Katholische
Datenschutzaufsicht Nord

10. Jahresbericht

2023

Herausgegeben von

Katholische Datenschutzaufsicht Nord
Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg, der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.
Unser Lieben Frauen Kirchhof 20
28195 Bremen

Telefon: 0421 330056-0
E-Mail: info@kdsa-nord.de

Diesen Tätigkeitsbericht können Sie auch auf unserer Internetseite abrufen unter:
https://www.kdsa-nord.de/Jahresberichte

Sofern im Folgenden nur die männliche Bezeichnung gewählt wurde, so ist dies nicht geschlechtsspezifisch gemeint, sondern geschah ausschließlich aus Gründen der besseren Lesbarkeit.

Inhaltsverzeichnis

Vorwort

Nach vielen Jahren der guten Zusammenarbeit hat sich Herr Mündelein als ein sehr erfahrener und sehr geschätzter Kollege zum Ende des Jahres 2022 in den wohlverdienten Ruhestand verabschiedet. Für diese gemeinsamen Jahre, die konstruktiven und zum Teil auch kontroversen Diskussionen und auch das offene Ohr möchte ich mich herzlich bedanken und wünsche Herrn Mündelein und seiner Familie alles Gute für die Zukunft.

Nun kann ich meinen ersten Bericht für den Zeitraum vom 1. Januar 2023 bis zum 31. Dezember 2023 vorlegen. Zum 1. Januar 2023 bin ich als gemeinsamer Diözesandatenschutzbeauftragter für die norddeutschen (Erz-)Bistümer sowie das Bischöflich Münstersche Offizialat in Vechta für vier Jahre berufen worden. Für dieses mir entgegengebrachte Vertrauen bin ich sehr dankbar.

Gleich zu Beginn möchte ich auf die leichte Neugestaltung dieses Tätigkeitsberichts hinweisen. Eine Neuerung betrifft die „Hinweise“ zu einzelnen Themen. Mit diesen Hinweisen soll kurz die datenschutzrechtliche Relevanz der einzelnen Themen zusammengefasst und ggf. Hilfen zur Umsetzung oder Sensibilisierung gegeben werden. Eine weitere Neuerung betrifft die Neustrukturierung der Darstellung ausgewählter Fälle. Diese sind nun nicht mehr nach Beschwerden oder Datenschutzverletzungen gegliedert, sondern jeweils im Block für bestimmte Einrichtungen dargestellt. Es soll dabei jedoch nicht der Eindruck entstehen, dass beispielsweise der Einsatz einer Wildkamera oder der offene E-Mailverteiler ausschließlich ein Problem der Bistümer oder Kirchengemeinden sei.

Für kirchliche Einrichtungen haben sich wichtige Änderungen durch die Entwicklungen im europäischen Datenschutzrecht ergeben. Der bereits mehrfach durch den EuGH aufgehobene Angemessenheitsbeschluss in Bezug auf die Übermittlung personenbezogener Daten in die USA geht in die nächste Runde. Das nunmehr erlassene EU-U.S. Data Privacy Framework kann als Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in die USA herangezogen werden. Leider wird bei aller Freude über diese aus Sicht der Einrichtungen positive Entwicklung nicht immer gesehen, dass es auch andere Faktoren bei der Übermittlung von personenbezogenen Daten in Drittstaaten gibt. So ist ebenso die nach wie vor bestehende Zugriffsmöglichkeit auf die dort gespeicherten personenbezogenen Daten zu berücksichtigen. Auch die Datenverarbeitung zu (nicht zulässigen) eigenen Zwecken durch den Auftragsverarbeiter ist derzeit noch ein ungelöstes Problem.

Es werden zudem drei Entscheidungen des Europäischen Gerichtshofs dargestellt. Im Wesentlichen befassen sich die dargestellten Fälle mit den Auskunftsansprüchen von betroffenen Personen. Der EuGH hat entschieden, was der Begriff „Kopie“ von personenbezogenen Daten im Zusammenhang mit dem Auskunftsanspruch bedeutet. In einer weiteren Entscheidung

stellte der EuGH klar, dass die betroffene Person einen Anspruch auf Nennung der konkreten Empfänger von personenbezogenen Daten hat. Auch hat der EuGH entschieden, dass eine kostenlose erste Kopie auch dann zu erteilen ist, wenn nationale Vorschriften für den Gesundheitsbereich eine kostenpflichtige Kopie vorsehen.

Der Europäische Datenschutzausschuss hat im Jahr 2023 eine Richtlinie für die Berechnung von Bußgeldern herausgegeben. Diese Richtlinie dient der einheitlichen und reproduzierbaren Berechnung von Bußgeldern. Nur durch Anwendung eines einheitlichen Ansatzes auch durch die katholischen Aufsichten kann eine vergleichbare Sanktionierung von Verstößen gegen datenschutzrechtliche Vorgaben gewährleistet bleiben.

Die Meldung einer Datenschutzverletzung ist zum Anlass genommen worden zu prüfen, inwieweit Anordnungen, welche die KDSA Nord in den Vorjahren erlassen hat, auch tatsächlich umgesetzt worden sind. Die bereits im Jahr 2021 durchgeführte Querschnittsprüfung in den Kindertagesstätten hatte als Folge einige Anordnungen ergeben. Bei der durchgeführten Nachprüfung haben wir zwölf von ursprünglich 38 geprüften Einrichtungen angeschrieben mit der Bitte, die Umsetzung der Anordnungen innerhalb einer bestimmten Frist nachzuweisen. Die Ergebnisse dieser Nachprüfung können im Abschnitt 2.5 nachgelesen werden. Auch wenn nicht in jedem Fall eine Nachprüfung der Anordnungen durchgeführt werden muss, scheint eine zumindest stichprobenartige Kontrolle angemessen und auch erforderlich zu sein.

Ich wünsche Ihnen viel Freude bei der Lektüre des 10. Tätigkeitsberichts.

Bremen, im August 2024

Andreas Bloms
Diözesandatenschutzbeauftragter

1. Aktuelle Entwicklungen im Datenschutz und Bedeutung für kirchliche Stellen

1.1. Europarecht

Wie wohl jede andere Datenschutzaufsicht auch schauen wir stets gespannt auf Gespräche, Kritiken, Planungen und Entwicklungen in Gesetzgebung und Rechtsprechung auf Europäischer Ebene. Das gemäß Art. 91 DSGVO festgelegte Recht der Kirchen, ihre eigenen Datenschutzregeln weiter anzuwenden, sofern diese mit der DSGVO in Einklang gebracht werden, führte nicht nur zum Inkrafttreten des heutigen KDG, das in vielen Teilen inhaltlich wie sprachlich eng an die Regelungen der DSGVO angelehnt ist. Vielmehr führte dies auch dazu, dass die Anwendung und Auslegung von Vorschriften der DSGVO erhöhte Bedeutung für den kirchlichen Bereich erlangten, um nicht – trotz gesetzgeberischem Einklang – in der praktischen Anwendung im Laufe der Jahre hinter dem europäischen Datenschutzniveau zurückzustehen.

1.1.1. Gesetzesänderung der DSGVO

Bereits zu Beginn des Jahres 2023 hat die Europäische Kommission für das zweite Quartal 2023 eine Gesetzesinitiative zur Änderung der DSGVO in Aussicht gestellt. Eine umfassende Reform war damit nicht angestrebt, sondern lediglich gezielte Änderungen, zum Beispiel zur Verbesserung der Zusammenarbeit von nationalen Aufsichtsbehörden, zur Beschleunigung von Verfahren bei grenzüberschreitenden Angelegenheiten und zur Konkretisierung von Beschwerdeverfahren. Diese Regelungsbereiche werden beobachtet, erlangen aber aktuell für den kirchlichen Bereich keine unmittelbare Bedeutung.

1.1.2. Digitale Rechte und Grundsätze

Die „Europäische Erklärung zu digitalen Rechten und Grundsätzen“[1], in der das Engagement der EU für einen sicheren und nachhaltigen Wandel im Einklang mit den Kernwerten und Grundrechten der EU dargelegt wird, ist am 15. Dezember 2022 von den Vorsitzenden des Europäischen Parlaments, des Rats und der europäischen Kommission unterzeichnet[2] und im Amtsblatt der Europäischen Union vom 23. Januar 2023 veröffentlicht worden[3]. Sie soll das Engagement der EU für einen sicheren und nachhaltigen digitalen Wandel sicherstellen. So wird im Abschnitt „Schutz der Privatsphäre und individuelle Kontrolle über Daten“ u.a. noch einmal das Recht

[1] https://digital-strategy.ec.europa.eu/de/library/european-declaration-digital-rights-and-principles (Abruf: 12.08.2024)
[2] https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7683 (Abruf: 12.08.2024)
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32023C0123(01) (Abruf: 12.08.2024)

sowohl auf Privatsphäre als auch auf den Schutz personenbezogener Daten zugesichert und die damit einhergehenden Verpflichtungen der Unterzeichner aufgeführt; z. B. „*dass jede Person die tatsächliche Kontrolle über ihre personenbezogenen und nicht personenbezogenen Daten im Einklang mit den EU-Datenschutzvorschriften und dem einschlägigen EU-Recht besitzt*“ (s. Kapitel V, Abschnitt „Schutz der Privatsphäre und individuelle Kontrolle über Daten“).

1.1.3. Europäische Datenstrategie

Auf Grundlage der Europäischen Datenstrategie soll ein Binnenmarkt für (personen- wie auch nicht-personenbezogene) Daten geschaffen werden. In diesem soll sichergestellt werden, dass bei einer Erhöhung der Menge an Daten, die für die Nutzung in Wirtschaft und Gesellschaft zur Verfügung stehen, gleichzeitig die Kontrolle bei den die Daten generierenden Einzelpersonen bleibt. Dazu wurden zwei Rechtsvorschriften, der Data Governance Act und der Data Act, eingeführt.

1.1.3.1. Data Governance Act (DGA)

Der Daten-Governance-Rechtsakt (EU 2022/868) zielt gemäß Art 1. Abs. 1 lit. a) darauf ab, die „*Weiterverwendung von Daten bestimmter Datenkategorien, die im Besitz öffentlicher Stellen sind, innerhalb der Union*“[4] zu regeln. Weitere Ziele sind die „*gemeinsame Nutzung von Daten durch die Regulierung neuartiger Datenintermediäre*“ ebenso wie die „*gemeinsame Nutzung von Daten für altruistische Zwecke zu fördern*.“[5] Im Anwendungsbereich liegen sowohl nicht-personenbezogene wie auch personenbezogene Daten, wobei der DGA nach Art. 1 Abs. 3 die DSGVO und die entsprechenden Bestimmungen des nationalen Rechts unberührt lässt; insbesondere wird mit dem DGA „*keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten [geschaffen], noch berührt es die in [der Datenschutzgrundverordnung] […] festgelegten Rechte und Pflichten*“. Der DGA gilt seit dem 24. September 2023.

1.1.3.2. Data Act (DA)

Die Datenverordnung (EU 2020/1828) soll die Datenwirtschaft in der EU verbessern, indem Daten (z. B. aus industriellen Anwendungen) zugänglicher und nutzbarer gemacht werden. Um Fairness sicherzustellen, regelt der DA, wer welche Daten unter welchen Voraussetzungen nutzen kann. Dazu zählen insbesondere die Daten, die von vernetzten Geräten generiert werden, die also mit dem Internet verbunden sind und das Internet of Things bilden. U. a. wird auch den Nutzern der vernetzten

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0868 (Abruf 12.08.2024)
[5] https://digital-strategy.ec.europa.eu/de/policies/data-governance-act-explained (Abruf: 12.08.2024)

Produkte (vernetzte Autos, Medizin- und Fitnessgeräte, Industrie- oder Landmaschinen) sowie der zugehörigen Dienste umfänglicher Zugriff auf die generierten (personenbezogenen wie nicht-personenbezogenen) Daten eingeräumt (s. Art. 3 Abs. 1 DA).

Wie der DGA lässt auch diese Verordnung gemäß Art. 1 Abs. 5 DA die DSGVO und die entsprechenden Bestimmungen des nationalen Rechts unberührt.

Veröffentlicht wurde der Data Act am 22. Dezember 2023 im Amtsblatt der EU[6]. Er gilt ab dem 12. September 2025.

1.1.4. Das Digital Service Act Paket

Darüber hinaus zielen das Gesetz über digitale Dienste (DSA) und das Gesetz über Digitale Märkte (DMA) auf die Schaffung eines gesicherten digitalen Raumes, in dem die Grundrechte der Nutzer geschützt werden und für Unternehmen die gleichen Wettbewerbsbedingungen gelten.

