Katholische
Datenschutzaufsicht Nord

11. Jahresbericht

2024

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

Redaktionsschluss: 31. Mai 2025

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

Im diesjährigen Tätigkeitsbericht soll neben der relevanten Entwicklung im europäischen Recht auch die Gesetzgebung innerhalb der norddeutschen (Erz-)Bistümer näher betrachtet werden. In diesem Zusammenhang hatten viele (Erz-)Bistümer bereits in den vergangenen Jahren die „Musterordnung zur Regelung von Einsichts- und Auskunftsrechten für die Kommissionen zur Aufarbeitung sexuellen Missbrauchs Minderjähriger und schutz- oder hilfebedürftiger Erwachsener, für Forschungszwecke und für Rechtsanwaltskanzleien“ in Kraft gesetzt. Die norddeutschen (Erz-)Bistümer haben im Berichtsjahr nun ebenfalls entsprechende Regelungen verabschiedet. Das Bistum Osnabrück und das Bistum Hildesheim haben auf der Grundlage der erstellten Ordnungen nunmehr im Rahmen einer Interessenabwägung die Möglichkeit, den Unabhängigen Aufarbeitungskommissionen personenbezogene Daten zukommen zu lassen. Das Erzbistum Hamburg hingegen setzt im Hinblick auf die Missbrauchsopfer von vornherein explizit eine Einwilligung voraus.

Im Berichtszeitraum ist in Kooperation mit dem Katholischen Datenschutzzentrum Frankfurt/M. eine Sensibilisierungskampagne zum Umgang mit Datenschutzverletzungen gestartet. Die Ergebnisse werden im nächsten Tätigkeitsbericht dargestellt.

Eine größere Prüfungsaktion wird bei den Schulen in katholischer Trägerschaft durchgeführt. Ziel hierbei ist die Kontrolle des rechtmäßigen und sicheren Betriebs von Videoüberwachungsanlagen. In diesem Bericht werden die möglichen Prüfungspunkte noch einmal ausführlich beschrieben.

Wie in jedem Tätigkeitsbericht sollen auch in diesem Jahr die relevantesten Fälle aus der Tätigkeit der Katholischen Datenschutzaufsicht Nord kurz dargestellt und erläutert werden.

Ich wünsche Ihnen viel Freude bei der Lektüre des 11. Tätigkeitsberichts.

Bremen, im Oktober 2025

Andreas Bloms
Diözesandatenschutzbeauftragter

1. Aktuelle Entwicklungen im Datenschutz und Bedeutung für kirchliche Stellen

1.1. Europarecht

Im Folgenden sollen die auch für das Kirchliche Datenschutzrecht relevanten Neuerungen und Veröffentlichungen auf europäischer Ebene dargestellt werden. Hierzu gehören neben Änderungen der Datenschutz-Grundverordnung (DSGVO) und der relevanten Rechtsprechung des Europäischen Gerichtshofs (EuGH) auch Veröffentlichungen des Europäischen Datenschutzausschusses (EDSA). Dieser Ausschuss soll eine einheitliche Anwendung der DSGVO auf europäischer Ebene sicherstellen.

1.1.1. KI-Verordnung

Am 1. August 2024 ist die Verordnung über künstliche Intelligenz[1] in Kraft getreten. Der risikobasierte Ansatz der Verordnung unterscheidet zwischen risikoarmen KI-Systemen, bestimmten KI-Systemen mit Transparenzpflichten, Hochrisiko-KI-Systemen und KI-Systemen mit unannehmbaren Risiken.

Der Einsatz von KI-Systemen mit einem nicht hinnehmbaren Risiko wird ganz verboten. Hierzu gehören KI-Systeme, welche z.B. menschliches Verhalten manipulieren oder gem. Art. 5 Abs. 1 lit. e) Verordnung über künstliche Intelligenz „Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet […] erstellen oder erweitern."

Zu den Hochrisiko-KI-Systemen gehören nach Anhang III der Verordnung z. B. „KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten." Der Einsatz von Hochrisiko-KI-Systemen unterliegt erweiterten Voraussetzungen nach Kapitel 3 Abschnitt 2 der Verordnung. Hierzu gehören u.a. die Einrichtung eines Risikomanagementsystems, die Protokollierung der Vorgänge sowie die menschliche Aufsicht des KI-Systems.

