverarbeitung bezogen auf die einzelnen Aufgaben des Verarbeiters detailliert beschreibt.

2.2.7 Freiburg und Trier erlassen Ordnungen zu Einsichts- und Auskunftsrechten in Sachakten

Im Berichtszeitraum haben die Erzdiözese Freiburg sowie die Diözese Trier eigene Ordnungen „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“ in Kraft gesetzt.

Die Ordnungen regeln die Offenlegung von Unterlagen aller kirchlichen Rechtsträger und deren Einrichtungen in den beiden (Erz-)Diözesen, unabhängig von ihrer Rechtsform, in Form der Übermittlung (Auskunft) und in Form der Bereitstellung (Einsicht) gegenüber unabhängigen Aufarbeitungskommissionen, zu Forschungszwecken sowie gegenüber Rechtsanwaltskanzleien.

Soweit sich aus den beiden Regelwerken nichts Abweichendes ergibt, finden für die Verarbeitung personenbezogener Daten jeweils das KDG und die zu seiner Durchführung ergangenen Vorschriften, insbesondere die Durchführungsverordnung zum Kirchlichen Datenschutzgesetz (KDG-DVO), sowie die Kirchliche Archivordnung (KAO) in ihrer jeweils geltenden Fassung Anwendung.

Das Bistum Fulda hatte bereits zuvor als einziges Bistum im Zuständigkeitsbereich das Gesetz zur Regelung der Einsichtsrechte in Personalakten ausdrücklich auf Sachakten und Ähnliches erweitert. Im Tätigkeitsbericht für das Jahr 2022 wurde hierüber eingehend berichtet.

2.3 Ausgewählte Rechtsprechung staatlicher Gerichte

Der EuGH hat sich im Jahr 2023 intensiv um die Konkretisierung des Auskunftsanspruchs gemäß Art. 15 DSGVO gekümmert. Er hat einige wegweisende Entscheidungen gefällt, die bei der Auslegung der Vorschrift unterstützen.

2.3.1 Konkrete Empfänger zu benennen

Gleich zu Beginn des Berichtszeitraums hat der EuGH (Urteil vom 12. Januar 2023, Az.: C-154/21) entschieden, dass im Rahmen eines Auskunftsanspruchs jedem Betroffenen das Recht zusteht zu erfahren, an wen seine personenbezogenen Daten weitergegeben wurden. Der betroffenen Person – und nicht dem Verantwortlichen – obliegt also die Entscheidung, ob sie Auskunft über konkrete Empfänger oder über Empfängerkategorien gemäß Art. 15 Abs. 1 lit. c) DSGVO wünscht.

Der für die Datenverarbeitung Verantwortliche könne sich jedoch darauf beschränken, nur die Empfängerkategorien mitzuteilen, wenn es nicht möglich ist, die Empfänger zu identifizieren, oder wenn der Antrag offenkundig unbegründet oder exzessiv sei – was allerdings der Verantwortliche nachzuweisen habe.

Der Gerichtshof weist darauf hin, dass dieses Auskunftsrecht der betroffenen Person insbesondere erforderlich ist, um es ihr gegebenenfalls zu ermöglichen, die anderen Rechte auszuüben, die ihr gemäß der DSGVO zukommen, konkret das Recht auf Berichtigung, das Recht auf Löschung („Recht auf Vergessenwerden“), das Recht auf Einschränkung der Verarbeitung, das Recht auf Widerspruch gegen die Verarbeitung oder auch das Recht auf einen Rechtsbehelf im Schadensfall.

2.3.2 Datenverarbeitung im Beschäftigungskontext

Am 30. März 2023 hat der EuGH in einem Urteil (Az.: C-34/21) festgestellt, dass § 23 des hessischen Datenschutz- und Informationsfreiheitsgesetzes (und damit auch der wortgleiche § 26 Abs. 1 S. 1 des Bundesdatenschutzgesetzes (BDSG)) gegen Europarecht verstößt, weil es sich dabei um keine gegenüber den europarechtlichen Regelungen „spezifischere Vorschrift“ im Sinne des Art. 88 DSGVO handele.

Die hier geregelte „Datenerfassung für Zwecke des Beschäftigungsverhältnisses“ – wie es im BDSG heißt - erfüllt nach Ansicht des EuGH die Voraussetzungen einer Öffnungsklausel nicht, sodass die Schaffung eigener Regelungen an dieser Stelle nicht möglich ist. Der Wortlaut der hessischen Regelung wiederholt laut EuGH-Urteil nur die allgemeinen europarechtlichen Rechtmäßigkeitsbedingungen und Rechtsgrundlagen, insbesondere die Verarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 Unterabsatz 1 lit. b) DSGVO.

Auch wenn die Entscheidung des EuGH zunächst nur eine hessische Regelung zum Beschäftigtendatenschutz betrifft, die zudem ausschließlich auf die Datenverarbeitung durch öffentliche Stellen Anwendung findet, so lassen sich die Erläuterungen der Europarichter doch auch auf § 26 Abs. 1 S.1 BDSG übertragen und stellen damit dessen Vereinbarkeit mit Art. 88 DSGVO erheblich in Frage.

” Die Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz dürften durch diese EuGH-Entscheidung in jedem Fall verstärkt werden. “

Datenverarbeitungen im Beschäftigungskontext werden deswegen jedoch nicht beendet oder ausgesetzt werden müssen, denn es lassen sich diesbezüglich andere Rechtsgrundlagen finden, deren Anwendbarkeit von den verantwortlichen Stellen zu prüfen sein wird.

Deutlich gemacht hat der EuGH aber mit seinem Urteil, dass die interpretationsbedürftigen Vorschriften des deutschen Beschäftigtendatenschutzes nicht mit den Vorgaben des Art. 88 DSGVO vereinbar sind. Die Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz dürften durch diese EuGH-Entscheidung in jedem Fall verstärkt werden.

2.3.3 Kopie als Teil des Auskunftsanspruchs

Das Recht, eine Kopie der personenbezogenen Daten zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten ausgehändigt wird. Dieses Recht, so der EuGH in seinem Urteil vom 4. Mai 2023 (Az.: C-487/21), impliziert das Recht, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die diese Daten

enthalten, zu erlangen, wenn dies unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr zustehenden Rechte in der DSGVO zu ermöglichen. Dabei sind aber auch immer die Rechte und Freiheiten Dritter zu beachten – wobei die Abwägung nicht dazu führen dürfe, dass der betroffenen Person jegliche Auskunft verweigert würde.

Des Weiteren stellen die Richter klar, dass sich der in Art. 15 Abs. 3 Satz 3 DSGVO verwendete Begriff „Informationen“ ausschließlich auf personenbezogene Daten bezieht, von denen der Verantwortliche Kopien zur Verfügung zu stellen hat. § 17 Abs. 3 Satz 3 KDG ist wortgleich mit der genannten DSGVO-Vorschrift, was die Übertragbarkeit auf den kirchlichen Datenschutz zur Folge hat.

In diesem Urteil hat sich der EuGH auch mit dem Verhältnis von Absatz 1 (Recht auf Auskunft) und Absatz 3 (Recht auf Kopie) des Art. 15 der Grundverordnung dahingehend beschäftigt, ob diese unterschiedliche Ansprüche darstellen. Er kommt zu dem Schluss, dass Absatz 1 den Gegenstand sowie den Anwendungsbereich des der betroffenen Person zustehenden Auskunftsrechts festlegt und Absatz 3 lediglich die praktischen Modalitäten der Erfüllung regelt. Das Recht auf Erhalt einer Kopie in Absatz 3 ist also Teil des Auskunftsanspruchs aus Absatz 1 – und kein eigener, extra geltend zu machender Anspruch.

Das Kath. Datenschutzzentrum Frankfurt/M. empfiehlt an dieser Stelle regelmäßig, dass verantwortliche Stellen aufgrund der weiten Auslegung des Begriffs „Kopie“ durch den EuGH zur Vorbereitung auf ein solches mögliches Begehren einen Prozess etablieren und die involvierten Mitarbeiterinnen und Mitarbeiter hierzu schulen sollten.