1.1.4.1. Digital Services Act (DSA)

Das Gesetz über digitale Dienste (EU 2022/2065) zielt auf die Verhinderung von illegalen oder schädlichen Online-Aktivitäten und das Unterbinden der Verbreitung von Desinformation ab. Es gilt für sehr große Online-Plattformen und Suchmaschinen sowie Hosting- und Vermittlungsdienste. Dabei komplementieren die Regelungen des DSA diejenigen der DSGVO bspw. im Hinblick darauf, dass angezeigte Werbung nicht auf Profiling (i. S. d. DSGVO) beruhen darf, das unter Verwendung besonderer Kategorien personenbezogener Daten erstellt worden ist (Art. 26 Abs. 3 DSA); Ähnliches gilt für Profiling-Daten minderjähriger Nutzer (Art. 28 Abs. 2 DSA). Die Anbieter von Online-Plattformen, die Empfehlungssysteme verwenden, müssen die dahinterliegenden Mechanismen darstellen, wobei die Anbieter sehr großer Online-Plattformen oder Suchmaschinen in den Empfehlungssystemen auch eine Option bereitstellen müssen, die nicht auf Profiling gemäß der Definition gemäß Art. 4 Abs. 4 DSGVO beruht (Art. 27, 38 DSA).

Die Verordnung selbst gilt ab dem 17. Februar 2024, allerdings gelten einige (z.B. Berichts-)Pflichten bereits seit dem 16. November 2022. Gemäß Art. 2 Abs. 4 lit. g) DSA bleiben die Unionsvorschriften zum Schutz personenbezogener Daten, insbesondere die DSGVO und die Richtlinie 2002/58/EG, von den Regelungen des DSA unberührt.

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854 (Abruf: 12.08.2024)

1.1.4.2. Digital Markets Act (DMA)

Für das Gesetz über Digitale Märkte (EU 2022/1925), das im Amtsblatt der Europäischen Union vom 12. Oktober 2022[7] veröffentlicht wurde und das grundsätzlich seit dem 2. Mai 2023 gilt, ist gemäß Art. 54 DMA seit dem 25. Juni 2023 auch die letzte Anwendungsfrist erreicht.[8]

Das Gesetz erlegt den marktbeherrschenden digitalen Plattformen, den sog. „Gatekeepern“ (dt. „Torwächtern“), Regeln auf, u.a. dass eigene Dienste nicht bevorzugt angeboten oder der Zugang zu anderen nicht erschwert werden darf. Am 6. September 2023 wurden von der Europäischen Kommission mit Alphabet, Amazon, Apple, ByteDance, Meta und Microsoft sechs Torwächter und 22 zentrale Plattformdienste benannt[9].

Im Hinblick auf personenbezogene Daten dürfte vor allem interessant sein, dass der DMA u.a. fordert, dass Daten verschiedener Dienste nicht ohne Zustimmung des Nutzers zusammengeführt werden dürfen (Art. 5 Abs. 2 lit. b) DMA), sowie dass eine Beschreibung aller eingesetzten Techniken zum Verbraucher-Profiling beim Europäischen Datenschutzausschuss vorgelegt wird (Art. 15 Abs. 1 DMA).

1.1.5. KI-Verordnung

Seit April 2021 arbeiten das Europäische Parlament und der europäische Rat parallel zu der allgemeinen Marktentwicklung an einem Vorschlag für eine Verordnung zur „Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union“[10], um den Einsatz von Methoden der künstlichen Intelligenz (KI) zu reglementieren.

Der Vorschlag enthält die Regelung, dass die Verarbeitung personenbezogener Daten den Regelungen der DSGVO unterliegen soll. Im Hinblick auf datenschutzrechtliche Fragestellungen hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bereits im November 2019 ein „Positionspapier […] zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“[11] veröffentlicht.

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ%3AL%3A2022%3A265%3ATOC (Abruf: 12.08.2024)
[8] https://eur-lex.europa.eu/eli/reg/2022/1925/2022-10-12?locale=de (konsolidierte Fassung) (Abruf: 12.08.2024)
[9] https://ec.europa.eu/commission/presscorner/detail/de/ip_23_4328 (Abruf 12.08.2024)
[10] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0206 (Abruf 12.08.2024)
[11] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der

1.1.6. EU-U.S. Data Privacy Framework

Am 10. Juli 2023 hat die Europäische Kommission einen neuen Angemessenheitsbeschluss „für einen sicheren und vertrauenswürdigen Datenverkehr zwischen der EU und den USA“ angenommen[12, 13]. Das auch „EU-U.S. Data Privacy Framework“ genannte Rahmenwerk[14] stellt den Nachfolger des Datenschutzabkommens Privacy Shield dar, das mit dem Urteil des EuGH vom 16. Juli 2020 („Schrems II“, C-311/18) für ungültig erklärt worden war.

Das EU-U.S. Data Privacy Framework ist nicht unumstritten. Auf eine Veröffentlichung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur „Übermittlung personenbezogener Daten aus Europa an die USA – Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023“[15], die auf den 4. September 2023 datiert und gegen die Stimme des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit verabschiedet worden ist, meldet sich dieser im Rahmen einer Pressemitteilung ebenfalls am 4. September 2023[16]. In seiner Stellungnahme weist er auf die Ergänzungsbedürftigkeit der Anwendungshinweise hin und bezieht sich dabei einerseits auf die Pflichten des Verantwortlichen, andererseits auf die Kritikpunkte des Europäischen Datenschutzausschusses und von Max Schrems.

Am 6. September 2023 reichte ferner Philippe Latombe Klage gegen die Europäische Kommission ein (Rechtssache T-553/23) und stellte einen Antrag auf Aussetzung des Durchführungsbeschlusses (EU 2023/1795; C(2023) 4745)[17]. Der Antrag wurde aufgrund fehlender Dringlichkeit am 12. Oktober 2023 zurückgewiesen.[18]

Für kirchliche Einrichtungen dürfte der neue Angemessenheitsbeschluss am häufigsten im Zusammenhang mit der Beauftragung von Auftragsverarbeitern relevant

Entwicklung und dem Betrieb von KI-Systemen (Stand: 06.11.2019) URL: https://www.datenschutz-konferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf (Abruf: 12.08.2024)

[12] https://ec.europa.eu/commission/presscorner/detail/de/ip_23_3721 (Abruf: 12.08.2024)

[13] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023D1795 (Abruf 12.08.2024)

[14] https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en (Abruf: 12.08.2024)

[15] https://www.datenschutzzentrum.de/uploads/dsk/23-09-04_DSK-Anwendungshinweise_EU-US_DPF.pdf (Abruf: 12.08.2024)

[16] https://tlfdi.de/aktuelles/anwendungshinweise-der-dsk-zum-angemessenheitsbeschluss-des-eu-us-data-privacy-framework-der-tlfdi-weicht-vom-votum-der-dsk-ab-und-nimmt-stellung/ (Abruf: 12.08.2024)

[17] https://op.europa.eu/s/zPEZ (Abruf: 12.08.2024)

[18] https://eur-lex.europa.eu/legal-content/DE/SUM/?uri=CELEX:62023TO0553_INF (Abruf: 12.08.2024)

werden, die selbst oder deren Unterauftragnehmer in den Vereinigten Staaten von Amerika lokalisiert sind. Nach dem o.g. Wegfall des Privacy Shield ist auf der Grundlage des EU-U.S. Data Privacy Framework eine Datenübermittlung an einen Teilnehmer am Framework gemäß § 40 Abs. 1 KDG wieder möglich.

Davon unberührt besteht für Einrichtungen im Anwendungsbereich des KDG die Pflicht zur Einhaltung der Anforderungen aus § 29 Abs. 3 KDG; dazu zählen u. a. die Regelung von Gegenstand, Dauer sowie Art und Zweck der Verarbeitung, ebenso wie die Art der verarbeiteten personenbezogenen Daten. Ferner muss den Anforderungen aus § 29 Abs. 4 KDG entsprochen werden, dass personenbezogene Daten u.a. nur auf dokumentierte Weisung des Verantwortlichen und nicht für eigene Zwecke des Auftragsverarbeiters verarbeitet werden dürfen. Für eingesetzte Unterauftragnehmer gelten ferner die Regelungen aus § 29 Abs. 2 KDG. (s. dazu auch die Meldung auf der Homepage KDSA-Nord.de[19])

1.1.7. EuGH-Entscheidungen

Im Folgenden werden drei Gerichtsentscheidungen vorgestellt, welche auch für kirchliche Einrichtungen eine hohe Relevanz haben.

1.1.7.1. Zurverfügungstellung einer Kopie

Der EuGH hat mit Urteil vom 4. Mai 2023, C-487/21[20], eine wichtige Entscheidung zu der Zurverfügungstellung einer Kopie im Zusammenhang mit dem Auskunftsanspruch von betroffenen Personen getroffen.

Hintergrund

Nach § 17 Abs. 3 KDG stellt der Verantwortliche „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.“ Im Ausgangsverfahren ist die Frage gestellt worden, ob es zur Erfüllung dieser Pflicht ausreicht, wenn der Verantwortliche die personenbezogenen Daten als Tabelle in aggregierter Form übermittelt oder ob die Übermittlung von Auszügen oder ganzen Dokumenten und Auszügen aus Datenbanken erforderlich ist.

Hierzu stellte der EuGH fest, dass

> *„das Recht, vom für die Verarbeitung Verantwortlichen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche*

[19] https://www.kdsa-nord.de/20230712 (Abruf: 12.08.2024)

[20] https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0487 (Abruf: 12.08.2024)

Reproduktion aller dieser Daten ausgefolgt wird. Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind.“
(aao., Rn. 45)“

Dieses umfassende Recht ergibt sich aus dem Transparenzgrundsatz, welcher ebenfalls im Kirchlichen Datenschutzgesetz geregelt ist. Nach § 14 Abs. 1 KDG müssen die Informationen, welche der betroffenen Person zur Verfügung gestellt werden, in präziser, leicht zugänglicher und verständlicher sowie in klarer und einfacher Sprache abgefasst sein. Diese Transparenzpflichten beziehen sich sowohl auf die Informationspflichten nach § 15 und § 16 KDG, als auch auf die Mitteilungen gemäß den §§ 17 bis 24 und 34 KDG. Nach dem Erwägungsgrund 58 der DSGVO wirkt der Transparenzgrundsatz umso stärker, je komplexer die Verarbeitungsvorgänge sind.

Dieser Transparenzgrundsatz wird jedoch durch die Rechte und Freiheiten anderer Personen eingeschränkt. Sofern in den Kopien auch personenbezogene Daten Dritter enthalten sind, sind diese zum Schutz ihrer personenbezogenen Daten ggf. zu schwärzen.

1.1.7.2. Auskunftsrecht zu konkreten Empfängern

Ein weiteres Urteil (EuGH, Urteil vom 12.01.2023, C-154/21[21]) beschäftigt sich mit dem konkreten Umfang des Auskunftsanspruchs.

Hintergrund

Nach § 17 Abs. 1 KDG hat die betroffene Person u.a. das Recht auf Mitteilung der „Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden“. Der Begriff „Empfänger“ ist weiter gefasst als der Begriff „Dritter“. Dritter i.S.d. § 4 Nr. 12 KDG ist jede andere Stelle „außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten“. Es erfolgt somit eine Negativabgrenzung zu anderen an der Datenverarbeitung Beteiligten. Empfänger sind nach § 4 Nr. 11 KDG diejenigen,

[21] https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0154 (Abruf: 12.08.2024)

welchen personenbezogene Daten offengelegt werden, „unabhängig davon, ob es sich bei Ihnen um einen Dritten handelt oder nicht“. Der Begriff Empfänger umfasst somit insbesondere auch die Auftragsverarbeiter des Verantwortlichen.

Hierzu stellte der EuGH fest, dass

> „*das in dieser [Art. 15 Abs. 1 DSGVO] Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen.“*
> *(aao., Rn. 51)*

Für die kirchlichen Einrichtungen folgt hieraus u.a. die Verpflichtung, den betroffenen Personen auf Verlangen auch die konkreten Auftragsverarbeiter mitzuteilen.

1.1.7.3. Kostenlose erste Kopie von Patientenakten

Auch mit dem Recht auf eine kostenlose erste Kopie von Patientenakten hat sich der EuGH (Urteil vom 26.10.2023 - C-307/22[22]) in einer weiteren relevanten Entscheidung beschäftigt.

Hintergrund

Grundsätzlich hat die betroffene Person gem. § 17 Abs. 3 KDG einen Anspruch auf eine Kopie der sie betreffenden personenbezogenen Daten. Diese erste Kopie ist grundsätzlich kostenfrei zu erteilen. Nach § 630g Abs. 2 Bürgerliches Gesetzbuch (BGB) hingegen kann der Patient eine elektronische Abschrift von der Patientenakte verlangen, wobei der Patient dem Behandelnden allerdings die entstandenen Kosten zu erstatten hat. Für die Einrichtungen, insbesondere Krankenhäuser, stellte sich somit stets die Frage, ob eine datenschutzrechtliche (kostenfreie) Kopie oder eine (kostenpflichtige) Kopie nach § 630g BGB geltend gemacht wird.