Bei KI-Systemen, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, muss in der Regel sichergestellt werden, dass die Nutzer darüber informiert werden, dass sie mit einem KI-System interagieren. Zu diesen KI-Systemen gehören z. B. Chatbots. KI-Systeme, welche z. B. dazu bestimmt sind, eine eng gefasste Verfahrensaufgabe durchzuführen, unterliegen nicht diesen Informationspflichten.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L_202401689 (letzter Abruf: 01.09.2025)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat eine Orientierungshilfe zum Thema „Künstliche Intelligenz und Datenschutz“[2] herausgebracht. Die Orientierungshilfe richtet sich in erster Linie an Unternehmen, Behörden und andere Organisationen, die beabsichtigen, KI-Systeme für die Verarbeitung personenbezogener Daten einzusetzen. Ebenso hat sich der Europäische Datenschutzausschuss in einer „Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen“[3] vom 2. Dezember 2024 geäußert.

Die Nutzung von KI-Systemen ist in vielen kirchlichen Einrichtungen denkbar und möglich. Nicht zuletzt aufgrund der verschiedenen KI-Modelle ist es wichtig, die datenschutzrechtlichen Regelungen des KDG von Beginn an (bei der Erstentscheidung und Auswahl eines Systems) und in jeder Phase (Implementierung, ggf. Training, Einsatz etc.) zu berücksichtigen. In den meisten Fällen dürfte die Durchführung einer Datenschutz-Folgenabschätzung erforderlich sein.

1.1.2. Zertifizierung nach Art. 42 DSGVO

Nach Art. 42 DSGVO besteht die Möglichkeit der Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass die DSGVO bei Verarbeitungstätigkeiten von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Die Regelung ist nicht neu, hatte jedoch mangels vorhandener Zertifikate noch keine praktische Relevanz für die Einrichtungen.

Das erste für Deutschland geltende Art. 42 DSGVO-Zertifikat konnte nach einem langen Akkreditierungsprozess im Februar 2024 von der EuroPriSe Cert GmbH[4] für Auftragsverarbeiter angeboten werden.[5]

Im Hinblick auf die technischen und organisatorischen Maßnahmen (§ 26 Abs. 4 KDG), die Technikgestaltung und Voreinstellung (§ 27 Abs. 3 KDG) sowie die Verarbeitung personenbezogener Daten im Auftrag (§ 29 Abs. 6 KDG) kann ein nach europäischem Recht genehmigtes Zertifizierungsverfahren als Faktor herangezogenen

[2] https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf (letzter Abruf: 01.09.2025)
[3] https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf (letzter Abruf: 01.09.2025)
[4] Zum Redaktionsschluss dieses Berichts hat die EuroPriSe Cert GmbH ihren Geschäftsbetrieb vollständig eingestellt. https://web.archive.org/web/20250615061114/https://euprivacyseal.com/de/ (letzter Abruf: 01.09.2025)
[5] https://www.ldi.nrw.de/ldi-nrw-erteilt-die-befugnis-fuer-erste-deutsche-zertifizierungsstelle (letzter Abruf: 01.09.2025)

werden, um hinreichende Garantien für die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen zu können.

Eine Zertifizierung gemäß Art. 42 DSGVO kann daher bei der Auswahl der Auftragsverarbeiter eine Entscheidungshilfe auch für kirchliche Einrichtungen sein. Darüber hinaus kann die Überprüfung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters, die mindestens im Abstand von zwei Jahren erfolgen muss, durch die Vorlage eines entsprechenden Zertifikats ersetzt bzw. ergänzt werden (§ 15 Abs. 5 S. 2 KDG-DVO); je nach Inhalt des Kriterienkatalogs, der einem Datenschutzsiegel zugrunde liegt, ist dann ggf. ergänzend die Einhaltung spezifischer Regelungen aus dem KDG bzw. der KDG-DVO zu prüfen.

1.1.3. EuGH - Mündliche Übermittlung von Informationen fällt in den Anwendungsbereich der DSGVO

Aufgrund eines Vorabentscheidungsersuchens hatte der EuGH in seiner Entscheidung (EuGH, Urteil v. 07.03.2024 – C-740/22 EuGH[6]) die Frage zu beantworten, ob eine mündliche Auskunft als eine Verarbeitung angesehen werden kann und ob diese in den Anwendungsbereich der DSGVO fällt.