2.3.4 Interne sind keine Empfänger

Eine klare Grenze im Rahmen des Auskunftsbegehrens hat der EuGH (Urteil vom 22. Juni 2023, Az.: C-579/21) im letzten Jahr auch bei internen Empfängern gezogen: Nach dieser Entscheidung sind Beschäftigte des Verantwortlichen nicht als Empfänger im Sinne der DSGVO anzusehen, wenn sie personenbezogene Daten unter der Aufsicht des Verantwortlichen und im Einklang mit seinen Weisungen verarbeiten. Über diese müsse also im Rahmen eines Auskunftsanspruchs nicht beauskunftet werden.

Eine Ausnahme davon sehen die Europarichter dann, wenn diese Informationen unerlässlich sind, um der betroffenen Person zu ermöglichen, die ihr durch diese Verordnung verliehenen Rechte wirksam wahrzunehmen – immer vorausgesetzt, dass die Rechte und Freiheiten der Mitarbeitenden berücksichtigt werden. Falls nämlich die Wahrnehmung eines Rechts auf Auskunft, das die praktische Wirksamkeit der Rechte, die der betroffenen Person durch die DSGVO eingeräumt werden, sicherstellt, zum einen und die Rechte und

Freiheiten anderer Personen zum anderen miteinander kollidierten, seien die in Rede stehenden Rechte und Freiheiten gegeneinander abzuwägen. Nach Möglichkeit seien Modalitäten zu wählen, die diese Rechte und Freiheiten nicht verletzen.

Sollte es also doch einmal notwendig sein, Informationen über die Identität von Mitarbeitenden bereitzustellen, ist nach dem EuGH zuvor eine Abwägung zwischen dem Recht auf Auskunft der betroffenen Person und den Rechten und Freiheiten der anderen Personen vorzunehmen.

Des Weiteren hat er in diesem Urteil festgestellt, dass die DSGVO, die seit dem 25. Mai 2018 gilt, auch auf ein nach diesem Datum vorgebrachtes Auskunftsersuchen anwendbar ist, wenn die dieses Ersuchen betreffenden Verarbeitungsvorgänge vor dem Anwendungsdatum der DSGVO erfolgten.

Diese Konstellation ist auch im kirchlichen Bereich gar nicht so selten, dass nämlich Datenverarbeitungsvorgänge zu einem Zeitpunkt stattgefunden haben, in dem das KDG noch keine Geltung hatte. Eine ausdrückliche Vorschrift, die die rückwirkende Anwendung des KDG auf Sachverhalte aus der Zeit vor seinem Inkrafttreten normiert, fehlt.

„ Beschäftigte des Verantwortlichen sind nicht als Empfänger im Sinne der DSGVO anzusehen. “

Es ist mittlerweile aber wohl ständige Rechtsprechung der kirchlichen Datenschutzgerichte, dass sich deren Zuständigkeit nicht auf Anträge, deren zugrunde liegender Sachverhalt aus der Zeit seit dem Inkrafttreten von KDG und KDSGO herrührt, beschränkt. Vielmehr haben die Gerichte in ihren Beschlüssen klargestellt, dass sie auch für die Prüfung von Sachverhalten zuständig sind, die aus der Zeit vor dem 24. Mai 2018 stammen.

2.3.5 *Auskunftsanspruch braucht keine Begründung*

Schließlich hat der EuGH (Urteil vom 26. Oktober 2023, Az.: C-307/22) im Berichtszeitraum auch entschieden, dass ein Auskunftsantrag einer betroffenen Person keiner Begründung bedarf.

Dies hat beispielsweise zur Folge, dass ein Verantwortlicher keine Begründung mehr im Rahmen der Geltendmachung eines Auskunftsanspruchs verlangen kann und es somit nicht mehr möglich ist, ein solches Begehren mit dem Hinweis auf datenschutzfremde Zwecke abzuwehren. Das Gericht rechtfertigt die nicht notwendige Begründungspflicht mit dem Hinweis auf eine vom Gesetzgeber ausdrücklich gewollte einfache Ausübung der Rechte von betroffenen Personen.

In ihrem Urteil haben die Europarichter nicht nur entschieden, dass die Geltendmachung des Auskunftsanspruchs keiner Begründung bedarf, sondern darüber hinaus auch, dass die erste Auskunft nichts kosten darf.

Dies hat weitreichende Auswirkungen – vor allem im Bereich der Patientenakte. Denn nach § 630g Abs. 2 Satz 2 des Bürgerlichen Gesetzbuches (BGB) hat der Patient „dem Behandelnden die entstandenen Kosten zu erstatten“. Aber eine solche nationale Vorschrift kann für den EuGH das datenschutzrechtliche Auskunftsrecht nicht wirksam beschränken. Dies wäre nach den Ausführungen der Europarichter im Rahmen des Art. 23 DSGVO nur möglich, wenn die Beschränkung notwendig und verhältnismäßig ist und den Schutz der Rechte und Freiheiten anderer Personen sicherstellt. Darunter würden zwar grundsätzlich auch die wirtschaftlichen Interessen von Verantwortlichen wie zum Beispiel behandelnden Ärzten fallen. So habe der Unionsgesetzgeber die wirtschaftlichen Interessen der Verantwortlichen in Art. 12 Abs. 5 und Art. 15 Abs. 3 Satz 2 DSGVO berücksichtigt. Diese legen die Umstände fest, unter denen der Verantwortliche ein Entgelt für die Kosten der Zurverfügungstellung einer Kopie der personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, verlangen kann.

Dem nationalen Gesetzgeber sei es jedoch verwehrt, mit Blick auf den Schutz der wirtschaftlichen Interessen der Behandelnden eine nationale Regelung zu erlassen, die der betroffenen Person zum Schutz der wirtschaftlichen Interessen des Verantwortlichen die Kosten für eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung durch den Verantwortlichen sind, auferlegt. Dies würde die praktische Wirksamkeit des Rechts der betroffenen Person auf Auskunft über ihre personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, in Frage stellen.

Des Weiteren hat nach den Ausführungen des EuGH der Patient das Recht, eine vollständige Kopie der Dokumente zu erhalten, die sich in seiner Patientenakte befinden, wenn dies zum Verständnis der in diesen Dokumenten enthaltenen personenbezogenen Daten erforderlich ist. Das schließt Daten aus der Patientenakte ein, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten.

Ob dann allerdings der Verantwortliche wirklich die Kopie der kompletten Patientenakte unentgeltlich herausgeben muss oder im Rahmen des Auskunftsanspruchs nur Kopien der personenbezogenen Daten (aus der Patientenakte) wie es ausdrücklich im Gesetzestext von KDG und DSGVO heißt, werden wohl wieder die staatlichen oder kirchlichen Gerichte beantworten müssen.

2.3.6 Exzessive Auskunftserteilung?

Wie eine Auskunft auszusehen hat, steht nach einem klaren Urteil des Österreichischen Bundesverwaltungsgerichts (ÖBVwG, Entscheidung vom 3. August 2023, Az.: W101 2258430-1/33E) nicht zur Disposition des Betroffenen. Die Daten sind danach so zu beauskunften, wie sie beim Verantwortlichen gespeichert sind. Der Betroffene könne folglich nicht verlangen, dass die Daten vorher sortiert, gekürzt oder doppelte Informationen beseitigt werden, die im Original auch so vorliegen.

Im vorliegenden Fall sah sich der Betroffene in seinem Recht auf Auskunft verletzt, weil er „zu umfangreiche“ Informationen hinsichtlich seiner verarbeiteten Daten erhalten habe. Dem folgten die österreichischen Verwaltungsrichter nicht und sahen folglich den Beschwerdeführer diesbezüglich nicht in seinem Recht auf Auskunft verletzt. Es genüge zur Wahrung des Rechtes auf Auskunft grundsätzlich, wenn der Beschwerdeführer eine vollständige Übersicht seiner personenbezogenen Daten in verständlicher Form erhalte.