[22] https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0307 (Abruf: 12.08.2024)

Hierzu stellte der EuGH fest, dass

> „*Art. 12 Abs. 5 sowie Art. 15 Abs. 1 und 3 DSGVO dahin auszulegen sind, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, zur Verfügung zu stellen, auch dann gilt, wenn der betreffende Antrag mit einem anderen als den in Satz 1 des 63. Erwägungsgrundes der DSGVO genannten Zwecken begründet wird.*“
> (aao., Rn. 52)

Weiter bezieht sich der EuGH auf das auch in diesem Bericht bereits dargestellte Urteil vom 4. Mai 2023 (vgl. Ziffer 1.1.7.1). In Bezug auf die Patientenakte konkretisiert der EuGH, dass

> „*Art. 15 Abs. 3 Satz 1 DSGVO dahin auszulegen ist, im Rahmen eines Arzt-Patienten-Verhältnisses das Recht auf Erhalt einer Kopie der personenbezogenen Daten, die Gegenstand einer Verarbeitung sind, umfasst, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten überlassen wird. Dieses Recht setzt voraus, eine vollständige Kopie der Dokumente zu erhalten, die sich in der Patientenakte befinden und unter anderem diese Daten enthalten, wenn die Zurverfügungstellung einer solchen Kopie erforderlich ist, um der betroffenen Person die Überprüfung der Richtigkeit und Vollständigkeit der Daten zu ermöglichen und die Verständlichkeit der Daten zu gewährleisten. In Bezug auf die Gesundheitsdaten der betroffenen Person schließt dieses Recht jedenfalls das Recht ein, eine Kopie der Daten aus ihrer Patientenakte zu erhalten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu an ihr vorgenommenen Behandlungen oder Eingriffen umfasst.*“
> (aao., Rn. 79)

In einer Patientenakte werden nach § 630f BGB sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufgezeichnet. Vor dem Hintergrund dieser Entscheidung ist davon auszugehen, dass die Patientenakte als Ganzes dem Anspruch auf eine erste kostenlose Kopie unterliegt.

1.1.8. EDSA-Leitlinien für die Berechnung von Bußgeldern

Am 24. Mai 2023 hat der Europäische Datenschutzausschuss (EDSA) nach einer öffentlichen Konsultation die endgültigen „Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO“ in der Version 2.1[23] angenommen. Mit diesen soll die Bußgeldpraxis im Geltungsbereich der DSGVO nun nach einheitlichen Maßstäben erfolgen und die Verhängung von Bußgeldern harmonisiert werden.

Entwickelt wurde eine Methode mit fünf Schritten zur Ermittlung von Geldbußen für Verstöße gegen die DSGVO, die u.a. die Schwere des Verstoßes sowie die Umsätze des Unternehmens berücksichtigt und gemäß den Anforderungen aus Art. 83 Abs. 2 DSGVO auch die erschwerenden und ggf. mildernden Umstände im Zusammenhang mit dem Verhalten des Verantwortlichen berücksichtigt. Über allem steht die grundsätzliche Anforderung, dass eine ggf. verhängte Geldbuße „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ ist (s. Art. 83 Abs. 1, 3 DSGVO). Die o.g. Anforderungen finden sich nahezu wortgleich in § 51 Abs. 2, 3 KDG.

Insbesondere vor dem Hintergrund von Artikel 91 DSGVO wirken sich die EDSA-Leitlinien auch auf die kirchlichen Einrichtungen aus. Neben den genannten Gemeinsamkeiten in der DSGVO und dem KDG bestehen Unterschiede darin, dass die Datenschutzaufsicht nach dem Wortlaut des KDG ein Bußgeld verhängen „kann“ und dass die Höchstgrenze für eine Geldbuße bei (nur) 500.000 Euro liegt. Um eine Vergleichbarkeit des Schutzniveaus auch auf Sanktionsebene bei einer ggf. verhängten Geldbuße sicherzustellen, wird die Auffassung vertreten, dass der im KDG festgeschriebene Höchstbetrag von 500.000 EUR als „Kappungsgrenze“ anzusehen ist: für identische Datenschutzverstöße im Geltungsbereich der DSGVO wie auch im Geltungsbereich des KDG gelten – bis zur genannten Höchstsumme – vergleichbare Maßstäbe. Dies schließt eine Einstufung eines evtl. Datenschutzverstoßes in Anlehnung an Art. 83 Abs. 4-6 DSGVO und damit einhergehende maximale Sanktionssummen als Ausgangswerte für die Berechnung ein. Nur auf diesem Weg lässt sich eine vergleichbar wirksame, verhältnismäßige und abschreckende Wirkung bei der Verhängung einer Geldbuße erzielen.

Das bisherige Bußgeldberechnungsverfahren wird in Anlehnung an die EDSA-Leitlinien angepasst und soll 2024 erstmalig zur Anwendung gelangen.

[23] https://www.edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_de_0.pdf (Abruf: 12.08.2024)

1.2. Bundesrecht

1.2.1. Bundesdatenschutzgesetz

Im August 2023 legte das Bundesministerium des Innern und für Heimat einen Referentenentwurf zur Änderung des Bundesdatenschutzgesetzes vor. Ein wesentlicher Änderungsvorschlag ergibt sich für die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Diese soll durch § 16a institutionalisiert werden.

1.2.2. Beschäftigtendatenschutzgesetz

Noch im August 2023 hatte die Bundesregierung in ihrer Digitalstrategie[24] angekündigt, im Quartal 04/2023 einen Rahmen für ein Beschäftigtendatenschutzgesetz vorzulegen. Hierdurch sollen „Rechtsklarheit für Arbeitgeber sowie Beschäftigte“ geschaffen und die „Persönlichkeitsrechte der Beschäftigten effektiv“ geschützt werden. Bis zum Ende des Berichtszeitraums ist jedoch noch kein Entwurf eines neuen Beschäftigtendatenschutzgesetzes bekannt.

1.2.3. Hinweisgeberschutzgesetz

Am 2. Juli 2023 ist das Gesetz für einen Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) in Kraft getreten. Ziel des Gesetzes ist gem. § 1 Abs. 1, den „Schutz von natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen“ sicherzustellen.

Diese auch bei den Bistümern (s. nächster Abschnitt) eingerichteten Meldestellen sind gem. § 8 Abs. 1 HinSchG grundsätzlich verpflichtet, die Vertraulichkeit der hinweisgebenden Person und der Personen, die Gegenstand oder Teil der Meldung sind, zu wahren. Diese grundsätzliche Vertraulichkeitsverpflichtung gilt insbesondere auch für datenschutzrechtliche Auskunfts- und Informationsansprüche nach dem Kirchlichen Datenschutzgesetz.

Die Informationspflicht an betroffene Personen gilt gem. § 15 Abs. 5 lit. a) KDG dann nicht,

> „*wenn und soweit die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen*

[24] https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.html (Abruf: 12.08.2024)

Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss,“

Diese Ausnahme gilt auch bei Auskunftsansprüchen: Nach § 17 Abs. 6 lit. a) KDG besteht das Recht auf Auskunft dann nicht, wenn die betroffenen Personen u.a. nach § 15 Abs. 5 KDG nicht zu informieren sind.

Auch in der Gesetzesbegründung zum HinSchG[25] heißt es, dass das überwiegende berechtigte Interesse Dritter, hier der hinweisgebenden Person, an der Geheimhaltung regelmäßig anzunehmen ist. Kirchliche Meldestellen haben diese Vorgaben sowohl in Bezug auf die Informationspflichten als auch in Bezug auf geltend gemachte Auskunftsansprüche zwingend zu beachten, soweit keine Ausnahmen vom Vertraulichkeitsgebot nach § 9 HinSchG vorliegen.

Der Schutz der Vertraulichkeit ist auch auf Ebene der Berechtigungsvergabe sicherzustellen. Zugriff dürfen gem. § 16 Abs. 2 HinSchG nur diejenigen haben, die für die Entgegennahme und Bearbeitung der Meldungen zuständig sind, sowie die Personen, die bei der Erfüllung dieser Aufgaben unterstützend tätig werden.

1.3. Datenschutzrecht der Kirche

1.3.1. Gesetzgebung Bistümer

Die (Erz-)Bistümer sowie das Bischöflich Münstersche Offizialat in Vechta haben im Jahr 2023 u.a. unterschiedliche gesetzliche Regelungen im Bereich des Hinweisgeberschutzgesetzes und der Personalakten erlassen.

1.3.1.1. Ausführungsgesetz zum Hinweisgeberschutzgesetz im Erzbistum Hamburg

Das Erzbistum Hamburg hat mit dem „Gesetz zur Ausführung des Gesetzes für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) im Erzbistum Hamburg“ vom 8. Dezember 2023 die interne Meldestelle nach dem HinSchG bestimmt. Nach § 1 des Ausführungsgesetzes ist das Erzbistum Hamburg als gemeinsame Meldestelle für

- das Erzbistum Hamburg,
- den Erzbischöflichen Stuhl zu Hamburg,
- das Metropolitankapitel,
- das Erzbischöfliche Amt Schwerin,
- die Kirchengemeinden im Erzbistum Hamburg und

[25] BT.-Drs. 20/3442, S. 74

– die kirchlichen Stiftungen, die nach kirchlichem Recht öffentliche juristische Personen sind und deren Sitz im Erzbistum Hamburg liegt,

zuständig. Die Verpflichtung zur Vertraulichkeit, welche bereits in § 8 Abs. 1 HinSchG benannt ist, wird in § 8 Abs. 1 des Ausführungsgesetzes ebenfalls geregelt.

1.3.1.2. Ausführungsbestimmungen zum Hinweisgeberschutzgesetz im Bistum Osnabrück

Auch das Bistum Osnabrück hat mit Wirkung zum 1. Dezember 2023 „Ausführungsbestimmungen zur Umsetzung des Hinweisgeberschutzgesetzes (HinSchG) sowie der Ordnung zum Betrieb einer internen Meldestelle im Bistum Osnabrück (MeldeStO)“[26] erlassen. Das Bistum Osnabrück führt gem. § 2 Abs. 1 der Ausführungsbestimmungen ein Hinweisgebersystem in Form einer internen Meldestelle ein. Zuständig ist das Bistum Osnabrück sowohl für das Bistum Osnabrück selbst sowie „*für die weiteren öffentlichen juristischen Personen kanonischen Rechts im Bistum Osnabrück, die im Sinne von can. 1276 § 1 CIC der Aufsicht des Ortsordinarius unterstehen.*“ Ausgenommen hiervon ist der Caritasverband für die Diözese Osnabrück. Für sonstige kirchliche Rechtsträger besteht gem. § 1 Abs. 4 der Ausführungsbestimmungen die Möglichkeit, im Rahmen einer Vereinbarung die vom Bistum eingerichtete interne Meldestelle in Anspruch zu nehmen.

1.3.1.3. Personalaktenordnung im Bistum Hildesheim

Das Bistum Hildesheim hat mit Wirkung zum 1. Januar 2023 „Ausführungsbestimmungen PAO §§13 und 16: Recht auf Akteneinsicht und Entfernung von Personalaktendaten“ [27] erlassen. Hierdurch wird insbesondere das bereits mit Wirkung zum 1. Januar 2022 in Kraft getretene Akteneinsichtsrecht der Ordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten (Personalaktenordnung)“[28] (PAO) konkretisiert.

1.3.1.4. Ausführungsbestimmungen zur Führung bestimmter Personalakten

Die (Erz-)Bistümer sowie das Bischöflich Münstersche Offizialat in Vechta haben im Jahr 2023 unterschiedliche Ausführungsbestimmungen zur Rahmenordnung über die Führung von Personalakten und Verarbeitung von Personalaktendaten von Klerikern und Kirchenbeamten erlassen. Die Ausführungsbestimmungen können in den

[26] https://bistum-osnabrueck.de/wp-content/uploads/2017/01/02-2024.pdf (Abruf: 12.08.2024)
[27] https://www.bistum-hildesheim.de/fileadmin/dateien/PDFs/Materialboerse/Kirchlicher_Anzeiger/KA-2023-01.pdf (Abruf: 12.08.2024)
[28] https://www.bistum-hildesheim.de/fileadmin/dateien/PDFs/Materialboerse/Kirchlicher_Anzeiger/KA-2022-01.pdf (Abruf: 12.08.2024)

jeweiligen Amtsblättern der (Erz-)Bistümer eingesehen und heruntergeladen werden. [29,30,31]

1.3.1.5. Fundraising

Mit Wirkung zum 1. August 2023 ist die im Bistum Hildesheim erlassene „Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim – Fundraising Ordnung“ außer Kraft gesetzt worden. (Kirchlicher Anzeiger 2023, Nr. 5 / 15.08.2023, Seite 101)

1.3.2. Entscheidungen der Datenschutzgerichte

Auch die kirchlichen Datenschutzgerichte, sowohl das Interdiözesane Datenschutzgericht (IDSG 1. Instanz) als auch das Datenschutzgericht der Deutschen Bischofskonferenz (2. Instanz), haben im Jahr 2023 eine Vielzahl von Entscheidungen veröffentlicht (abrufbar auf der Webseite der DBK[32,33]). Die Entscheidungen im Kirchlichen Datenschutzrecht tragen nicht nur zum Rechtsfrieden im Einzelfall bei, sondern können darüber hinaus auch wertvolle Hinweise bei der Auslegung datenschutzrechtlicher Vorschriften geben.

In einer Entscheidung hat sich das IDSG[34] mit der Möglichkeit der Fristverlängerung nach § 14 Abs. 3 S. 2 KDG befasst.