Hintergrund

Der Begriff der "Verarbeitung“ ist in Art. 4 Ziffer 2 DSGVO definiert als jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte[r] Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ wie (u.a.) die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Durch die weite Formulierung „jeder Vorgang“ und des „wie“ vor der Aufzählung möglicher Verarbeitungsformen kommt der EuGH zu dem Ergebnis, dass auch die mündliche Übermittlung als „Verarbeitung“ anzusehen ist.

Ferner hatte das Gericht zu prüfen, ob die mündliche Verarbeitung in den Anwendungsbereich der DSGVO fällt. Nach Art. 2 Abs. 1 DSGVO gilt die Verordnung für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62022CJ0740 (letzter Abruf: 01.09.2025)

Hierzu stellte der EuGH fest:

> *„Im vorliegenden Fall geht aus dem Vorabentscheidungsersuchen hervor, dass die von der Klägerin des Ausgangsverfahren angefragten Daten in einem „Personenregister eines Gerichts“ enthalten sind. […] Daher ist auf die erste Frage zu antworten, dass Art. 2 Abs. 1 und Art. 4 Nr. 2 DSGVO dahin auszulegen sind, dass eine mündliche Auskunft über möglicherweise verhängte oder bereits verbüßte Strafen in Bezug auf eine natürliche Person eine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 Verordnung darstellt, die in den sachlichen Anwendungsbereich dieser Verordnung fällt, wenn diese Informationen in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“*
>
> *(aao., Rn. 38 f.)*

Der EuGH kommt somit zu dem Ergebnis, dass auch die mündliche Auskunft aus einem Dateisystem den Anforderungen der DSGVO unterliegt. Da sowohl der Begriff der „Verarbeitung“ als auch der sachliche Anwendungsbereich der DSGVO mit dem KDG gleichlautend sind, sind die Grundsätze auf das KDG zu übertragen.

1.1.4. EuGH – Begriff des Gesundheitsdatums ist weit auszulegen

In einer anderen Entscheidung äußerte sich der EuGH zur Frage, ob es sich bei Bestelldaten, die im Rahmen einer Online-Arzneimittelbestellung anzugeben sind, wie Name, Lieferadresse, Angaben zum bestellten Medikament, bereits um Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO handelt, auch wenn es sich um nicht verschreibungspflichtige Medikamente handelt. (EuGH, Urteil v. 04.10.2024 – C-21/23)[7]

Hintergrund

Gesundheitsdaten sind den besonderen Kategorien personenbezogener Daten zuzuordnen und unterliegen den strengen Anforderungen des Art. 9 DSGVO. Nach der Definition in Art. 4 Nr. 15 DSGVO sind „Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Hierzu stellte der EuGH fest:

> *„Damit personenbezogene Daten als Gesundheitsdaten […] eingestuft werden können, genügt folglich, dass aus diesen Daten mittels gedanklicher*

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62023CJ0021 (letzter Abruf: 01.09.2025)

Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden kann […].“
(aao., Rn. 83)

Der EuGH bekräftigt damit, dass der Begriff Gesundheitsdaten weit zu fassen ist und der Bezug der Personendaten zu einem (frei verkäuflichen) Medikament ausreichend ist.

Diese Grundsätze können auf das KDG übertragen werden und haben zum Beispiel bei der Zuordnung von personenbezogenen Daten in die Datenschutzklassen Relevanz. Allein der Kontext, in dem (isoliert betrachtet) wenig sensible Daten wie Name und Anschrift verarbeitet werden, kann dazu führen, dass die Datenschutzklasse III anzunehmen ist. Das erfordert zum einen die Ergreifung erhöhter IT-Sicherheitsmaßnahmen und ist zum anderen bei der Frage einer Benachrichtigungspflicht i.S.d. § 34 KDG zu berücksichtigen.