Die Entscheidung wurde zwar in Österreich gefällt, da die Rechtsgrundlagen jedoch in der DSGVO zu finden sind, spielt das Urteil auch jenseits der Landesgrenzen eine Rolle und dient als Auslegungs- und Anwendungshilfe für den europäischen Datenschutz. Der Richterspruch hat auch eine große praktische Bedeutung vor allem bei umfangreichen Auskunftsbegehren wie im zugrunde liegenden Fall. Die katholische Datenschutzaufsicht hat sich ebenfalls immer wieder mit Fällen extrem umfangreicher Auskünfte zu beschäftigen, in denen beispielsweise auch Doppelungen bemängelt wurden.

Darüber hinaus hat das Gericht in seinem Urteil entschieden, dass nach der DSGVO eine betroffene Person keinen subjektiven Rechtsanspruch auf Benennung eines Datenschutzbeauftragten hat und es ihr folglich auch nicht zusteht, ein Auskunftsbegehren vom jeweiligen Datenschutzbeauftragten und nicht vom Verantwortlichen beantwortet zu bekommen.



2.4 Wichtige Entscheidungen der katholischen Datenschutzgerichte

2.4.1 Zweckwidriges Zitieren aus einer Personalakte

Ein Sportlehrer an einer katholischen Schule ist erfolgreich gegen das Verlesen eines über 30 Jahre alten Empfehlungsschreibens anlässlich seiner Einstellung in den Schuldienst im Rahmen eines Personalgesprächs vorgegangen. Vorgelesen hatte die – durchaus positive – Bescheinigung eines Universitätsprofessors aus der Personalakte eine Schulleiterin im Beisein des Lehrers und seiner Vertrauensperson sowie des Schulleiters, der dieses Schreiben in der Personalakte bisher nicht zur Kenntnis genommen hatte.

Der Lehrer sah darin – anders als die Verantwortliche und die Datenschutzaufsicht, die über die Beschwerde zu entscheiden hatte, – eine zweckwidrige Verarbeitung, in die er nicht, auch nicht konkludent, eingewilligt habe.

„ ... [...] im Verlesen des Schriftstücks während eines [...] durchgeführten Personalgesprächs Jahrzehnte nach Abschluss des Bewerbungsverfahrens und ohne Bezug dazu [läge] datenschutzrechtlich eine (neuerliche) Verwendung der Daten. “

Für das Datenschutzgericht (Beschluss vom 31. Mai 2023, Az.: IDSG 24/2020) ist der Lehrer durch die zweckwidrige Datenverarbeitung in Form der Verwendung des Schreibens durch das Vorlesen in seinen Datenschutzrechten verletzt worden. Die darin liegende Verarbeitung personenbezogener Daten war für das IDSG unbefugt im Sinne des § 5 S. 1 KDG, weil kein Rechtmäßigkeitsgrund nach § 6 Abs. 2 oder 4 KDG vorgelegen habe.

Die naheliegende Frage des aufmerksamen Lesers, dass der Schulleiter als Vorgesetzter ja womöglich berechtigt war, Einsicht in die Personalakte zu nehmen und so rechtmäßig Kenntnis von der Bescheinigung zu erlangen, beantwortet sich bei der weiteren Lektüre der Entscheidungsgründe. Nach Überzeugung des IDSG hätte die Bescheinigung schon längst aus der Akte entfernt werden müssen. Sie mag für die Begründung des Beschäftigungsverhältnisses gemäß § 53 KDG erforderlich gewesen sein, aber sicherlich nicht für dessen Durchführung, so die Richter. Die Verwendung habe lediglich „der Anreicherung“ des Gesprächs gedient.

Im Übrigen bleibt das IDSG auch im Rahmen dieser Entscheidung seiner Linie treu und sieht auch vorliegend die Schulstiftung als Rechtsträgerin der Schulverwaltung als Verantwortliche an und nicht etwa die Schulleiterin, die in dem streitbefangenen Personalgespräch für diese gehandelt hat.

2.4.2 Verarbeitung sensibler Daten zum Schutz lebenswichtiger Interessen

In einem weiteren Fall im Berichtszeitraum hatte das IDSG (Beschluss vom 28. Februar 2023, Az.: IDSG 08/2020) unter anderem darüber zu entscheiden, was denn konkret „lebenswichtige Interessen“ sind, die gemäß § 11 Abs. 2 lit. c) KDG die Verarbeitung besonderer Kategorien personenbezogener Daten erlauben.

Nach der genannten Vorschrift ist eine Verarbeitung sensibler Daten ausdrücklich nicht untersagt, wenn die Verarbeitung „zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich“ ist und die betroffene Person „aus körperlichen oder rechtlichen Gründen außerstande“ ist, „ihre Einwilligung zu geben“.

Im zugrunde liegenden Fall wurde der damals noch minderjährige Betroffene beim Antragsgegner palliativ versorgt. Die Mitarbeitenden dieses Palliativdienstes hatten jedoch Zweifel bezüglich der von den Eltern des Betroffenen mitgeteilten Diagnose „ALS“ und der Medikation. Sie recherchierten daraufhin ohne Einwilligung oder Schweigepflichtentbindung die Krankengeschichte bei den zuvor behandelnden Ärzten. Sie schätzten seinen Zustand als akut lebensbedrohlich ein, brachen die bisherige Behandlung ab und veranlassten die stationäre Krankenhausaufnahme.

Das Datenschutzgericht sieht die medizinischen Recherchetätigkeiten der Beschäftigten als datenschutzrechtlich zulässig an. Die Datenrecherche sei zum Schutz lebenswichtiger Interessen des Antragstellers erforderlich gewesen. Zur Abwendung der akuten Lebensgefahr habe dieser Erkenntnisstand „aus der hier maßgeblichen ex-ante-Sicht“ geboten, unverzüglich zunächst die medizinische Diagnose abzuklären. Der Betroffene sei aufgrund seiner Minderjährigkeit außerstande gewesen, seine Einwilligung zu geben, die Einholung der Einwilligung bei seinen Sorgeberechtigten sei „zum Scheitern verurteilt“ gewesen und eine Ersetzung der Einwilligung durch das Familiengericht wäre nach Darstellung der Richter wohl zu spät gekommen.

Da soweit ersichtlich zu dieser Ausnahmeregelung kaum Rechtsprechung ergangen ist, ist die Entscheidung des IDSG als Hilfe zur Auslegung des Rechtsbegriffs „lebenswichtige Interessen“ – ob im KDG oder in der DSGVO – zu begrüßen.

Den Ausnahmecharakter („Ultima Ratio“) dieses Zulässigkeitstatbestands in Art. 9 Abs. 2 lit. c) DSGVO, dem § 11 Abs. 2 lit. c) KDG entspricht, stellt auch ErwG 46 zur DSGVO klar, wonach personenbezogene Daten nur dann aufgrund eines lebenswichtigen Interesses verarbeitet werden sollten, „wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann“.

Darüber hinaus ging es im vorliegenden Verfahren noch um eine nicht zeitgerechte und nicht vollständige Auskunft über die Daten in einer Patientenakte.

ErwG 46 zur DSGVO – lebenswichtiges Interesse

Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.

Im von Prof. Dr. Gernot Sydow herausgegebenen Kommentar zum Kirchlichen Datenschutzrecht (1. Auflage, 2021) heißt es zur Definition der „lebenswichtigen Interessen“ in § 11 Abs. 2 lit. c) KDG (Rn. 18): „Lebenswichtige Interessen sind solche existenzieller Natur. Dabei muss nicht konkrete Lebensgefahr vorliegen. Demgegenüber reicht bloße Nützlichkeit nicht aus. Auch nicht, dass die Datenverarbeitung objektiv vorteilhaft oder allgemein gesundheitsfördernd ist. Lassen sich die lebenswichtigen Interessen der betroffenen Person auf anderem Wege vergleichbar effektiv schützen, ist die Verarbeitung nicht erforderlich und damit unzulässig.“

2.4.3 Gerichtliche Kassationsbefugnis – deutliche Kritik an KDSGO

In der zweiten Instanz hatte sich das Datenschutzgericht der Deutschen Bischofskonferenz (DSG-DBK, Beschluss vom 8. Februar 2023, Az.: DSG-DBK 02/2022) im Berichtszeitraum unter anderem mit der Weitergabe eines Visitationszwischenberichts an Dritte zu beschäftigen. Das Gericht nutzte die Gelegenheit, um ausgiebig Schelte an der Kirchlichen Datenschutzgerichtsordnung (KDSGO) zu üben.