Hintergrund

Grundsätzlich müssen Informationen u.a. bei der Geltendmachung von Auskunftsansprüchen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden. Diese Frist kann nach § 14 Abs. 3 S. 2 KDG um zwei Monate verlängert werden, „*wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.*“

[29] https://erzbistum-hamburg.de/Amtsblatt-Erzbistum-Hamburg-1536 (Abruf: 12.08.2024)
[30] https://www.bistum-hildesheim.de/service/materialien/kirchlicher-anzeiger/ (Abruf: 12.08.2024)
[31] https://bistum-osnabrueck.de/amtsblatt/ (Abruf: 12.08.2024)
[32] 1. Instanz: https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen (Abruf: 12.08.2024)
[33] 2. Instanz: https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/entscheidungen (Abruf: 12.08.2024)
[34] https://www.dbk.de/fileadmin/user_upload/IDSG_08_2020_Beschluss_vom_28.02.2023_Anonym.Fassung.pdf (Abruf: 12.08.2024)

Feststellung

Mit einer sehr hohen Klarheit stellt das IDSG fest, dass die Voraussetzungen für eine Fristverlängerung, unabhängig von der fehlenden Information an die betroffene Person, in dem Verfahren nicht vorlagen.

> „*Die noch durch die Folgen der Covid-19-Pandemie gesteigerte Belastung des Palliativdienstes hat entgegen der Auffassung des Antragsgegners keine Bedeutung für die Frage einer Komplexität der Anträge. Abgesehen davon handelte es sich bei der Bearbeitung der Anträge um eine Aufgabe der Verwaltungsbeschäftigten des Antragsgegners.*“

Hiernach kommt es nicht auf eine grundsätzlich hohe Auslastung der Mitarbeiter einer Einrichtung an. Die Komplexität und hohe Anzahl von Anträgen sind also in Bezug auf die jeweilige Person oder Gruppe von Personen, welche für die Bearbeitung der Anfrage zuständig ist, zu bewerten.

Grundsätzlich sollten Einrichtungen die erforderlichen Informationen, wie gesetzlich vorgesehen, unverzüglich, spätestens jedoch innerhalb einer Frist von einem Monat, zur Verfügung stellen. Zur Erfüllung dieser Pflicht empfiehlt es sich, eine interne Richtlinie oder Vorgabe zu erarbeiten, in der die einzelnen Schritte ggf. auch schematisch dargestellt werden. Weiter sollten Einrichtungen sicherstellen, dass sämtliche Mitarbeiter regelmäßig über die Rechte der betroffenen Personen geschult werden. Denn nur so kann sichergestellt werden, dass Anfragen von betroffenen Personen auch an die zuständigen Stellen zur fristgerechten Bearbeitung weitergeleitet werden.

Sofern der Verantwortliche die Frist um zwei Monate verlängern möchte, muss dies der betroffenen Person mitgeteilt werden. Die Fristverlängerung ist zudem zu begründen. Bei der Begründung ist darauf zu achten, dass diese hinreichend konkret ist, sodass die Gründe für die Fristverlängerung transparent nachvollzogen werden können.

2. Aus unserer Aufsichtstätigkeit

Im Rahmen unserer Aufsichtstätigkeit erreichen uns Meldungen über Datenschutzverletzungen ebenso wie Beschwerden oder Hinweise zu Missständen beim Umgang mit personenbezogenen Daten.

Sowohl der Eingang von Datenschutzverletzungen als auch die Anzahl von Beschwerden haben sich gegenüber dem Vorjahr nicht wesentlich verändert. Ein leichter Anstieg ist bei den Beratungsanfragen zu verzeichnen.

Einige der bearbeiteten Fälle sollen im Folgenden in verallgemeinerter Form dargestellt und unsere diesbezüglichen Einschätzungen mitgeteilt werden.

Aus den beschriebenen Fällen lassen sich allgemeine, nicht abschließende Hinweise für die Verantwortlichen wie auch für diejenigen, deren Daten verarbeitet werden, ableiten.

Ebenso werden die im Berichtsjahr durchgeführten datenschutzrechtlichen Prüfungen sowie die Veranstaltungen dargestellt, die wir ausgerichtet und an denen wir teilgenommen haben.

2.1. Bistümer und Kirchengemeinden

2.1.1. Weitergabe von Meldedaten an Zeitungsverlage – Es geht weiter

Bereits im Jahresbericht 2022 ist darauf hingewiesen worden, dass eine Weitergabe von personenbezogenen Daten zum Zwecke der gezielten Haustürwerbung an eine Kirchenzeitung als nicht zulässig angesehen wird. Das hierzu laufende Beschwerdeverfahren konnte zugunsten der Beschwerdeführerin im Berichtsjahr abschlossen werden. Sowohl die Weitergabe von personenbezogenen Daten an die Kirchenzeitung als auch die Nutzung dieser personenbezogenen Daten durch die Kirchenzeitung ist als rechtswidrig bewertet worden. Hieraus folgten die Anordnungen, zum einen eine erneute Weitergabe von personenbezogenen Daten an die Kirchenzeitung zu unterlassen und zum anderen, die nicht rechtmäßig erhobenen personenbezogenen Daten zu löschen.

Die Beschwerdegegner haben gegen die Entscheidung der KDSA Nord Rechtsmittel eingelegt, sodass die gerichtliche Klärung der Weitergabe der personenbezogenen Daten noch aussteht. Mit einem Abschluss des laufenden Gerichtsverfahrens ist in 2024/2025 zu rechnen.

Hinweis – Was ist zu beachten?

Unabhängig vom Ausgang der gerichtlichen Entscheidung muss im Einzelfall grundsätzlich festgestellt und dargelegt werden können, dass eine Datenverarbeitung durch eine Rechtsgrundlage gerechtfertigt ist. Dabei ist insbesondere die Bewertung unbestimmter Rechtsbegriffe wie hier des kirchlichen Interesses nicht immer einfach. Um der Gefahr einer zu extensiven Auslegung des kirchlichen Interesses vorzubeugen, müssen objektive Kriterien zur Auslegung herangezogen werden.

Um den Anwendungsbereich sinnvoll einzugrenzen, kann zunächst die Einordnung der betreffenden Tätigkeiten in eine der folgenden Kategorien erfolgen:

- Seelsorge und Verkündigung
- Caritative Aktivitäten
- Pflege und Förderung des Bekenntnisses

Im Weiteren sollte bedacht werden, dass diese Kategorien in ihrem Kern berührt sein müssen und nicht jede Motivation, die im entfernten Sinne (auch) einer der genannten Kategorien dienen (kann), dazu führt, dass das kirchliche Interesse als Rechtsgrundlage herangezogen werden kann.

2.1.2. Offener E-Mail-Verteiler

Die Kommunikation per E-Mail ist in den meisten Pfarrbüros Standard. Insbesondere bei der Nutzung von E-Mail-Verteilern zum serienmäßigen Versand beispielsweise von Pfarrbriefen, Einladungen oder allgemeinen Informationen zu Ferienfreizeiten, kommt es immer noch regelmäßig zu Datenschutzverletzungen durch die Verwendung eines offenen E-Mail-Verteilers. In den überwiegenden Fällen kennen die betreffenden Mitarbeiter des Pfarrbüros die Pflicht zur Nutzung der bcc-Funktion und es handelt sich um ein Versehen.

Hinweis – Was ist zu beachten?

Die Wirkung regelmäßiger Sensibilisierungen sollte nicht unterschätzt werden! Je öfter einem Mitarbeiter das Szenario vor Augen geführt wird, desto öfter denkt derjenige daran und führt entsprechende Arbeitsschritte bewusster aus.

Unterstützend können die Einstellungen im E-Mail-Programm (z.B. über eine Gruppenrichtlinie) so angepasst werden, dass das bcc-Feld immer eingeblendet ist.

2.1.3. Einsatz von Wildkameras

Meist ist es ein unerwartetes Ereignis wie Vandalismus durch Beschädigung von Inventar in der Kirche oder Graffitis an den Außenwänden, welches dazu führt, dass „schnell eine Kamera her“ muss. Da diese in erster Linie abschrecken und potentielle Täter aufnehmen soll, mag den Verantwortlichen ein einfaches günstiges Modell aus dem Discounter genügen, welches auch in technischer Hinsicht simpel zu bedienen ist.

Im Rahmen einer Prüfung sind wir auf den Einsatz einer sog. Wildkamera gestoßen, die aus ebendiesen Gründen, preisgünstig und technisch unkompliziert, beschafft und im Eingangsbereich einer Kirche aufgehängt wurde. Wildkameras sind in der Regel mit Bewegungssensoren ausgestattet und nehmen erst dann Bilder auf, wenn eine Bewegung festgestellt wird.

Die besagte Wildkamera verfügte über einen lokalen Chip, auf dem die Bilddaten gespeichert wurden. Auf die Videoüberwachung wurde mit Hinweisschildern hingewiesen. Eine datenschutzrechtliche Prüfung der Zulässigkeit des Videoeinsatzes war im Vorfeld jedoch nicht erfolgt.

Der Einsatz einer Videoüberwachung stellt einen erheblichen Eingriff ist die Persönlichkeitsrechte der erfassten Personen dar und muss daher ausreichend geplant werden. Die gesetzlichen Anforderungen an die Videoüberwachung ergeben sich aus § 52 KDG. Hiernach ist die Videoüberwachung nur zulässig, soweit sie „zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ erforderlich ist und keine Anhaltspunkte bestehen, dass „schutzwürdige Interessen der betroffenen Person überwiegen.“

Neben der Zweckbestimmung der Videoüberwachung hat stets eine Gewichtung der schutzwürdigen Interessen der betroffenen Personen zu erfolgen. Sowohl die Orte/ Bereiche einer Videoüberwachung als auch die allgemeine und technische Ausgestaltung spielen hierfür eine Rolle. Eine Erfassung aller Gläubigen beim Ein- und Ausgehen in eine Kirche kann bereits eine erhebliche Beeinträchtigung der Ausübung der Glaubensfreiheit sein, die einer besonderen Rechtfertigung bedarf (z.B. durch nachweisbar hohen entstandenen Schaden, Wiederholungsgefahr, fehlende Alternativen). Eine differenzierte Ausgestaltung des Videoeinsatzes, beispielsweise durch eingeschränkte Aufnahmezeiten (z.B. nur abends und nachts), eine kurze Speicherdauer und die Festlegung von technischen und organisatorischen Maßnahmen, einschließlich Verschlüsselung und engen Zugriffsrechten sind unbedingt erforderlich.

Hinweis – Was ist zu beachten?

Im Vorfeld jedes Videoeinsatzes ist zu prüfen, ob dieser tatsächlich das Mittel der Wahl ist. Sind sensible Bereiche betroffen, kann eine Datenschutz-Folgenschätzung erforderlich sein.

Um einen datenschutzkonformen Einsatz einer Videokamera sicherzustellen, ist die Einbindung des betrieblichen Datenschutzbeauftragten zu empfehlen. In diesem Rahmen lässt sich ggf. auch feststellen, ob bestimmte Kameratypen aufgrund ihrer technischen Ausstattung für den geplanten Einsatz ungeeignet sind und welche technischen und organisatorischen Maßnahmen gemäß § 26 KDG umzusetzen sind.

Es ist zudem zu beachten, dass es Bereiche gibt, die grundsätzlich nicht überwacht werden dürfen, da der Eingriff in die Ausübung der Glaubensfreiheit nicht gerechtfertigt werden kann. Hierzu zählen beispielsweise der Beichtstuhl oder Bereiche, die für das Gebet genutzt werden.

2.1.4. Fristverlängerung zur Erfüllung des Auskunftsanspruchs

In einem Beschwerdeverfahren ging es u.a. um die Erfüllung des Auskunftsanspruchs nach § 17 KDG. Die Beschwerdegegnerin erteilte die Auskunft nicht rechtzeitig und begründete das Erfordernis einer Fristverlängerung um zwei Monate damit, dass aufgrund der Ortsverschiedenheit von Räumlichkeiten und Personal eine sofortige Bearbeitung erschwert sei. Die personenbezogenen Daten, welche zu beauskunften waren, befanden sich an unterschiedlichen Speicherorten, sodass diese zunächst zusammengetragen werden mussten. Diese Begründung konnte die Fristverlängerung um zwei Monate jedoch nicht rechtfertigen, sodass die Auskunft nicht fristgerecht erteilt worden ist.

Hinweis – Was ist zu beachten?

Wie bereits unter Abschnitt 1.3.2 hervorgehoben, gelten für das Erfordernis einer Fristverlängerung hohe Anforderungen. Grundsätzlich können unterschiedliche Speicherorte die Komplexität von Anträgen erhöhen. Die Information an die betroffene Person zur Begründung der Fristverlängerung muss jedoch hinreichend konkret sein, sodass die Gründe für die Fristverlängerung transparent nachvollzogen werden können. Formelhafte Formulierungen genügen den Anforderungen nicht.

Eine umfangreiche Hilfestellung wird auch vom Europäischen Datenschutzausschuss (EDSA) durch die „Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht“[35] zur Verfügung gestellt. Enthalten sind auch Hinweise darauf, wann Anträge als komplex angesehen werden können.