1.2. Bundesrecht

Zu dem bereits in den Bundestag eingebrachten Gesetz zur Änderung des Bundesdatenschutzgesetzes, welches noch im August 2023 als Referentenentwurf vorlag, fand am 15. Mai 2024 die erste Beratung statt. Dieses Gesetz ist vor der Beendigung der Legislaturperiode jedoch nicht mehr durch den Bundestag verabschiedet worden. Ein neuer Entwurf zur Änderung des Bundesdatenschutzgesetzes liegt noch nicht vor.

Zum geplanten Beschäftigtendatenschutzgesetz, für das im Oktober 2024 ein Referentenentwurf vorgelegt wurde, gibt es noch keine Fortschritte. Mit der neuen Regierung scheint unklar, ob dieses Gesetz, das einen besonders verantwortungsvollen Umgang mit Beschäftigtendaten sicherstellen und für mehr Rechtssicherheit sorgen soll, noch angestrebt wird.

1.3. Datenschutzrecht der Kirche

1.3.1. Gesetzgebung Bistümer

1.3.1.1. Ordnungen zur Regelung von Auskunfts- und Einsichtsrechten zur Aufarbeitung sexualisierter Gewalt

Sowohl das Erzbistum Hamburg[8] als auch das Bistum Hildesheim[9] und das Bistum Osnabrück[10] haben im Jahr 2024 Regelungen zu Auskunfts- und Einsichtsrechten zur Aufarbeitung sexualisierter Gewalt erlassen. Zur sicheren Verarbeitung der in diesem Rahmen verarbeiteten personenbezogenen Daten durch den Datenempfänger siehe Abschnitt 1.3.3.

Bistum Osnabrück und Bistum Hildesheim

Die Ordnungen im Bistum Osnabrück und im Bistum Hildesheim sind im Wesentlichen gleichlautend. Drei Voraussetzungen müssen kumulativ nach § 2 der jeweiligen Ordnung erfüllt sein.

Zunächst muss geprüft werden, ob die Offenlegung der personenbezogenen Daten für die Durchführung der Aufarbeitung erforderlich ist.

Die zweite Voraussetzung ist, dass die Nutzung von anonymisierten Daten zu diesem Zweck nicht möglich oder die Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden ist. Der Verantwortliche hat somit für den jeweiligen Vorgang festzustellen und zu dokumentieren, dass eine Anonymisierung im Einzelfall nicht erfolgen kann. Sofern eine Anonymisierung erfolgen kann, sind die personenbezogenen Daten zu anonymisieren. Die Prüfung, ob eine Anonymisierung möglich ist, ist in jedem Einzelfall vorrangig vor der Interessenabwägung durchzuführen.

Im dritten Schritt sind das in § 1 der Ordnungen verankerte besondere kirchliche Interesse an der Aufarbeitung und die schutzwürdigen Interessen der betroffenen Person gegeneinander abzuwägen, wobei das besondere kirchliche Interesse an der Aufarbeitung die schutzwürdigen Interessen der betroffenen Person erheblich überwiegen muss. Auch diese Interessenabwägung ist zu dokumentieren. Zu einer datenschutzrechtlichen Interessenabwägung hat der EuGH festgestellt, dass bei „*der entsprechenden Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen […] insbesondere die vernünftigen Erwartungen der betroffenen Person*

[8] https://erzbistum-hamburg.de/_amtsblatt/2024/202410.pdf (letzter Abruf: 01.09.2025)
[9] https://www.bistum-hildesheim.de/fileadmin/dateien/PDFs/Materialboerse/Kirchlicher_Anzeiger/KA-2024-04.pdf (letzter Abruf: 01.09.2025)
[10] https://www.dioezesanbibliothek-osnabrueck.de/app/download/8213116481/06-2024.pdf?t=1740658658 (letzter Abruf: 01.09.2025)

sowie der Umfang der fraglichen Verarbeitung und deren Auswirkungen auf diese Person zu berücksichtigen“ (EuGH, Urteil v. 04.07.2023 – C-252/21, Rn. 116[11]) sind. Dieser Aspekt erlangt bei der Interessenabwägung insbesondere bezogen auf die vom Missbrauch betroffenen Personen besonderes Gewicht. Weiterhin sind – evtl. im Vorfeld getätigte – Zusagen an vom Missbrauch betroffene Personen, die erhobenen und gespeicherten personenbezogenen Daten nicht offenzulegen, ebenfalls zu beachten. Diese Zusagen können nicht durch später erlassene Rechtsgrundlagen aufgehoben werden. In solchen Fällen bleibt von vornherein kein Raum für eine individuelle Interessenabwägung.