In der Sache selbst hat das DSG-DBK – zum ersten Mal übrigens nach einer mündlichen Verhandlung – wie schon die Vorinstanz entschieden, dass die Weitergabe des Zwischenberichts, der personenbezogene Daten enthalten hat, durch die Visitatoren an die befragten Dritten datenschutzwidrig war. Verantwortlich hierfür war nach Überzeugung der Richter der Erzbischof, der den Auftrag zur Visitation erteilt hat.

Bereits an dieser Stelle sah sich das Gericht gefordert, auf die Verantwortlichkeit des Bischofs näher einzugehen. Denn der vorliegende Sachverhalt unterscheidet sich von

den üblicherweise diskutierten, unstrittigen Konstellationen dadurch, dass der Auftrag zur Visitation nicht durch eine juristische Person – etwa das Erzbistum – erteilt worden ist, sondern durch den Erzbischof, weil Visitationsbefugnisse nach can. 396 ff. CIC kirchenrechtlich stets dem Bischof und nicht der Diözese zukommen. Da der Erzbischof hier über Mittel und Zwecke der Datenverarbeitung zu Zwecken der Visitation entscheiden konnte, sei er als datenschutzrechtlich Verantwortlicher anzusehen.

Einen Mitarbeiterexzess haben die Richter ausgeschlossen und mit dem Hinweis versehen, dass es in diesem Fall gar nicht zuständig wäre.

Des Weiteren beschäftigte sich das Gericht mit der grundsätzlichen Frage, ob die kirchlichen Datenschutzgerichte überhaupt befugt sind, rechtswidrige Verfügungen der kirchlichen Datenschutzaufsichten aufzuheben.

Das entspreche zwar der „mittlerweile gefestigten und zutreffenden Rechtsprechung des Interdiözesanen Datenschutzgerichts“. Die Frage der gerichtlichen Aufhebungsbefugnis habe aber „in der nur 18 Paragraphen umfassenden KDSGO keine ausdrückliche Regelung gefunden“. Die KDSGO sei für eine Prozessordnung ausgesprochen kurz und regle zahlreiche Fragen nicht ausdrücklich, „ohne anzuordnen, auf welches Regelwerk subsidiär bei fehlender Normierung in der KDSGO zurückzugreifen“ sei, so die deutliche Kritik der DSG-DBK-Richter.

Hinzu komme, dass § 14 Abs. 2 KDSGO auch keine explizite Tenorierungsmöglichkeit in Bezug auf eine Feststellung der Rechtswidrigkeit einer Entscheidung der Datenschutzaufsicht verleihe. § 14 Abs. 2 lit. c) KDSGO ermöglicht ausdrücklich nur die „Feststellung des Vorliegens und des Umfangs einer Datenschutzverletzung“. Die Datenschutzgerichte könnten die ihnen übertragene Aufgabe aber nur wahrnehmen, wenn § 14 Abs. 2 KDSGO nicht abschließend sei.

Und diese Regelungsabstinenz setze sich für die Entscheidungsbefugnis des DSG-DBK in Bezug auf erstinstanzliche Entscheidungen fort. Wenn aber in der Praxis die zweite Instanz unstreitig Entscheidungen der ersten Instanz auch ohne explizite KDSGO-Regelung aufheben könne, müsse das erst recht für eine Aufhebungsbefugnis für rechtswidrige Entscheidungen der Datenschutzaufsicht gelten. „Sonst müssten die Befugnisse des Datenschutzgerichts der Deutschen Bischofskonferenz gegenüber einem kirchlichen Gericht weitergehend sein als gegenüber einer kirchlichen Behörde – eine Wertung, die kaum verständlich wäre.“ Das Gericht stützt seine Argumentation auch auf die Präambel zur KDSGO: Danach soll die Ordnung einen wirksamen gerichtlichen Rechtsschutz im Einklang mit der DSGVO schaffen, also deren Rechtsschutzstandard nicht unterschreiten – und folglich eine Aufhebungsbefugnis umfassen.

3 Schwerpunkte der Tätigkeiten im Berichtszeitraum

3.1 Datenschutzverletzungen

Im Vergleich zum Vorjahr ist die Zahl der gemeldeten Datenschutzverletzungen nahezu gleichgeblieben, in einzelnen Bereichen war ein Anstieg der Meldungen zu verzeichnen: Die Meldungen aus dem Gesundheitswesen haben um ca. 30 % zugenommen, die Zahl der Datenschutzverletzungen im schulischen Umfeld hat sich verdreifacht.

Neben dem „Allzeit-Klassiker“, dem Versand von E-Mails mit einem offenen Verteiler, wurde auch im Berichtszeitraum die Offenlegung personenbezogener Daten durch die unterschiedlichsten Verluste gemeldet: Krankenakten, Diensthandys, ärztliche Verordnungen, Laptops, Kita-Aufnahmehefte wurden gestohlen oder gingen verloren. Auch Einbrüche in Kindertagesstätten einhergehend mit dem Diebstahl von Laptops oder Kameras wurden oft gemeldet, was einmal mehr die Notwendigkeit der Verschlüsselung der Endgeräte bzw. die Speicherung von personenbezogenen Daten möglichst nicht auf lokalen Speichermedien deutlich macht.

„ Die Meldungen aus dem Gesundheitswesen haben um ca. 30 % zugenommen, die Zahl der Datenschutzverletzungen im schulischen Umfeld hat sich verdreifacht. “

Unter anderem wurde auch der Verlust eines Diensthandys gemeldet, das gestohlen wurde, während der rechtmäßige Besitzer in der Straßenbahn Erste Hilfe leistete – eine wahrhaft traurige Meldung.

Die auf dem Weg zum Bäcker einem offensichtlich hungrigen Lehrer aus der Hosentasche gefallenen Abiturprüfungslisten dagegen sind ganz ohne fremdes Zutun abhandengekommen – hier stellte sich allerdings die Frage, ob das Mitführen der Listen in der Hosentasche eine geeignete technische Maßnahme zum Schutz der personenbezogenen Daten darstellt, was von der Aufsichtsbehörde mit einem klaren „Nein“ beantwortet wurde.

Erneut gab es Meldungen zu Fotos oder Videos von Kindern oder hilfebedürftigen Personen, die im WhatsApp-Status oder auch auf TikTok eingestellt und somit verbreitet wurden. Neben den datenschutzrechtlich zu ergreifenden Maßnahmen schlossen sich in diesen Fällen meist auch arbeitsrechtliche Konsequenzen durch die Verantwortlichen an.

Auch wenn für die Meldung einer Datenschutzverletzung im KDG eine Frist von 72 Stunden festgeschrieben ist, so lässt das Kath. Datenschutzzentrum Frankfurt/M. doch Milde walten, wenn der verzögerte Eingang der Meldung mit dem Besuch einer „familiären Rüstzeit im Kloster“ begründet wird – Ehrlichkeit muss belohnt werden.

Und auch tatkräftiges Handeln zur Behebung einer entstandenen Datenschutzverletzung und zur Verhinderung weiteren Ungemachs war zu verzeichnen: Ein an eine falsche Faxnummer versendetes Fax, das personenbezogene Daten enthielt, wurde nach dem

Bemerken des Fehlers binnen Minuten vom Verursacher beim falschen Empfänger, einem nahe gelegenen Supermarkt, persönlich abgeholt, sodass die Einsichtnahme unbefugter Dritter ausgeschlossen werden konnte.