2.1.5. Zugriffskontrolle bei Backup-Daten

In einem uns gemeldeten Fall bestand die Notwendigkeit des Einspielens einer Datensicherung; ein entsprechendes Backup stand zwar zur Verfügung und die Wiederherstellung der Daten war erfolgreich, allerdings waren anschließend die im Produktiv-Datenbestand eingerichteten Zugriffsberechtigungen nicht mehr wirksam und Nutzer konnten auch auf Daten zugreifen, die nicht ihrer Zuständigkeit unterlagen.

Der Schutz personenbezogener Daten vor unbeabsichtigtem Verlust oder unbeabsichtigter Zerstörung ist einer der Grundsätze für die Verarbeitung personenbezogener Daten aus § 7 Abs.1 lit. f) KDG.

Zu diesem Zweck wird in § 16 Abs. 2 KDG-DVO konkret das regelmäßige Anfertigen von Datensicherungen gefordert; für Daten der Datenschutzklassen II und III besteht ferner die konkrete Anforderung, dass Sicherungskopien vor Fremdzugriff und gleichzeitiger Zerstörung mit den Originaldaten geschützt werden müssen (s. § 12 Abs. 2 lit. c) KDG-DVO). § 16 Abs.1 KDG-DVO fordert in diesem Zuge für eine Systematisierung der Überlegungen die Erstellung eines Datensicherungskonzepts.

Hinweis – Was ist zu beachten?

Je nach Ausgestaltung des Prozesses zur Sicherung personenbezogener Daten ist es dringend geboten zu prüfen, ob die ursprünglich eingerichteten Zugriffsberechtigungen auch nach der Wiederherstellung aus dem Backup noch wirksam sind.

Der Umfang und die Häufigkeit der Datensicherungen sind an der jeweiligen Verarbeitungstätigkeit auszurichten.

2.1.6. Systematischer Einbruchdiebstahl

Bei Einbrüchen und Diebstählen in vier über denselben Landkreis verteilten Standorten wurden u. a. Tresore aufgebrochen und elektronische Geräte, Bargeld,

[35] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de (Abruf: 12.08.2024)

Bankkarten, Fahrzeugpapiere und -schlüssel entwendet. Das Vorgehen, bei dem ein Universaltransponder entwendet und für den Zutritt in die Räumlichkeiten auch an anderen Standorten verwendet wurde, deutet auf ein gezieltes Vorgehen hin.

Universelle Zugangs- wie auch Zutrittsberechtigungen sind für Kriminelle lohnende Beute. Der hier gestohlene und im Folgenden genutzte Universaltransponder hat für den unautorisierten Zutritt zu den Räumlichkeiten in etwa den gleichen Stellenwert wie Administrationspasswörter, mit denen ein Zugang zu einer Vielzahl von IT-Systemen möglich ist.

Hinweis – Was ist zu beachten?

Vor dem Hintergrund der besonderen Schutzbedürftigkeit von Universaltranspondern und der Vergleichbarkeit mit Administrationspasswörtern lässt sich aus § 23 KDG-DVO ableiten, dass jegliche Form von universellen Zutritts-, Zugangs- oder Zugriffsmitteln besonders gesichert aufzubewahren sind. Geeignete Maßnahmen können beispielsweise die Aufbewahrung in einem Tresor oder einem gesicherten Schlüsselschrank sein, auf den nur ein fest definierter Personenkreis Zugriff hat. Dadurch kann auch die Gefahr gezielter Angriffe/Entwendungen „von innen“ reduziert werden.

Je nach Gegebenheit lassen sich auch durch die Aufteilung der Berechtigungen auf unterschiedliche Universal-Transponder Schadenspotenziale verringern.

2.2. Gesundheitseinrichtungen

2.2.1. Unzulässige Einsichtnahmen in Patientenakten und Mitarbeiterexzess

Ein unzulässiger Zugriff auf Patientenakten durch Klinikpersonal hat uns im Berichtsjahr nicht nur in einem Einzelfall beschäftigt. Der Aufruf einer digitalen Patientenakte ist oft leicht und seitens der vergebenen Berechtigungen nicht immer daran geknüpft, dass eine Beteiligung an der Behandlung besteht. Das Unrechtsbewusstsein der Mitarbeiter schien – in den von uns bearbeiteten Fällen – dabei erstaunlich gering zu sein, insbesondere da es nicht bei einer Einsichtnahme geblieben ist, sondern die erlangten Informationen auch an Dritte weitergegeben wurden. So wurden in einem der Fälle Behandlungsinformationen aus der Patientenakte im privaten Umfeld des Patienten verbreitet und dieser dadurch erheblich in seiner gesellschaftlichen Stellung beeinträchtigt.

Wird ein Fall an uns herangetragen, in dem ein Mitarbeiter einer Gesundheitseinrichtung unzulässigerweise auf eine Patientenakte zugegriffen hat, wird stets geprüft, ob (auch) eine datenschutzrechtliche Verantwortlichkeit des Mitarbeiters in Frage kommt (sog. „Mitarbeiterexzess“) und dieser ggf. selbst Adressat einer aufsichtsrechtlichen Maßnahme sein kann. Diese Möglich- und Notwendigkeit besteht aus unserer Sicht immer dann, wenn deutlich wird, dass die Einsichtnahme und Weiterverwendung der Daten nicht dienstlich bestimmt sind, sondern zu eigenen privaten Zwecken des Mitarbeiters erfolgen. Werden bestehende technische und organisatorische Maßnahmen bewusst umgangen oder missachtet und erfolgt die weitere Verwendung dieser Daten zu rein privaten Zwecken (z. B. Posting über private Social Media Accounts, s. auch Abschnitt 2.2.6), so ist regelmäßig von einem Mitarbeiterexzess auszugehen, für den der Mitarbeiter zur Verantwortung gezogen werden kann. In einem solchen Fall erfolgt eine Abgabe dieses (ggf. Teils des) Verfahrens an die zuständige Landesdatenschutzaufsicht.

Aufseiten der Gesundheitseinrichtungen besteht eine besondere Verantwortung, solchen Fällen so weit wie möglich vorzubeugen. Gegebenenfalls liegt im Einzelfall auch ein Versäumnis in Form eines Organisationsverschuldens seitens der Einrichtung vor; diese Prüfung ist dann Gegenstand der Untersuchungen der kirchlichen Aufsicht. Geprüft werden insbesondere folgende Punkte:

Berechtigungskonzept

Gibt es ein Berechtigungskonzept? Wie ist dieses ausgestaltet? Ist das Need-to-know-Prinzip berücksichtigt? Genügt das Berechtigungskonzept den Vorgaben der OH-KIS? Welche Besonderheiten gibt es, die möglicherweise weite Zugriffsrechte rechtfertigen? Hätte die konkret betroffene Akte überhaupt zugänglich sein dürfen, was beispielsweise bei bereits abgeschlossenen Behandlungsfällen oder VIP-Akten nur eingeschränkt der Fall sein kann.

Uns ist bewusst, dass, nicht zuletzt wegen des Fachkräftemangels und der angespannten Finanzlage im Gesundheitswesen, Klinikpersonal interdisziplinär arbeitet und stationsübergreifend eingesetzt wird. Auch das ist jedoch keine Rechtfertigung dafür, die Berechtigungen unbegrenzt auszuweiten, um „für den Fall der Fälle“ eine sofortige Zugriffsmöglichkeit für alle Bereiche zu bieten. Berechtigungen müssen so vergeben sein, dass Mitarbeiter lediglich auf die für ihre Aufgabenerfüllung notwendigen Patientendaten zugreifen können. Darüberhinausgehende Zugriffe können natürlich, bspw. in Notfällen, ihre Berechtigung haben, sollten dann aber gemäß dem Konzept des Sonderzugriffs aus der OH KIS ausgestaltet sein.

Schulung und Sensibilisierung

Gibt es ein Schulungskonzept? In welcher Form und Häufigkeit finden Schulungs- und Sensibilisierungsmaßnahmen zum Datenschutz statt? Welche konkreten Inhalte werden vermittelt? Wird die Teilnahme an den Schulungen und Sensibilisierungsmaßnahmen dokumentiert? Ist sichergestellt, dass alle Mitarbeiter an den Schulungsmaßnahmen teilnehmen? Kann die Teilnahme für jeden Mitarbeiter nachgewiesen werden?

Gerade beim Umgang mit Gesundheitsdaten erwarten wir ein effektives und funktionierendes Schulungsmanagement. Es liegt auf der Hand, dass es hier nicht ausreicht, die Mitarbeiter alle zwei oder drei Jahre einer Pflichtschulung (Online oder Präsenz) zu unterziehen. Vielmehr muss sichergestellt sein, dass die Mitarbeiter zu allen relevanten Themen geschult werden und diese Themen durch regelmäßige Sensibilisierungsmaßnahmen aufgefrischt, verankert und vertieft werden. Als besonders effektiv wird die Kombination aus festen Datenschutzschulungen und kleineren Sensibilisierungen zu Einzelthemen bewertet, die in Dienstbesprechungen und Mailings erfolgen können. Die Durchführung aller Sensibilisierungsmaßnahmen und die Teilnahme aller Mitarbeiter sollten nachgewiesen werden können.

Hinweis – Was ist zu beachten?

Das bestehende Berechtigungskonzept sollte so ausgestaltet sein, dass die Rechte entsprechend den Vorgaben der OH-KIS differenziert vergeben werden. Nicht nur die initiale Vergabe von Berechtigungen sollte nach einem festgelegten, überprüfbaren Verfahren erfolgen, sondern auch die Änderung (z.B. beim Wechsel der Tätigkeit) und der Entzug von Rechten (z.B. bei Ausscheiden). Die bestehenden Berechtigungen sollten regelmäßig auf Aktualität geprüft werden.

Die Mitarbeiter sollten explizit und nachweisbar zum verantwortungsvollen Umgang mit den Ihnen zugänglichen Informationen und insbesondere den Zugriffsrechten geschult und sensibilisiert werden.

2.2.2. Unzureichende Maßnahmen bei besonders schutzbedürftigen Patientengruppen

Die oben geschilderten Verstöße durch unberechtigte Zugriffe auf Patientenakten können besonders schwerwiegend sein, wenn die Patienten zu der gemäß der OH-KIS besonders schutzwürdigen Patientengruppe zählen. Das sind in der Regel Patienten, die in der Klinik bekannt sind und daher das Interesse an der

Krankengeschichte und der mit einer unbefugten Offenlegung verbundene Schaden besonders hoch sein kann. Zu diesen Patienten zählen zum einen Mitarbeiter der Klinik, aber auch berühmte Persönlichkeiten. Die OH KIS sieht in diesen Fällen die Möglichkeit einer besonderen Kennzeichnung der Fallakten und der Einrichtung besonderer Zugriffsberechtigungen vor. Auch wenn die OH KIS im Teil II Abschnitt 1.12 und 1.13 im Hinblick auf die Verbindlichkeit der Maßnahmenforderung bei den o.g. Gruppen unterscheidet, wird unsererseits die Auffassung vertreten, dass der Schaden, der mit einer unbefugten Offenlegung personenbezogener Daten einhergeht, es in beiden Fällen (Prominente und Mitarbeiter) rechtfertigt, diesen Patientengruppen den VIP-Status pflichtmäßig anzubieten. Die in diesem Zusammenhang in den Umsetzungshinweisen zur OH KIS[36] genannte Option der Nutzung eines Pseudonyms sei in diesem Zusammenhang ebenfalls erwähnt.

Zumindest in einem von uns bearbeiteten Fall hat sich gezeigt, dass die Mitarbeiter einer Klinik keine Kenntnis von diesen Möglichkeiten hatten.

Hinweis – Was ist zu beachten?

Für Mitarbeiter einer Gesundheitseinrichtung ist in der Regel von einer besonderen Schutzwürdigkeit auszugehen, wenn sie Patient der eigenen Einrichtung werden. Mitarbeitern ist daher die Option der Nutzung eines „VIP-Status“ oder die Erfassung unter einem Pseudonym anzubieten. Hierauf sollte bspw. durch interne Bekanntmachungen und idealerweise zusätzlich bei der Aufnahme hingewiesen werden.

2.2.3. Verwechslung von Arztbriefen

In regelmäßigen Abständen erhalten wir Meldungen von Datenschutzverletzungen aus Gesundheitseinrichtungen aufgrund einer fehlerhaften Herausgabe oder eines Fehlversands von Arztbriefen. Die Ursachen für eine Verwechslung der Dokumente können sehr unterschiedlich sein, wie beispielsweise ungeregelte Prozesse beim Postausgang, Unachtsamkeit der Mitarbeiter beim manuellen Kuvertieren oder auch eine fehlerhafte Einstellung sowie technische Mängel der Kuvertiermaschinen.