Wenn diese Voraussetzungen kumulativ erfüllt sind, können die personenbezogenen Daten durch Bereitstellung der Informationen offengelegt werden. Die verantwortlichen kirchlichen Stellen, welche zur Offenlegung von personenbezogenen Daten berechtigt werden, haben hierzu geeignete Verfahren zu schaffen, um die Auskunft aus und Einsicht in die entsprechenden Akten sicherzustellen.

Erzbistum Hamburg

Das „*Gesetz zur Regelung von Einsichts- und Auskunftsrechten für die Aufarbeitungskommission im Rahmen der unabhängigen Aufarbeitung von sexuellem Missbrauch“* im Erzbistum Hamburg unterscheidet im Gegensatz zu den o.g. Ordnungen zwischen den vom Missbrauch unmittelbar betroffenen Personen sowie den sonstigen Personen. Sonstige Personen in diesem Sinne können nach § 5 des Gesetzes insbesondere Täter, Beschuldigte, Zeugen und andere Personen sein. Für die Offenlegung von personenbezogenen Daten der vom Missbrauch betroffenen Personen ist eine Einwilligung erforderlich. Sollte diese Einwilligung nicht erteilt werden, können die vom Missbrauch betroffenen Personen in die Anonymisierung ihrer personenbezogenen Daten einwilligen, um hierdurch eine Aufarbeitung ohne einen Personenbezug zu gewährleisten.

Bei den sonstigen Personen sind die Unterlagen vor der Offenlegung zu anonymisieren. Soweit eine Nutzung anonymisierter Daten nicht möglich oder die Anonymisierung mit einem unverhältnismäßigen Aufwand verbunden ist, ist eine Interessenabwägung durchzuführen. Trotz der sprachlichen Unterschiede ist diese Regelung gleichbedeutend mit den Regelungen, welche im Bistum Osnabrück und im Bistum

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62021CJ0252 (letzter Abruf: 01.09.2025)

Hildesheim erlassen worden sind. Auch in diesen Ordnungen ist die Möglichkeit der Anonymisierung vorrangig zu prüfen.

1.3.1.2. Auftragsdatenverarbeitung im Bistum Hildesheim

Das Bistum Hildesheim hat ein Gesetz über die Auftragsdatenverarbeitung zwischen juristischen Personen im Bistum Hildesheim[12] veröffentlicht. Ziel dieses Gesetzes ist es, die Verarbeitung von personenbezogenen Daten im Auftrag zwischen den juristischen Personen im Bistum Hildesheim zu regeln. Eine entsprechende Durchführungsverordnung soll noch erlassen werden.

1.3.1.3. IT-Endbenutzerrichtlinie im Bistum Osnabrück

Das Bistum Osnabrück hat eine „IT-Endbenutzerrichtlinie für Mitarbeitende in den kirchlichen Einrichtungen im Bistum Osnabrück (Instruktion)“[13] veröffentlicht. Diese IT-Endbenutzerrichtlinie richtet sich an alle haupt- und ehrenamtlichen Mitarbeiter, welche in den kirchlichen Körperschaften, Anstalten, Stiftungen und in den sonstigen kirchlichen verfassten Bereich zugehörigen Rechtsträgern im Bistum Osnabrück tätig sind und enthält Vorgaben in Bezug auf die praktische Umsetzung des Datenschutzes in den jeweiligen Einrichtungen. Dazu gehören u.a. die Gestaltung von Passwörtern, die sichere Nutzung von IT-Komponenten, Software und Cloudservices sowie die Internetnutzung durch die jeweiligen Mitarbeiter.

1.3.2. Entscheidungen der Datenschutzgerichte

Insbesondere das Interdiözesane Datenschutzgericht (IDSG 1. Instanz) hat im Jahr 2024 sehr praxisrelevante Entscheidungen veröffentlicht (abrufbar auf der Webseite der DBK[14,15]). Zwei dieser Entscheidungen sollen im Folgenden vorgestellt werden.