Hinsichtlich der Meldungen von Datenschutzverletzungen ist diesseits im Berichtszeitraum besonders die Häufung von Datenpannen bei IT-Dienstleistern, ebenso bei Dienstleistern dieser Dienstleister, ins Auge gefallen – sei es durch Hackerangriffe oder Nachlässigkeiten vor Ort. Diese hatten für die Verantwortlichen, also die Auftraggeber, teils gravierende Folgen. So blieben beispielsweise zahlreiche digitale Infotafeln an Schulen schwarz und das über einen längeren Zeitraum.

3.1.1 Private Handynummer auf Abwegen

Die Möglichkeit, die Mobilfunknummer einer Frau zu erhalten, ohne diese im direkten Kontakt darum zu bitten, hat der Mitarbeiter einer Krankenhausrezeption genutzt, indem er die Handynummer aus den ihm vorliegenden Aufnahmeunterlagen der Patientin entnahm. Nachdem die Patientin die ambulante Notfallaufnahme wieder verlassen hatte, sendete der Krankenhausmitarbeiter ihr eine Kurznachricht, in der er um ein persönliches Treffen bat. Die Patientin informierte die Klinik über diesen Vorfall, der Verantwortliche leitete arbeitsrechtliche Maßnahmen gegen den betreffenden Mitarbeiter ein – und diese unberechtigte Nutzung der ihm zur Kenntnis gelangten personenbezogenen Daten nahm für diesen kein gutes Ende.

3.1.2 Videoüberwachung? – Hier bestimmt nicht!

In einer Kindertagesstätte wurde in der Personaltoilette unter dem Waschbecken und direkt gegenüber dem Toilettenbecken eine dort fest installierte Kamera gefunden, die auch eine Speicherkarte enthielt. Diese massive Datenschutzverletzung wurde dem Kath. Datenschutzzentrum Frankfurt/M. gemeldet, gleichzeitig wurde Strafanzeige bei der Polizei gestellt. Die Ermittlungsarbeiten der Polizei waren erfolgreich, der Täter konnte ermittelt und überführt werden.

Bei diesem sehr unschönen Vorfall waren neben den datenschutzrechtlichen Aspekten vor allem auch arbeits- und strafrechtliche Bereiche betroffen, die durch den Arbeitgeber bzw. durch die polizeilichen und staatsanwaltlichen Ermittlungen verfolgt wurden. Der Täter erhielt die fristlose Kündigung, darüber hinaus sind strafrechtliche Folgen zu erwarten. Die datenschutzrechtlichen Aspekte traten hinter diesen Maßnahmen zurück. Für den Verantwortlichen ergaben sich keine weiteren Konsequenzen oder Handlungserfordernisse, denn das Verhalten des Täters musste er sich nicht zurechnen lassen.

3.1.3 *Hinter den Kulissen einer fachgerechten Abfallentsorgung*

Tiefe Einblicke bekommt die Datenschutzaufsicht im Laufe der Zeit auch in die Müllentsorgung vornehmlich im Krankenhausbereich durch die oftmals äußerst detailreichen und offensichtlich in vielen Bereichen kundigen betrieblichen Datenschutzbeauftragten bzw. -koordinatorinnen und -koordinatoren. Landeten vor einiger Zeit beispielsweise heikle Streitakten im herkömmlichen Müll, so waren es im Berichtszeitraum Patientenakten,



die versehentlich mit schnödem gewöhnlichem Abfall entsorgt wurden – obwohl deren Vernichtung streng geregelt ist. Um das geringe Risiko für die enthaltenen personenbezogenen Daten zu untermauern, wurde das Verpressen des Mülls so anschaulich beschrieben, dass für die Datenschutzaufsicht glaubwürdig nachvollziehbar wurde, dass selbst außerordentlich neugierigen Zeitgenossen der Spaß am Lesen von mit allerlei auch durchaus unappetitlichem Unrat verpresstem Papier vergehen dürfte. Aber auch die kenntnisreiche Schilderung des Abtransports des Inhalts der Restmüllpresscontainer mit Lastwagen und deren maschinelle Umlagerung auf Güterzüge bis zum letzten Bestimmungsort wurde von den Mitarbeiterinnen und Mitarbeitern gerne und interessiert gelesen und bearbeitet.

3.1.4 *XS, M oder XXL – wer trägt was?*

Gemeinsam an sportlichen Veranstaltungen wie Firmenläufen teilzunehmen, ist für viele Unternehmen und Institutionen mittlerweile fester Bestandteil von Team-Building-Prozessen. Ob die Offenlegung der Geburtsdaten und der Konfektionsgrößen sämtlicher Teilnehmenden gegenüber allen anderen der Förderung des Gemeinschaftsgefühls zuträglich ist, scheint jedoch fraglich. Deshalb wurde dieser Vorfall der Aufsichtsbehörde als Datenschutzverletzung gemeldet. Der Verursacher wurde noch einmal datenschutzrechtlich belehrt. Aus dem Kreis der Betroffenen gab es zwar keine Rückmeldungen, was am Vorliegen einer Datenschutzverletzung jedoch nichts ändert.

3.2 Beschwerden

Anders als die relativ konstant gebliebene Anzahl der gemeldeten Datenschutzverletzungen war die Zahl der Beschwerden im Jahr 2023 leicht rückläufig. Ein nicht unerheblicher Teil der Beschwerden bezog sich auf unzureichend erteilte Auskunftersuchen, bei ca. 30 % der Beschwerden handelte es sich um Vorfälle aus dem Krankenhausumfeld.

3.2.1 *Nachwirkungen von Corona*

Corona hat seinen pandemischen Schrecken bereits seit über einem Jahr verloren, dennoch wirken sich manche in dieser Zeit etablierten Maßnahmen bis heute aus – und das nicht immer positiv.

Für den Besucher einer Notfallambulanz war die seit der Corona-Pandemie vor der Anmeldung angebrachte Plexiglasscheibe Grund für eine Beschwerde beim Kath. Datenschutzzentrum Frankfurt/M. Die Plexiglasscheibe, die an der Anmeldung einst als Infektionsschutz zwischen Mitarbeiter und Patient installiert worden war, wirkt sich hinderlich auf die Verständigung aus, sodass eine datenschutzkonforme Übermittlung der notwendigerweise an der Anmeldung zu erhebenden personenbezogenen Daten bis heute nicht möglich ist. Erschwerend kommt hinzu, dass sich der Warteraum für die Patienten in unmittelbarer Nähe und damit in Hörweite befindet. Der durch die Beschwerde und die Einschaltung der Aufsichtsbehörde auf den Missstand aufmerksam gewordene Verantwortliche konnte durch die Änderung kleinerer technischer und organisatorischer Maßnahmen für Abhilfe sorgen: Die Patientenaufnahme wurde in einen administrativen an der Anmeldung stattfindenden und einen inhaltlichen in einem separaten Raum stattfindenden Teil getrennt. Zudem wird die Tür des Warteraums von der Milchglasfolie befreit und kann damit zukünftig geschlossen bleiben, jedoch trotzdem die Einsichtnahme für die Beschäftigten ermöglichen. Einmal mehr hat sich hier gezeigt, dass auch kleine Maßnahmen große Wirkung zeigen können.

” Auch kleine Maßnahmen können große Wirkung zeigen. “

3.2.2 *Auch ohne Einwilligung kann die Weitergabe von Gesundheitsdaten rechtmäßig sein*

Der Vater eines in einer Kindertagesstätte betreuten Kindes sah in der Weitergabe eines ärztlichen Attests an das zuständige Gesundheitsamt eine Datenschutzverletzung und reichte eine Beschwerde bei der Aufsichtsbehörde ein.

Gemäß § 33 Infektionsschutzgesetz (IfSG) dürfen in Gemeinschaftseinrichtungen nur Personen betreut werden, die unter anderem entweder einen ausreichenden Impfschutz gegen Masern aufweisen oder aufgrund einer medizinischen Kontraindikation nicht geimpft werden können.

Dem vorgelegten Attest sollte die Kontraindikation zum gesetzlich nachzuweisenden Masern-Impfschutz zu entnehmen sein, es genügte jedoch den gesetzlichen Vorgaben des IfSG nicht. Im IfSG ist als Folge die Übermittlung des Attests an das Gesundheitsamt vorgesehen, eine Einwilligung des Betroffenen ist weder erforderlich noch gesetzlich festgelegt.