Ob es sich hierbei um eine meldepflichtige Datenschutzverletzung handelt, wird von den Gesundheitseinrichtungen sehr unterschiedlich bewertet. Das ist aus unserer Sicht kaum nachvollziehbar: Die Dokumente enthalten in der Regel Patientendaten,

[36] Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme, 2. überarbeitete Fassung, Stand: 25. März 2014, S. 22.

wie Angaben zur Diagnose, Medikation und Behandlungspläne. Dabei handelt es sich um Gesundheitsdaten, die zu den besonderen Kategorien personenbezogener Daten gehören und damit der Datenschutzklasse III zuzuordnen sind. Eine Offenlegung dieser Daten an Unbefugte führt daher im Regelfall zu einer Gefahr für die Rechte und Freiheiten der betroffenen Patienten und damit zu einer Meldepflicht gemäß § 33 Abs. 1 KDG. Auch wenn diese Gefahr unterschiedlich hoch bewertet werden kann, je nachdem wie umfangreich der enthaltene Datensatz ist, um welche „falschen" Empfänger es sich handelt (Privatperson, Arztpraxis, Behörde) oder wie der Umgang der Empfänger mit dem Erhalt der Dokumente ist, so ist eine Meldung an die Datenschutzaufsicht grundsätzlich erforderlich.

Hinweis – Was ist zu beachten?

Verwechslungen können passieren und sind nicht immer zu verhindern. Jedoch sind vom Verantwortlichen Maßnahmen zu treffen, um dieses Risiko so weit wie möglich zu reduzieren:

Es sollte ein Verfahren für den Postausgang festgelegt und umgesetzt werden. Die zuständigen Mitarbeiter müssen zudem regelmäßig sensibilisiert werden.

Eventuelle Fehler müssen analysiert werden und ggf. zu einer Anpassung des Verfahrens führen. Es sollten auch anlasslos regelmäßige Kontrollen durchgeführt und ggf. das Verfahren angepasst werden.

Ist eine Kuvertiermaschine im Einsatz, ist diese engmaschig zu kontrollieren, um zu vermeiden, dass eine mögliche falsche Einstellung oder ein technischer Defekt über einen längeren Zeitraum Fehlsendungen verursacht.

Fehlversendungen von Gesundheitsdaten sind grundsätzlich meldepflichtig.

2.2.4. Veröffentlichung von Gesundheitsdaten

Ein internes Krankenhaus-Magazin, Fachartikel in Fachzeitschriften, Power-Point-Präsentationen auf Ärzte-Kongressen – dies sind nur einige Beispiele, wo medizinische Veröffentlichungen zu finden sind. In der Regel erfolgen die Veröffentlichungen ohne direkten Bezug zu bestimmten Patienten. Zur Veranschaulichung von Krankheitsbildern und Diagnosen sind Fachartikel aber nicht selten mit Bildern angereichert, z. B. Röntgenbilder, MRT-Bilder o. ä., die u. U. die Herstellung eines Personenbezugs ermöglichen. In einem uns gemeldeten Fall wurde versehentlich ein Röntgenbild eines Patienten in einem Fachartikel veröffentlicht, auf dem die Daten des

Patienten zu lesen waren (Name, Geburtsdatum, Patientennummer). Eine entsprechende Einwilligung hatte der Patient nicht erteilt.

Hinweis – Was ist zu beachten?

Werden klinische Bilder für eine Veröffentlichung genutzt, sind im Vorfeld alle personenbezogenen Daten, die auf den Bildern abgedruckt sind, zu entfernen. Da die Bilder von der Auswahl bis zum Druck durch „mehrere Hände" gehen, ist es wichtig, dass alle Beteiligten angewiesen sind, die Bilder entsprechend zu kontrollieren.

Da ein Rückschluss auf einen konkreten Patienten auch ohne Angabe der Klardaten auf den Bildern möglich sein kann, sollten mögliche Veröffentlichungen auch im Rahmen des Einwilligungsmanagements berücksichtigt werden.

2.2.5. Gesundheitsdaten Verstorbener

Die Persönlichkeitsrechte Verstorbener erlöschen nicht mit dem Tod der Patienten. Hingegen gilt das Recht auf informationelle Selbstbestimmung ausweislich der Gesetzesbegründung der DSGVO nur für lebende Personen. Beschwerden, die sich auf personenbezogene Daten Verstorbener beziehen, fallen daher grundsätzlich nicht in den Aufgabenbereich der Datenschutzaufsicht (zumindest soweit dadurch nicht direkt Rückschlüsse auf Angehörige gezogen werden können). Da aber die ärztliche Schweigepflicht auch über den Tod der Patienten hinaus gilt, gibt es die Möglichkeit, zivilrechtliche Ansprüche gemäß § 823 BGB geltend zu machen sowie strafrechtliche Schritte gemäß § 203 StGB einzuleiten.

Hinweis – Was ist zu beachten?

Im Falle einer unzulässigen Offenbarung von Gesundheitsdaten Verstorbener ist die Datenschutzaufsicht zwar i.d.R. nicht die richtige Anlaufstelle. Mit Blick auf die drohenden zivil- und strafrechtlichen Konsequenzen sollte jedoch auch dieses Thema im Rahmen des Schulungsmanagements berücksichtigt werden.

2.2.6. Heimliches Live-Streaming aus Gesundheitseinrichtungen

Vom Phänomen des Live-Streamings über Social-Media-Plattformen blieben auch kirchliche Gesundheitseinrichtungen im Berichtszeitraum nicht verschont. So wenig nachvollziehbar die mangelnde Empathie derjenigen ist, die Bilder von sich und z. T. wehrlosen Personen oder (minderjährigen) Schutzbefohlenen ungefragt z. B. per

Livestream über private Accounts der Öffentlichkeit zugänglich machen, so klar ist doch die datenschutzrechtliche Bewertung.

Aus den Begriffsbestimmungen des KDG wird deutlich, dass der in diesem Szenario für eine Verarbeitung personenbezogener Daten (hier: Bild- bzw. Videodaten) Verantwortliche diejenige „*natürliche oder juristische Person […] [ist], die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.*“

Der Zweck ist in diesem Fall die eigene Profilierung auf den Social-Media-Kanälen, die Mittel sind das eigene Smartphone und der private Social-Media-Account. Die Verantwortung liegt damit oftmals allein beim Mitarbeiter, welcher sich gegenüber der zuständigen Landesdatenschutzaufsicht verantworten muss. Fälle wie diese werden grundsätzlich in Zusammenarbeit mit den staatlichen Aufsichtsbehörden bearbeitet. (s. auch „Mitarbeiterexzess“ in Abschnitt 2.2.1)

Hinweis – Was ist zu beachten?

Es sollte sichergestellt werden, dass alle in der Gesundheitseinrichtung Tätigen – vom Mitarbeiter, Leiharbeitnehmer bis hin zu Auszubildenden und Schülerpraktikanten – gezielt zur Einhaltung des Datengeheimnisses im Zusammenhang mit privaten Social-Media-Kanälen sensibilisiert werden.

In diesen Fällen drohen nicht nur Konsequenzen seitens der zuständigen Datenschutzaufsicht. Oft hat ein unerlaubtes Streaming auch arbeitsrechtliche Folgen.

2.3. Bildung und Kitas

2.3.1. Einbruchdiebstahl in Kitas

Einbrüche in Kindertagesstätten kommen nach wie vor recht häufig vor. In den Meldungen wird regelmäßig der Diebstahl von Laptops, Notebooks oder Kameras mitgeteilt. Leider ist festzustellen, dass in den meisten Fällen im Vorfeld keine ausreichenden Maßnahmen getroffen wurden, um die Daten der Kinder, Erziehungsberechtigten und Mitarbeiter im Falle eines Einbruchs adäquat zu schützen. Beispielsweise werden die Geräte offen in der Einrichtung und nicht verschlossen im Schrank aufbewahrt. Die Daten werden lokal gespeichert und eine Verschlüsselung der Daten, z. B. mittels Bitlocker, ist in den wenigsten Fällen eingesetzt worden.

Auch wenn es sich bei den Kitas in der Regel um kleinere Einrichtungen handelt, die unbestritten wenig personelle und zeitliche Ressourcen zur Verfügung haben,

müssen die gebotenen Schutzmaßnahmen mit Blick auf die Sensibilität der Daten (insb. Kinderdaten, Fotos) eingehalten werden. Die Tatsache, dass Einbrüche in – in der Regel ebenerdige – Kitas häufig vorkommen, verlangt entsprechende Vorkehrungen.

Hinweis – Was ist zu beachten?

Folgende Maßnahmen können die Risken, die sich aus Einbruchdiebstählen ergeben, verringern:

Außerhalb der Öffnungszeiten sollte die Hardware immer in abgeschlossenen Schränken aufbewahrt werden, so dass sie nicht sofort sichtbar ist.

Personenbezogene Daten der Datenschutzklassen II und III gemäß §§ 12, 13 KDG-DVO, um die es in der Kita regelmäßig geht, sind grundsätzlich nicht lokal, sondern auf zentralen Systemen in Räumen mit gesondertem Zutrittsschutz zu speichern. Sofern ausnahmsweise eine Speicherung auf lokalen Systemen erfolgt, ist diese Ausnahme zu begründen und sind die Systeme mit einem geeigneten Zugriffsschutz zu schützen, z. B. über eine Verschlüsselung der Festplatte nach aktuellem Stand der Technik.

Bei Geräten, die keine Verschlüsselung der Daten auf dem Gerät ermöglichen, wie z. B. Kameras, sollten die Daten in regelmäßigen, kurzen Abständen auf zentrale Systeme in besonders gegen unbefugten Zutritt gesicherten Räumen übertragen und von der Kamera gelöscht werden.

2.3.2. Verlust sensibler Schülerdaten – unverschlüsselter Stick

Im Bereich Schule hat sich gezeigt, dass auch hier z. T. noch mobile Speichermedien für sensible Daten genutzt werden, ohne diese durch Verschlüsselung zu schützen. In einem Fall ist ein unverschlüsselter USB-Stick mit umfangreichen Schülerlisten und Zeugnisnoten verloren gegangen. Weder der Verbleib des USB-Sticks noch die Frage, welche Daten konkret auf dem Stick gespeichert waren, konnten ermittelt werden.

Hinweis – Was ist zu beachten?

Gerade bei USB-Sticks besteht ein erhöhtes Verlustrisiko. Die Lehrer sollten angewiesen werden, Schülerdaten nur in genehmigten Ausnahmefällen auf USB-Sticks

zu speichern. Hierfür sollten ausschließlich schuleigene USB-Sticks genutzt werden, die angemessen verschlüsselt sind.

Die betreffenden Daten sollten mit Blick auf die Verfügbarkeit nicht ausschließlich auf dem USB-Stick gespeichert werden.

2.3.3. Umgang mit Fotos - Einwilligungsmanagement

Beim Thema Fotos von Kindern nehmen wir in Schulen und Kitas insgesamt einen sensiblen Umgang wahr. Insbesondere werden überwiegend umfassende Einwilligungserklärungen für die Nutzung der Fotos eingeholt. Ein Problem stellt sich hier aber oft an anderer Stelle, nämlich bei der Umsetzung der erteilten Einwilligungen. So erhalten wir Meldungen, dass Kinderfotos durch die Einrichtung veröffentlicht oder weitergegeben wurden, obwohl die Erziehungsberechtigten die Einwilligung bewusst nicht erteilt hatten.

Es genügt nicht, die Einwilligung mit dem Betreuungs- oder Schulvertrag abzufragen. Vielmehr müssen diese so aufbereitet werden, dass die Mitarbeiter, die letztlich mit den Fotos arbeiten, genau wissen, welche Kinder auf Fotoveröffentlichungen abgebildet sein dürfen und welche nicht. Auch müssen Aktualisierungen bekannt gemacht werden (beispielsweise bei einem Widerruf der Einwilligung).

Mit Blick darauf, dass untersagte Veröffentlichungen zum Teil erhebliche Folgen für die betroffenen Personen haben können, etwa wenn der Aufenthalt eines Kindes geheim bleiben muss, wird in der unzureichenden Umsetzung des Einwilligungsmanagements in diesem Bereich ein erheblicher Verstoß gegen datenschutzrechtliche Vorschriften gesehen.

Hinweis – Was ist zu beachten?

Ein funktionierendes Einwilligungsmanagement setzt neben der Gestaltung der Einwilligungserklärung (informierte Einwilligung) insbesondere voraus, dass alle am Prozess beteiligten Personen in der Einrichtung klar definiert sind und alle ihren Beitrag und ihre Verantwortung beim Umgang mit den Fotos kennen. Um sicherzustellen, dass jede erteilte, nicht erteilte und widerrufene Einwilligung auch Beachtung findet und mit den betreffenden Fotos entsprechend der vorliegenden Einwilligungen umgegangen wird, muss eine ausreichende Dokumentation mit allen Informationen dazu bereitgehalten werden. Diese Dokumentation ist aktuell zu

halten, um keine Änderungen zu übersehen. Wichtig ist auch eine regelmäßige Sensibilisierung der beteiligten Personen.

2.3.4. Unvollständige Zugriffskontrolle bei Schulsoftware

Insbesondere bei der einrichtungsübergreifenden Nutzung von Softwarelösungen für die Verarbeitung von Datenbeständen ist sicherzustellen, dass Nutzer nur auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können (Stichwort: Mandantentrennung). Um der grundsätzlichen Anforderung bei der Verarbeitung personenbezogener Daten nachzukommen, dass diese u.a. vor unbefugter und unrechtmäßiger Verarbeitung aber auch vor unbeabsichtigtem Verlust zu schützen sind (s. § 7 Abs. 1 lit. f) KDG), sind u.a. Maßnahmen zur Zugriffskontrolle zu ergreifen (s. § 6 Abs. 2 lit. c) KDG-DVO).

In der diesem Fall zugrundeliegenden Meldung einer Datenschutzverletzung waren diese Maßgaben, u.a. durch eine feingranulare Berechtigungsvergabe auf Softwareebene, berücksichtigt worden. Zu einer unbefugten Offenlegung kam es dennoch, da es neben dem Zugriff auf die Daten über die Software eine weitere, direkte Zugriffsmöglichkeit auf Dateiebene gab, die nicht ausreichend eingeschränkt war. Auf eben diese Umstände zielten dann auch die angeordneten Maßnahmen.

Hinweis – Was ist zu beachten?

Beim Einsatz von Softwarelösungen auf IT-Systemen ist die Implementierung von Berechtigungskonzepten, idealerweise unter Nutzung von Rollen und Rechten, die Methode der Wahl, um unberechtigte Datenzugriffe zu unterbinden. Zu einer umfänglichen Berechtigungsverwaltung gehören ferner noch eine regelmäßige Überprüfung der vergebenen Rollen und Rechte auf Aktualität.

Für einen wirkungsvollen, umfassenden Schutz ist die gesamte Architektur der Anwendung zu analysieren und alle Wege, über die ein Zugriff auf die verarbeiteten Daten möglich ist, sind zu berücksichtigen.

2.4. Caritas und Soziales

2.4.1. Diebstahl von Klientenakten

In der Meldung einer Datenschutzverletzung sind wir darüber informiert worden, dass ein Rucksack eines Mitarbeiters einer Beratungsstelle auf dem Arbeitsweg abhanden-

gekommen ist. In diesem Rucksack befanden sich mehrere sensible Dokumente und Daten sowie ein USB-Stick und eine Videokamera im Zusammenhang mit der Beratungstätigkeit.

Die Prüfung der in der Einrichtung ergriffenen Maßnahmen ergab, dass die Mitarbeiter nachweisbar regelmäßig Datenschutz-Schulungen erhalten. Zudem gab es interne Vorgaben zum Passwortschutz der Endgeräte und Zugänge. Eine Betriebsvereinbarung sah konkrete Vorgaben zum Datenschutz im Bereich der Dezentralen Arbeit vor. Dass es trotz der umfassenden Regelungen zu einem solchen Vorfall gekommen ist, lag zum Teil auch an menschlichen Fehlverhalten.

Bereits während der weiteren Ermittlungen hat die Einrichtung verdeutlicht, den Bereich des Dezentralen Arbeitens durch ergänzende Dienstanweisungen neu zu regeln. Auch sollten die Mitarbeiter erneut für den sicheren Transport von personenbezogen Daten insbesondere im Zusammenhang mit der Beratungstätigkeit sensibilisiert werden, sodass auf eine Anordnung verzichtet werden konnte.

Hinweis – Was ist zu beachten?

Bei der Verarbeitung von personenbezogenen Daten in Beratungseinrichtungen handelt es sich in der Regel um Daten der Datenschutzklasse III. Die besonderen Anforderungen, insbesondere die grundsätzlich vorzunehmende zentrale Speicherung, sind bereits in Abschnitt 2.3.1 dargestellt worden.

Sofern tatsächlich ein Transport von derart sensiblen Daten erforderlich ist, weil die Beratungstätigkeit auch zu Hause bei den Klienten durchgeführt wird, ist der Sensibilität der Daten durch entsprechende Maßnahmen zur Zugriffssicherung Rechnung zu tragen.

Wenn bei den Klienten unmittelbar Videoaufnahmen zu Beratungszwecken erhoben werden, muss sichergestellt werden, dass die Videoaufnahmen nicht unbeaufsichtigt, z. B. im Auto, verbleiben. Zum Beispiel können diese Videoaufnahmen auch unmittelbar nach Aufzeichnung in zentrale Systeme hochgeladen werden. So ist neben der Verfügbarkeit auch gleichzeitig die zentrale Speicherung der Daten sichergestellt.

2.4.2. Unzureichende Backup-Lösungen bei Daten der Datenschutzklasse III

Auch bei caritativen Einrichtungen kommt es häufiger zu Einbruchdiebstählen. In einem gemeldeten Fall ist ein mit Bitlocker verschlüsselter Laptop gestohlen worden.

Im Zusammenhang mit der weiteren Aufklärung des Sachverhalts ist aufgefallen, dass die Datensicherung auf einem unverschlüsselten mobilen Datenträger erfolgte. Diese Datensicherung lag im Zeitpunkt des Einbruchdiebstahls in räumlicher Nähe zu dem entwendeten Laptop, war jedoch nicht vom Diebstahl betroffen. In caritativen und anderen sozialen Einrichtungen werden wie bereits in Abschnitt 2.4.1 dargestellt in der Regel besonders sensible Daten verarbeitet, die überwiegend der Datenschutzklasse III zuzuordnen sind.

Die KDG-DVO sieht für personenbezogene Daten ab der Datenschutzklasse II gemäß § 12 Abs. 2 lit. d) KDG-DVO grundsätzlich eine zentrale Speicherung in besonders gegen unbefugten Zutritt gesicherten Räumen vor. Jedoch sind Ausnahmen möglich. Das Vorliegen eines solchen Ausnahmefalles entbindet allerdings nicht von der Pflicht, Sicherungskopien anzulegen, um die Verfügbarkeit der Daten sicherzustellen. Für Daten der Datenschutzklasse II und III sieht § 12 Abs. 2 lit c) KDG-DVO vor, dass Sicherungskopien vor Fremdzugriff und der gleichzeitigen Vernichtung mit den Originaldaten zu schützen sind. Daher reicht es gerade nicht aus, die Daten als Backup auf einer externen Festplatte zu speichern und diese in räumlicher Nähe zum Originaldatenträger aufzubewahren. Dies trifft erst recht auch auf interne Festplatten desselben IT-Systems sowie auf USB-Sticks zu, welche permanent an einem Laptop angeschlossen sind.

Hinweis – Was ist zu beachten?

Für Daten der Datenschutzklasse II und höher muss deren Verfügbarkeit durch die Erstellung von Sicherungskopien gewährleistet sein. Diese Kopien müssen – bei entsprechender Zugriffssicherung – vor der gleichzeitigen Vernichtung mit den Originaldaten geschützt werden. Idealerweise werden Sicherungskopien an unterschiedlichen geographischen Orten gelagert, zumindest aber in unterschiedlichen Brandabschnitten. Für weitere Überlegungen zur Backup-Strategie siehe auch Abschnitt 2.1.5.

2.5. Prüfungen 2023

Die Meldung einer Datenschutzverletzung durch eine Kita, die auch an der Querschnittsprüfung Kita (vgl. 8. Jahresbericht 2021) teilgenommen hat, war der Anlass für eine Nachprüfung in dieser Einrichtung. Dabei zeigte sich, dass die Anordnung im damaligen Bescheid, den Laptop zu verschlüsseln, durch die Kita nicht umgesetzt worden ist.

Daraufhin sind insgesamt zwölf Teilnehmer der Querschnittsprüfung ausgewählt worden, bei denen geprüft werden sollte, ob die erlassenen Anordnungen umgesetzt worden sind.

Insgesamt drei Einrichtungen konnten unmittelbar einen entsprechenden Nachweis über die Umsetzung der Anordnungen einreichen. Weitere sieben Einrichtungen haben die Anordnungen ebenfalls umgesetzt. Bei diesen sind jedoch noch ergänzende Hinweise erteilt worden. Bei den Hinweisen handelte es sich um Klarstellungen, welche ergänzenden Maßnahmen berücksichtigt werden sollten.

Bei zwei Einrichtungen war es erforderlich, einen Vor-Ort-Termin anzusetzen. Der erste Vor-Ort-Termin konnte noch im Berichtszeitraum abgeschlossen werden. Hierbei zeigte sich, dass bereits zahlreiche Dokumente und Regelungen in der Einrichtung vorhanden waren. Überwiegend fehlte es jedoch an deren Individualisierung bezogen auf die konkrete Einrichtung. Auch an der konkreten Umsetzung der vorhandenen Regelungen mangelte es zum Teil. Ein erneuter Besuch der Einrichtung ist in 2024 geplant.

2.6. Zusammenarbeit und Veranstaltungen

2.6.1. Ökumenischer Datenschutztag

Wie in den Jahren zuvor fand auch in 2023 der Ökumenische Datenschutztag statt. Veranstaltungsort der zweitägigen Veranstaltung war die Stadt Essen. Ein Thema war wie bereits in den vergangenen Jahren das Kirchliche Datenschutzmodell, welches auf der eigens dafür eingerichteten Homepage veröffentlicht worden ist. Weitere Einzelheiten hierzu sind im Abschnitt 3.1 zu finden.

2.6.2. Konferenz der Diözesandatenschutzbeauftragten

Die Konferenz der Diözesandatenschutzbeauftragten tagt mehrfach im Jahr nach einem abgestimmten Verfahrensablauf. Die Konferenz fördert den Datenschutz und verständigt sich auf gemeinsame Positionen bei zentralen und bistumsübergreifenden Fragestellungen. Dies geschieht unter anderem durch Entschließungen, Beschlüsse oder Orientierungshilfen, Stellungnahmen oder Pressemitteilungen. Der jeweils für ein Jahr gewählte Sprecher der Konferenz nimmt neben den sitzungsorganisatorischen Belangen u. a. auch die Kontaktfunktion zur Konferenz der staatlichen Datenschutzbeauftragten wahr. Im Berichtsjahr 2023 war Herr Ullrich von der Kirchlichen Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs Sprecher der Konferenz. Zur Sprecherin für das Jahr 2024 ist Frau Becker-Rathmair vom Katholischen Datenschutzzentrum Frankfurt/M. gewählt worden.

2.6.3. Arbeitskreise der Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) als Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder hat mehrere Arbeitskreise etabliert, in denen die Entscheidungen der DSK vorbereitet werden. Die Konferenz der Diözesandatenschutzbeauftragten ist über Vertreter an einigen Arbeitskreisen beteiligt.

Die Katholische Datenschutzaufsicht Nord nimmt in Vertretung für die Konferenz der Diözesandatenschutzbeauftragten am Arbeitskreis Technik und seit September 2023 auch am Arbeitskreis Medien teil.

Der Arbeitskreis Technik findet unter Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern halbjährlich statt.

Der Arbeitskreis Medien findet unter Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit und dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ebenfalls zweimal jährlich statt.

Die Teilnahme an den Arbeitskreisen der DSK bietet eine gute Möglichkeit zum gemeinsamen fachlichen Austausch zwischen den kirchlichen und staatlichen Datenschutzaufsichten und stellt die einheitliche Anwendung und Auslegung datenschutzrechtlicher Vorschriften sicher.

2.6.4. Informationsveranstaltungen

Auch in 2023 konnten die regelmäßigen Treffen sowohl mit den betrieblichen Datenschutzbeauftragten als auch mit den Referatsleitern der IT-Abteilungen der Bistümer im Rahmen der IT-Tagung fortgesetzt werden. Diese Treffen bieten sowohl für die Teilnehmer der Veranstaltungen als auch für die Katholische Datenschutzaufsicht Nord eine gute Gelegenheit zum gemeinsamen Austausch. Aktuelle Fälle sowie die hieraus abgeleiteten Maßnahmen und Empfehlungen aus unserer Tätigkeit können über diese Foren frühzeitig angebracht werden, damit diese bei der Beratung berücksichtigt werden können.

3. Weitere Themen

3.1. KDM

Beim Kirchlichen Datenschutzmodell (KDM), das auf der Version 2.0b des Standard-Datenschutzmodells (SDM) basiert, konnte die Erarbeitung eines fiktiven Praxisbeispiels und damit die Arbeit der zugehörigen UAG abgeschlossen werden; dazu zählte auch die Erstellung von Arbeitsmaterialien/Werkzeugen für die universelle Anwendung des KDM selbst. Die Verarbeitungstätigkeit „Bildungs- und Entwicklungsdokumentation eines Kindes in einer Kindertageseinrichtung“ ist Gegenstand des Beispiels gewesen und die Ergebnisse wurden mit Meldung aus Mai 2023 von der ökumenischen Arbeitsgruppe auf der Webseite https://www.kirchliches-datenschutzmodell.de zur Verfügung gestellt.

Die entwickelten und anhand des gewählten Beispiels exemplarisch ausgefüllten Unterlagen umfassen neben einem Arbeitsdokument auch eine zugehörige Arbeitstabelle sowie Erläuterungen zur Anwendung. Sie bieten eine Hilfestellung zur Anwendung des KDM, d. h. insbesondere zur Beschreibung der Verarbeitungstätigkeit sowie zur Durchführung einer Risikoanalyse und Risikobehandlung, u. a. auf der Grundlage der in den SDM-Bausteinen hinterlegten Maßnahmen.

Die Entwicklung im SDM soll weiterhin beobachtet und die ökumenische Arbeit fortgesetzt werden.