Die Beschwerde wurde abgewiesen.

3.2.3 Erzieherin ist im Krankenstand auf unbestimmte Zeit – sollten das alle Eltern erfahren?

Die Eltern der Kinder einer Kita-Gruppe über das längere Fehlen einer Erzieherin durch einen Elternbrief zu informieren, ist sicherlich gängige Praxis und auch sinnvoll. Den Grund für das Fehlen anzugeben, erscheint dagegen nicht notwendig und stellt aus datenschutzrechtlicher Sicht sogar durchaus einen Grund zur Beschwerde bei der Aufsichtsbehörde dar – erst recht, wenn es sich dabei um eine Langzeiterkrankung mit ungewissem Rückkehrdatum handelt. Darüber hinaus stellt die im Elternbrief erläuterte Mitteilung auch eine meldepflichtige Datenschutzverletzung gemäß KDG dar.

Der Beschwerde wurde stattgegeben und der Verantwortliche erhielt wegen dieses Verstoßes gegen das KDG einen entsprechenden Bescheid.

3.2.4 Unscharfe Trennung von Arbeit und Privatem

Gleich zu Beginn des Berichtszeitraums erreichte das Kath. Datenschutzzentrum Frankfurt/M. über eine Landesdatenschutzaufsicht eine Beschwerde – wie so oft aus dem Gesundheitsbereich. Eine Mutter teilte mit, dass eine Mitarbeiterin in einem Krankenhaus Gesundheitsdaten ihrer dort behandelten Tochter an den nicht sorgeberechtigten Vater herausgegeben habe, obwohl sie bereits bei der stationären Aufnahme darauf hingewiesen habe, dass diese Mitarbeiterin die neue Freundin des Kindsvaters sei. Als die Mitarbeiterin ihren Lapsus bemerkte, erreichte die Datenschutzverletzung im weiteren Verlauf auch die katholische Datenschutzaufsicht in Frankfurt/M. In der Meldung wies der Verantwortliche ebenfalls auf die arbeitsrechtlichen Konsequenzen für die neue Freundin des nicht sorgeberechtigten Vaters hin. Die Weitergabe von sensiblen Gesundheitsdaten ohne irgendeine einschlägige Rechtsgrundlage stellt einen schweren Datenschutzverstoß dar und blieb auch in diesem Fall nicht ohne Folgen.

Der Beschwerde wurde stattgegeben und der Verstoß in einem mit Anordnungen versehenen Bescheid beanstandet.

3.3 Anfragen

Im Berichtszeitraum ist die Anzahl der Anfragen um ca. 25 % zurückgegangen. Eine Tendenz zu vorherrschenden Themen oder Themenbereichen war nicht festzustellen. Die Themen der im Kath. Datenschutzzentrum Frankfurt/M. eingegangenen Anfragen reichten von A wie Auskunftersuchen über C wie Cloudsoftware, D wie Data Privacy Framework und Ö wie Ökumenische Notfallseelsorge bis hin zu S wie Sozialdaten und V wie Videoüberwachung. Darüber hinaus gingen auch Nachfragen zur Bestellung eines betrieblichen Datenschutzbeauftragten und zum konkreten Einsatz von Apps oder Software ein.

Eine Anfrage zum Einsatz eines neuen mobilen Datenerfassungssystems im Rahmen der häuslichen Altenpflege zeigte einmal mehr sehr deutlich, wie wichtig die frühzeitige Beachtung der datenschutzrechtlichen Vorgaben bei der Entwicklung und Implementierung neuer Arbeitsprozesse und der zugehörigen Softwareprodukte ist.

Zudem ist zu konstatieren, dass nicht jede Anfrage mit einer kurzen E-Mail oder einem Telefonat zu erledigen ist.

3.4 Gerichtsverfahren

In dieser Hinsicht war 2023 glücklicherweise ein eher ruhiges Jahr. Es sind keine Klagen gegen Bescheide des Kath. Datenschutzzentrums Frankfurt/M. hinzugekommen. Nach Abschluss bzw. Erledigung einiger Klagen in erster Instanz sind nunmehr mit Stand Ende Dezember 2023 lediglich noch drei Verfahren beim IDSG anhängig. In diesen geht es unter anderem um gesetzliche Grundlagen zu Löschfristen in kirchlichen Einrichtungen und nach wie vor um den Einsatz von Microsoft 365 an katholischen Schulen.

Allerdings sind zwei Verfahren mittlerweile eine Etage höher gewandert und warten in zweiter Instanz beim DSG-DBK auf entsprechende Richtersprüche. In einem der beiden Verfahren hat das IDSG einen Bescheid der Datenschutzaufsicht bestätigt, was den Antragsteller nicht davon abgehalten hat, auch die nächste Instanz anzurufen, um den Bescheid doch noch aus der Welt zu schaffen. Das gesamte Verfahren zieht sich bereits über mehrere Jahre hinweg, aber es ist das gute Recht des Klägers, den Rechtsweg umfänglich auszuschöpfen. Im zweiten Verfahren vor dem DSG-DBK lässt das Kath. Datenschutzzentrum Frankfurt/M. eine Entscheidung des IDSG überprüfen, die – so sie wider Erwarten Rechtskraft erlangen sollte – weitreichende Konsequenzen für kirchliche Datenschutzaufsichten mit sich brächte.

3.5 Prüfungen

Im Berichtszeitraum wurden die Tiefenprüfungen von katholischen Kindertagesstätten weiter fortgesetzt. Es fanden wieder Vor-Ort-Prüfungen in den Einrichtungen statt und ein Großteil der durchgeführten Prüfungen von Kitas und Kita-Verwaltungs-GmbHs konnte meist zur Zufriedenheit aller Beteiligten abgeschlossen werden. Ab und an waren umfangreichere Nachbesserungen und deren Nachweis nötig, die den Abschluss der einen oder anderen Prüfung etwas verzögert haben – was aber im Sinne einer konstruktiven Zusammenarbeit und einer angestrebten tatsächlichen Verbesserung des Datenschutzes vor Ort absolut in Ordnung war.

Anlassbezogene Prüfungen beispielsweise von Websites wurden weitergeführt und einige konnten abgeschlossen werden.



Neu geprüft wurde im zweiten Halbjahr 2023 ein kompletter Caritasverband. Die anlasslose datenschutzrechtliche Prüfung fand dank einer gründlichen Vorbereitung auf beiden Seiten in einer nach Aussage der teilnehmenden Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. ausgesprochen freundlichen Atmosphäre statt. Lediglich die abschließende Bewertung der nachgereichten Dokumente und einiger notwendiger Nacharbeiten stehen nunmehr in 2024 noch aus.

Hintergrund der regelmäßigen Prüfungen durch die Datenschutzaufsicht ist die gesetzliche Vorgabe, über die Einhaltung der datenschutzrechtlichen Vorschriften zu wachen und sich hiervon gemäß § 44 Abs. 2 lit. c) KDG gegebenenfalls durch Vor-Ort-Prüfungen zu überzeugen.

4 Veranstaltungen und Öffentlichkeitsarbeit

Trotz umfangreicher Umzugsaktivitäten inklusive Einsegnungsfeier, die das Jahr 2023 des Kath. Datenschutzzentrums Frankfurt/M. wesentlich prägten, konnten wieder Schulungs- und Fortbildungsveranstaltungen angeboten und durchgeführt werden.

So fanden auch die jährlichen Austauschtreffen mit den betrieblichen Datenschutzbeauftragten der (Erz-)Bischöflichen Ordinariate sowie der Diözesancaritas- und Fachverbände mit zahlreichen Teilnehmerinnen und Teilnehmern wieder statt. Diese regelmäßigen Begegnungen bilden eine wichtige Basis für ein konstruktives Miteinander in der täglichen Zusammenarbeit.

In den gut besuchten Veranstaltungen hielten Mitarbeiterinnen und Mitarbeiter der Datenschutzaufsicht aktuelle Vorträge zur kirchlichen Gerichtsbarkeit in Datenschutzsachen mit ausgewählten Beispielen der Spruchpraxis des IDSG und des Datenschutzgerichts 2. Instanz vor allem im Hinblick auf das Auskunftsrecht, die ordnungsgemäße Anhörung, die konkludente Einwilligung sowie auf die Verantwortlichkeit und den sogenannten Mitarbeiterexzess. Ein weiterer Vortrag beschäftigte sich eingehend mit dem Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework.

Im Anschluss an die Treffen bot sich den Teilnehmerinnen und Teilnehmern die Gelegenheit, die neuen Räumlichkeiten des Kath. Datenschutzzentrums Frankfurt/M. schon einmal zu besuchen. Wegen verzögerter Möbellieferungen konnten die Veranstaltungen noch nicht in den neuen Schulungsräumen am Frankfurter Roßmarkt stattfinden.

Außerdem referierte die Leiterin des Kath. Datenschutzzentrums Frankfurt/M., Frau Ursula Becker-Rathmair, anlässlich eines Workshops der Bundeskonferenz der kirchlichen Archive in Deutschland im Würzburger Burkardushaus zu den datenschutzrechtlichen Herausforderungen im Archivalltag.

Die Mitarbeiterinnen und Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. nahmen im Berichtszeitraum ebenfalls Fortbildungsmöglichkeiten im Datenschutz und in der Informationstechnik wahr.

5 Vernetzung mit anderen Datenschutzaufsichten

Die gute Zusammenarbeit der fünf katholischen Datenschutzaufsichten setzte sich auch im Berichtszeitraum fort. Sprecher der Konferenz der Diözesandatenschutzbeauftragten war Matthias Ullrich von der Kirchlichen Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs.



Dr. Michaela Hermes, Datenschutz der katholischen Kirche im Spannungsfeld zwischen kirchlicher Selbstbestimmung und europäischem Datenschutzrecht, Hrsg.: Dirk Heckmann, 2023, Verlag Duncker & Humblot

Der Austausch mit den evangelischen Kolleginnen und Kollegen hat sich im Berichtszeitraum noch intensiviert, weil viele aktuelle datenschutzrechtliche Fragestellungen die evangelischen und katholischen Datenschutzaufsichten gemeinsam betreffen. Der jährliche Ökumenische Datenschutztag fand 2023 in Essen statt, was von den Teilnehmenden gerne zu einem äußerst aufschlussreichen und kurzweiligen Besuch der ehemaligen Zeche Zollverein inklusive Steigerführung mit Püttgeschichten genutzt wurde. Impressionen hiervon finden sich auf Seite 39. Für den Datenschutztag konnte Frau Dr. Michaela Hermes, stellvertretende betriebliche Datenschutzbeauftragte der Erzdiözese München und Freising, für einen Impulsvortrag zum Thema „Datenschutz der katholischen Kirche im Spannungsfeld zwischen kirchlicher Selbstbestimmung und europäischem Datenschutzrecht“ gewonnen werden, dem sich eine intensive Diskussion anschloss.

Außerdem wurde auf der Veranstaltung das Fallbeispiel zum Kirchlichen Datenschutzmodell (KDM) vorgestellt und dann auch veröffentlicht. Mit einem fiktiv gewählten Praxisbeispiel „Die Bildungs- und Entwicklungsdokumentation eines Kindes in einer Kindertagesstätte“ wird darin die Systematik und praktische Anwendung des Kirchlichen Datenschutzmodells dargestellt.

► [Zum Nachlesen](#)

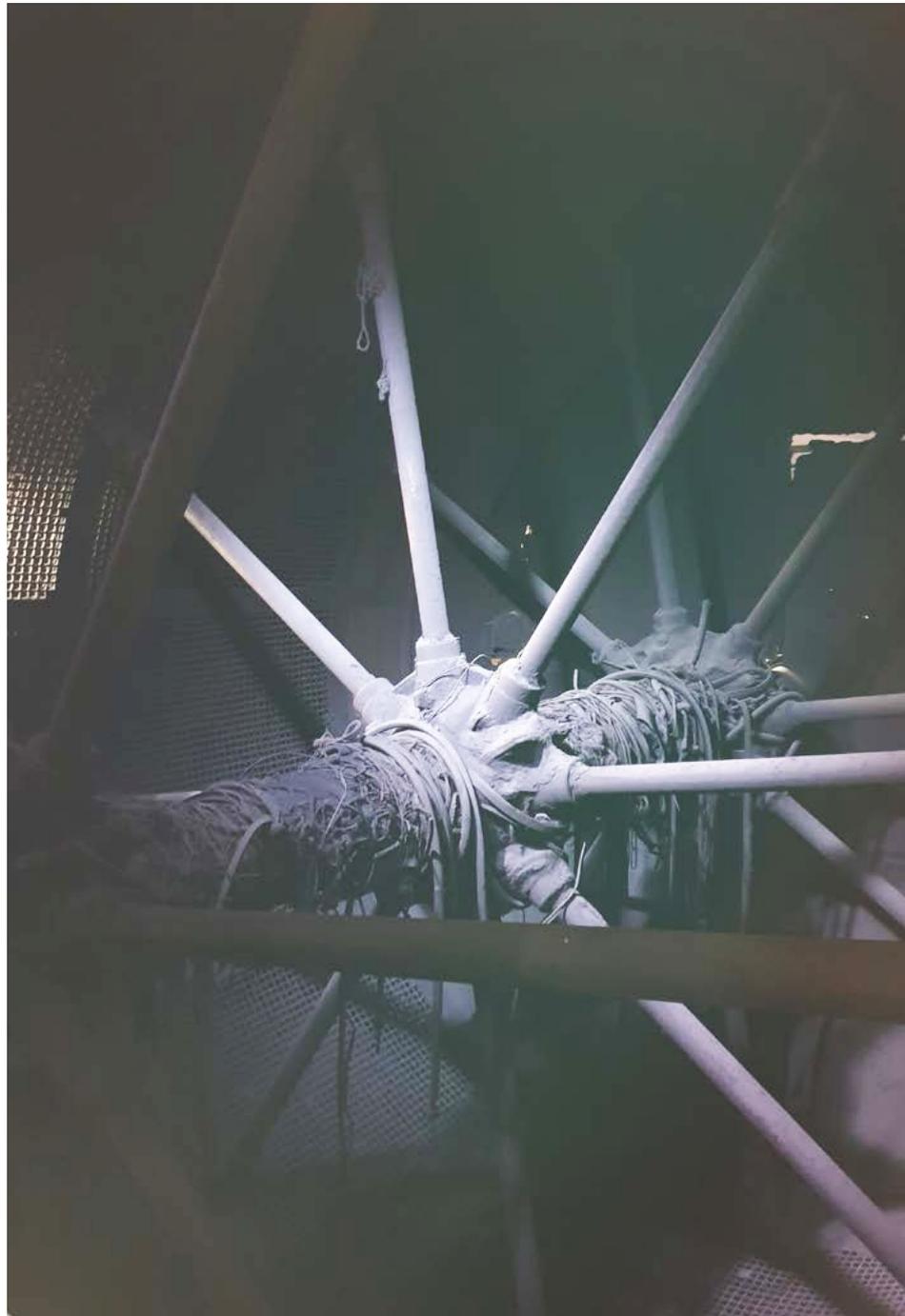


Weitere Informationen, Arbeitsdokumente und Erläuterungen zum KDM-Fallbeispiel finden sich unter nebenstehendem Link.

Wie schon im letzten Tätigkeitsbericht für das Jahr 2022 berichtet, nimmt ein Mitarbeiter des Kath. Datenschutzzentrums Frankfurt/M. am Arbeitskreis (AK) Gesundheit & Soziales der Datenschutzkonferenz (DSK) teil, dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Er berichtet – ebenso wie die anderen Vertreterinnen und Vertreter der katholischen Datenschutzaufsichten in anderen DSK-Arbeitskreisen – aus den AK-Sitzungen regelmäßig an die Konferenz der Diözesandatenschutzbeauftragten.