3.2. Künstliche Intelligenz (KI)

Mit der kostenfreien, öffentlichen Verfügbarkeit von ChatGPT seit November 2022, einem Chatbot und virtuellen Assistenten, der auf LLMs (Large Language Models) beruht, geriet der Forschungs- und Anwendungsbereich von KI-Methoden (auch AI, Artificial Intelligence) in den Fokus einer größeren Öffentlichkeit. Dabei bezeichnet „*Künstliche Intelligenz (KI) […] ein Teilgebiet der Informatik, welches sich mit der Erforschung von Mechanismen des intelligenten menschlichen Verhaltens befasst. Dabei geht es darum, technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu „lernen“ und mit Unsicherheiten umzugehen, statt klassisch programmiert zu werden*.“[37]

[37] Deutscher Bundestag, Drucksache 19/1982, S.2 https://dserver.bundestag.de/btd/19/019/1901982.pdf (Abruf: 12.08.2024)

Die Einsatzbereiche der im Folgenden von verschiedenen Firmen veröffentlichten Vielzahl von Chatbots bzw. generativer KI-Verfahren erstreckten sich neben dem Bereich der Text- u.a. auch auf den der Bild- und Videoerstellung.

Dabei können die Eingaben der Nutzer von den Tools durchaus als weitere Informationsquelle genutzt werden, um den eigenen Datenbestand zu erweitern und auch mit Hilfe der Eingabedaten das eigene Modell zu optimieren.

Die Leistungen der KI-Methoden im Bereich der Generierung von Texten, Fotos und Videos sind zweifelsohne auf mehreren Ebenen beeindruckend, bergen aber gleichzeitig das Potenzial einer missbräuchlichen Nutzung, z. B. im Zusammenhang mit der Generierung von glaubwürdigen Phishing-Nachrichten, der Generierung von Falsch-Nachrichten oder aber der Diskreditierung oder Erpressung von Personen durch manipulierte Bilder oder Videos.

Hinsichtlich der Konformität bzgl. der Anforderungen aus dem KDG unterscheiden sich KI-Methoden nur unwesentlich von anderen Verfahren, mit denen personenbezogene Daten verarbeitet werden. Zunächst besteht die Erforderlichkeit einer Rechtsgrundlage für die Verarbeitung (ggf. besonderer Kategorien) personenbezogener Daten. Ferner bestehen u.a. die Anforderung der Zweckbindung (§ 7 Abs. 1 lit. b) KDG), das Gebot der Datensparsamkeit (§ 7 Abs. 1 lit. c), e) KDG) und die Transparenzpflicht (§ 7 Abs. 2 KDG, §§ 14-16 KDG). Letztere enthält die Informationspflichten, die auch eine Beschreibung der eingesetzten Verfahren und der Empfänger oder Kategorien von Empfängern umfassen. Nicht zuletzt müssen die Betroffenenrechte (insbesondere das Auskunftsrecht, das Recht auf Berichtigung und das Recht auf Löschung) wahrgenommen werden können. Sofern die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat, ist ferner gemäß § 35 KDG vorab eine Datenschutz-Folgenabschätzung durchzuführen, die u.a. eine systematische Beschreibung der geplanten Vorgänge und Datenflüsse erfordert.

3.3. Patch-Management

Ein regelmäßiges Patch-Management, die Planung von Systemaktualisierungen, ist eine der Maßnahmen, die der für die Verarbeitung von personenbezogenen Daten Verantwortliche treffen muss, um die Sicherheit der personenbezogenen Daten zu gewährleisten (siehe § 16 Abs. 3 KDG-DVO). Eines der damit verfolgten Ziele ist der Schutz vor Schadsoftware, die Schwachstellen in IT-Systemen ausnutzt, um bspw. die Vertraulichkeit, Integrität oder Verfügbarkeit der IT-Systeme zu beeinträchtigen

oder der auf diesen Systemen verarbeiteten (personenbezogenen) Daten zu kompromittieren.

Diese Schwachstellen können auf verschiedenen Ebenen, wie etwa Firmware, Betriebssystem, aber auch Anwendungen auf Clients und Servern bestehen.

Abhilfe bietet das Einspielen von bereitgestellten Sicherheitsupdates – sofern die Schwachstellen bekannt sind und entsprechende „Patches“ zu Verfügung stehen. Anders verhält es sich bei Schwachstellen, die u. U. auch dem Hersteller bislang unbekannt sind oder für die noch kein Patch existiert; hier bieten ggf. vorläufige Behelfslösungen (wie etwa die vorübergehende Deaktivierung einzelner Dienste oder zusätzliche Einschränkungen auf Netzwerkebene) Abhilfe, die vor einem Ausnutzen der Schwachstellen und einer Kompromittierung schützen können.

Um eine zeitnahe Versorgung mit Sicherheitsupdates sicherzustellen, besteht zum einen die Möglichkeit betriebssystem- oder programminterne Update-Mechanismen zu aktivieren, andererseits informieren die meisten Produkthersteller über weitere Kanäle zu bereitstehenden Sicherheitsupdates.

Hersteller- und produktübergreifende Informationen sind u.a. auch auf dedizierten Webseiten und Feeds zu finden. So bietet bspw. das Bundesamt für Sicherheit in der Informationstechnik den „Warn- und Informationsdienst“ (WID) an[38], über den Hersteller-übergreifende Informationen abgerufen werden können.

Erwähnenswert ist in diesem Zusammenhang auch der „Known Exploited Vulnerabilities Catalog“[39] der US-amerikanischen Cybersecurity & Infrastructure Security Agency (CISA). In diesem Katalog sind Schwachstellen aufgeführt, deren Ausnutzung in der Praxis („in the wild“) bereits beobachtet worden ist. Diese Information kann bspw. dann hilfreich sein, wenn verschiedene Patch-Management-Aktivitäten priorisiert oder im Rahmen einer Risikoanalyse betrachtet werden müssen. Detaillierte Informationen sind auf der zugehörigen Webseite zu finden.[40]

Produkte, für die die Versorgung mit Sicherheitsupdates eingestellt worden ist, sind einer besonderen Bedrohung ausgesetzt, da bestehende sowie auch fortan gefundene Schwachstellen nicht mehr seitens des Herstellers ausgebessert werden. Dies stellt oftmals – insbesondere, wenn diese Geräte in exponierter Lage betrieben werden – ein nicht akzeptables Risiko dar.

[38] https://wid.cert-bund.de/portal/wid/kurzinformationen (Abruf: 12.08.2024) oder als RSS-Feed: https://wid.cert-bund.de/content/public/securityAdvisory/rss (Abruf: 12.08.2024)
[39] https://www.cisa.gov/known-exploited-vulnerabilities-catalog (Abruf: 12.08.2024)
[40] https://www.cisa.gov/known-exploited-vulnerabilities (Abruf: 12.08.2024)

3.4. Social Media

Mit Bescheid vom 17. Februar 2023 hat der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI) dem Presse- und Informationsamt der Bundesregierung (BPA) die „*Verarbeitung personenbezogener Daten im Rahmen der von der Bundesregierung betriebenen Facebook-Fanpage […] durch Einstellen ihres Betriebs untersagt.*“[41]

Zur Begründung führt der BfDI aus, dass die Verarbeitung von personenbezogenen Daten bei dem Betrieb der Facebook-Fanpage datenschutzrechtlich nicht gerechtfertigt sei, da weder eine geeignete Rechtsgrundlage noch eine wirksame Einwilligung der Nutzer vorliege.[42] Ebenso habe es das BPA versäumt, im Rahmen seiner Rechenschaftspflichten einen rechtmäßigen Betrieb der Facebook-Fanpage nachzuweisen. Der Nachweis der Rechtmäßigkeit könne zudem gar nicht geführt werden, da das BPA nicht genügend Informationen seitens Meta (Facebook) habe, „*aufgrund welcher Rechtsgrundlage und zu welchen konkreten Zwecken die Datenverarbeitungen stattfinden.*“[43]

Gegen diese Entscheidung hat das Presse- und Informationsamt der Bundesregierung am 16. März 2023 Klage beim zuständigen Verwaltungsgericht in Köln (Az.: 13 K 1419/23) eingereicht.

Die Konferenz der Diözesandatenschutzbeauftragten hat bereits mehrfach die Empfehlung ausgesprochen, auf den Betrieb einer Facebook-Fanpage zu verzichten.

[41] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1 (Abruf: 12.08.2024)
[42] aao. Seite 36
[43] aao. Seite 38

4. Katholische Datenschutzaufsicht Nord

4.1. Aufgaben

Die Aufgaben der Katholischen Datenschutzaufsicht Nord sind in § 44 KDG geregelt. Hiernach wacht die Datenschutzaufsicht über die Einhaltung der Vorschriften aus dem KDG sowie anderer Vorschriften über den Datenschutz.

Die Aufgabe des Diözesandatenschutzbeauftragten und seiner Mitarbeiter besteht in der Erhaltung des verfassungsmäßigen Rechts des Einzelnen auf Wahrung seiner informationellen Selbstbestimmung und damit der Möglichkeit, sein Leben in freier, selbstbestimmter Verantwortung zu führen.

Das Ziel wird durch eine Reihe von Maßnahmen erreicht.

- Durchführung von Prüfungen
- Bearbeitung von datenschutzrechtlichen Beschwerden
- Erlass von Anordnungen und ggf. Verhängung von Bußgeldern bei Verstößen gegen datenschutzrechtliche Vorschriften
- Durchführung von datenschutzrechtlichen Prüfungen in den jeweiligen Einrichtungen
- Beratung und Sensibilisierung von kirchlichen Stellen sowie Aussprechen von Empfehlungen zur Verbesserung des Datenschutzes

4.2. Struktur

Die geplante Umsetzung der rechtlichen Neustrukturierung der Katholischen Datenschutzaufsicht Nord in eine Körperschaft des öffentlichen Rechts ist – trotz der optimistischen Erwartungen (siehe Tätigkeitsbericht 2022) – auch im Berichtsjahr noch nicht vollendet worden. Wir schauen jedoch weiterhin optimistisch ins folgende Jahr.

Zur Erfüllung der Aufgaben wird dem Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung gestellt.

Die frei gewordene Stelle konnte durch öffentliche Ausschreibung zum 1. November 2023 nachbesetzt werden. Zum Ende des Berichtsjahres waren die zur Verfügung stehenden vier Stellen besetzt.

4.3. Finanzen

Die Personal- und Sachkosten der Katholischen Datenschutzaufsicht Nord werden durch eine Finanzumlage der beteiligten (Erz-)Bistümer und des Bischöflich Münsterschen Offizialats in Vechta nach einem vereinbarten Schlüssel getragen.

Die Finanz- und Budgethoheit liegt beim Diözesandatenschutzbeauftragten. Die Abwicklung des Haushaltes erfolgt über die Finanzabteilung des bischöflichen Generalvikariates Osnabrück als Belegenheitsbistum für die Stadt Bremen.

Für das Kalenderjahr 2023 wurden Haushaltsmittel in Höhe von 298.920 EUR aufgewendet. Die Haushaltsmittel für das Kalenderjahr 2022 betrugen 418.322 EUR.

Schlussbemerkung

Das im Jahr 2023 großgeschriebene Thema der Künstlichen Intelligenz, die datenschutzrechtlichen Implikationen sowie mögliche Einsatzszenarien sind zumindest bisher noch nicht an uns herangetragen worden. Aufgrund der immer schnelleren Entwicklung dieser Themen und auch der zunehmenden Relevanz für kirchliche Einrichtungen, insbesondere in den kirchlichen Krankenhäusern, gehen wir davon aus, dass das Thema künftig verstärkt auch in den Fokus unserer aufsichtsrechtlichen Tätigkeit rücken wird.

Prüfungen sind und bleiben das Mittel der Wahl, wenn es darum geht zu erfahren, wie die datenschutzrechtlichen Vorgaben in den einzelnen Einrichtungen umgesetzt werden. Aus diesem Grund wird der Fokus für das Jahr 2024 auf umfangreichere Prüfungen gelegt. So soll ein noch näher zu bestimmendes Einzelverfahren in Beratungsstellen der Caritas vorerst auf Grundlage einer Dokumentenprüfung Gegenstand einer Prüfung werden. Weiterhin ist beabsichtigt, den Einsatz von Videoüberwachungsanlagen in Bildungseinrichtungen zu prüfen. Zur datenschutzrechtlichen Bewertung des konkreten Einsatzes von Videoüberwachungsanlagen sind neben der Sichtung von Konzepten, Lageplanskizzen und Screenshots ebenso Vor-Ort-Besichtigungen vorgesehen. Erstmalig soll ein grundsätzliches Thema mit einer breit angelegten Umfrage behandelt werden. Gegenstand dieser Umfrage wird schwerpunktmäßig die konkrete Umsetzung des Verfahrens zum Umgang mit Datenschutzverletzungen in vorwiegend kleineren Einrichtungen sein. Die Ergebnisse und Erkenntnisse aus dieser Umfrage werden ebenfalls veröffentlicht.

Auch das Jahr 2024 wird ein in vielerlei Hinsicht spannendes Jahr.

Katholische Datenschutzaufsicht Nord
Unser Lieben Frauen Kirchhof 20
28195 Bremen

Telefon: 0421 330056-0
E-Mail: info@kdsa-nord.de
https://www.kdsa-nord.de