Impressionen

Die Zeche Zollverein war bis in die 1980er Jahre ein aktives Steinkohlebergwerk in Essen.



Die mächtige Siebtrommel in der Kohlenwäsche war ein wichtiger Baustein in der Kohleaufbereitung. Durch die Rotation der konischen Trommel wurde die Rohkohle, also die noch mit Gestein vermengte Kohle, nach Größe klassiert.

Die Heilige Barbara, Schutzpatronin der Bergleute, wachte über die Kumpel der Zeche Zollverein.

6 Hinweise des Kath. Datenschutzzentrums Frankfurt/M.

6.1 5 Jahre KDG – ein Grund zum Feiern!

Im Berichtsjahr 2023 hat das Kath. Datenschutzzentrum Frankfurt/M. seinen Einrichtungen im Zuständigkeitsbereich auch wieder praktische Hinweise zu aktuellen Datenschutzthemen auf seiner Website gegeben.

„ Grundrechte und Grundfreiheiten natürlicher Personen zu schützen – das ist die Aufgabe des Datenschutzes, dem in der Katholischen Kirche seit nunmehr fünf Jahren durch das Inkrafttreten des KDG am 24. Mai 2018 ein noch höherer Stellenwert zukommt. “

Das Gesetz über den Kirchlichen Datenschutz (KDG) ist am 24. Mai 2018, also vor genau fünf Jahren, in Kraft getreten.

Nötig wurde die Anpassung des bislang geltenden kirchlichen Datenschutzes durch europäische Vorgaben. Die Katholische Kirche hat die EU-Datenschutzgrundverordnung (DSGVO) aber nicht einfach übernommen, sondern durchaus eigene Akzente gesetzt und auch bekannte Elemente aus der Anordnung über den Kirchlichen Datenschutz (KDO) übernommen.

Anfangs musste sich das eine oder andere im kirchlichen Datenschutz noch etwas zurechtrücken, aber die meisten Befürchtungen haben sich nicht bewahrheitet.

Das KDG hat sich als Grundlage für katholische Einrichtungen zur Verarbeitung personenbezogener Daten bewährt und eröffnet kirchlichen Stellen neue Möglichkeiten, personenbezogene Daten rechtssicher zu nutzen. Das Gesetz gibt den Verantwortlichen vor Ort praktikable, aber auch den Datenschutzinstitutionen geeignete Instrumente und Lösungen an die Hand.

Grundrechte und Grundfreiheiten natürlicher Personen zu schützen – das ist die Aufgabe des Datenschutzes, dem in der Katholischen Kirche seit nunmehr fünf Jahren durch das Inkrafttreten des KDG am 24. Mai 2018 ein noch höherer Stellenwert zukommt.

6.2 Neue Grundlage für den Datentransfer mit den USA

Die Europäische Kommission hat mit Datum vom 10.07.2023 den Angemessenheitsbeschluss für das EU-US Data Privacy Framework angenommen. Mit diesem Angemessenheitsbeschluss, der die Nachfolgeregelung zum sog. Privacy Shield bestätigt, können nunmehr wieder Datenübermittlungen an zertifizierte Organisationen in den Vereinigten Staaten von Amerika erfolgen, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind. Es bleibt jedoch den Einrichtungen und kirchlichen Stellen überlassen zu prüfen, ob die betreffende Organisation über eine entsprechende vom U.S. Department of Commerce veröffentlichte Liste zertifiziert ist (diese Liste ist seit dem 17. Juli 2023 verfügbar).



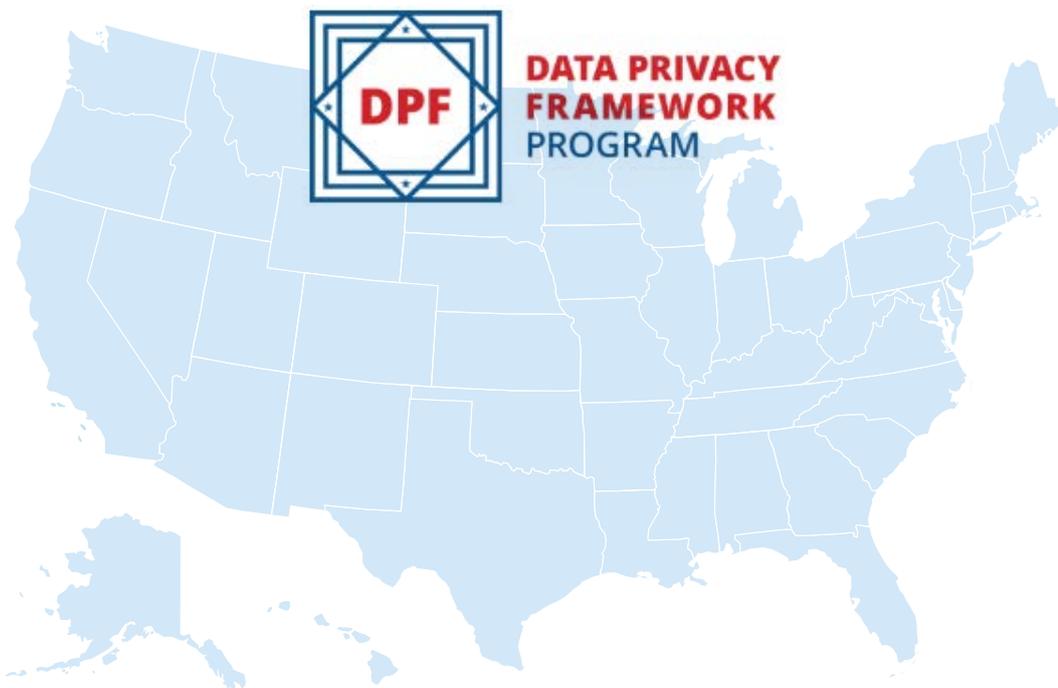
► [Data Privacy Framework List](#)

Es bleibt nun abzuwarten, ob diese Regelungen und der Angemessenheitsbeschluss einer möglichen neuerlichen gerichtlichen Überprüfung standhalten.

Eine ausführliche Darstellung zu diesem Themenkomplex findet sich in der Rubrik „Staatliche Gesetzgebung“ am Anfang dieses Tätigkeitsberichts (2.1.2).



► [Meldung des BfDi zum DPF](#)



7 Ausblick

Was den Standort und die Räumlichkeiten des Kath. Datenschutzzentrums Frankfurt/M. betrifft, so werden sich die bewegten Zeiten des Berichtsjahrs sicherlich nicht fortsetzen. Vielmehr können die anstehenden Aufgaben am neuen Standort – und mit noch einmal verstärktem Team – nun wieder in gewohnter Weise bewältigt werden.

Die Herausforderungen an sich werden zukünftig – so deutet es sich bereits an – weitere Bewegung mit sich bringen: Wie lange wird das EU-US Data Privacy Framework Bestand haben? Spannungsfeld KI und Datenschutz – was ist bereits durch die KI-Verordnung geregelt, was ist darüber hinaus gegebenenfalls noch regulierungsbedürftig? Werden perspektivisch digitale Bedrohungsszenarien wie Hackerangriffe oder Deepfakes unser Zusammenleben vermehrt bestimmen und wie kann dem unter Berücksichtigung des Datenschutzes begegnet werden?

Abseits dieser großen Themen gilt es selbstverständlich, die Integration des Datenschutzes in Konzepte, Denkweisen und Realisierungen von Projekten voranzutreiben. Ziel soll es weiterhin sein, den Datenschutz so in die Entwicklung und Gestaltung der Arbeitsprozesse einzubinden, dass er nicht ein isolierter, dem Prozess von außen zugeführter Teil, sondern ein vollständig integrierter und wesentlicher Bestandteil einer jeglichen Verarbeitung personenbezogener Daten ist.

Datenschutz ist spannend – und er wird es bleiben!

8 Die fünf Datenschutzaufsichten der Katholischen Kirche in Deutschland





**Kath. Datenschutzzentrum
Frankfurt/M.**
Tätigkeitsbericht 2023