1.3.2.1. Offenlegung einer im Bistum archivierten „Akte auf Anerkennung des Leids“

Das IDSG hat sich in einer Entscheidung vom 11. November 2024[16] mit den datenschutzrechtlichen Anforderungen an die Offenlegung einer archivierten „Akte auf Anerkennung des Leids“ gegenüber Dritten befasst.

---

[12] https://www.bistum-hildesheim.de/fileadmin/dateien/PDFs/Materialboerse/Kirchlicher_Anzeiger/KA-2024-03.pdf (letzter Abruf: 01.09.2025)
[13] https://www.dioezesanbibliothek-osnabrueck.de/app/download/8213116581/12-2024.pdf?t=1740658678 (letzter Abruf: 01.09.2025)
[14] 1. Instanz: https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-1-instanz/entscheidungen
[15] 2. Instanz: https://www.dbk.de/themen/kirche-staat-und-recht/kirchliche-gerichte-in-datenschutzangelegenheiten/interdioezesanes-datenschutzgericht-2-instanz/entscheidungen
[16] https://www.dbk.de/fileadmin/redaktion/diverse_downloads/weitere_einrichtungen/Datenschutzgericht/IDSG_16_2023_Beschluss_v._11.11.2024_anonymisierte_Fassung.pdf (letzter Abruf: 01.09.2025)

Hintergrund

Die betroffene Person hatte im Jahr 2011 einen Antrag auf Anerkennung des Leids bei der Interventionsstelle des Bistums gestellt. Der Mitarbeiter der Interventionsstelle sagte der betroffenen Person zu, die personenbezogenen Daten aus dem Antrag ausschließlich für das Verfahren zur Anerkennung des Leids zu verarbeiten und Dritten nicht zugänglich zu machen. Die durch das Bistum beauftragte wissenschaftliche Forschungseinrichtung zur Aufarbeitung des sexuellen Missbrauchs hatte beginnend ab 2019 im Rahmen der Projektdurchführung einen Zugang auch zum archivierten Aktenbestand, in dem sich die Akte auf Anerkennung des Leids aus dem Jahr 2011 befand. Vor der Einsichtnahme durch das Forschungsteam nahm das Bistum eine Schwärzung der Namen, Adressen, Geburtsdaten, telefonischer und sonstiger Erreichbarkeiten und Kontoverbindungen der betroffenen Personen vor. Auf die Einholung einer Einwilligung ist verzichtet worden.

Aufgrund von detaillierten Schilderungen in der durch die Forschungseinrichtung veröffentlichten Studie, welche im Wesentlichen der Akte auf Anerkennung des Leids entnommen worden sind, erschienen in der Lokalpresse des Ortes, in dem die betroffene Person über viele Jahre ein Geschäft führte, mehrere Artikel über die Missbrauchsgeschichte und führten zu einer Retraumatisierung der betroffenen Person.

Die betroffene Person machte geltend, dass die Offenlegung ihrer nicht ausreichend anonymisierten Daten an die Forschungseinrichtung datenschutzwidrig erfolgte, insbesondere aufgrund der erfolgten Zusicherung, die Daten würden nicht an Dritte weitergegeben.

Feststellungen des IDSG

Das IDSG kam, wie zuvor auch die zuständige Datenschutzaufsicht, zu dem Ergebnis, dass der Zugang zu der Akte auf Anerkennung des Leids ohne die Einwilligung der betroffenen Person rechtswidrig war.

Die erfolgte Schwärzung der genannten Parameter habe nicht dazu geführt, dass eine Anonymisierung im Sinne des KDG erreicht worden ist. Vielmehr war die Zuordnung des Inhalts der Akte zur betroffenen Person durch die detaillierte Falldarstellung auch nach der Schwärzung ohne großen Aufwand möglich. Das Gericht betont, dass die wissenschaftliche Aufarbeitung von sexuellem Missbrauch zwar ein erhebliches kirchliches Interesse darstellt, dieses aber zumindest im vorliegenden Fall, in dem eine ausdrückliche Vertraulichkeitszusage erteilt wurde, nicht überwiegen kann. Die Datenerhebungen im Rahmen von Verfahren zur Anerkennung des Leids erfolgten

zweckgebunden und umfassten nicht die wissenschaftliche Missbrauchsaufarbeitung. Auch ohne eine entsprechende Zusage bei der Datenerhebung sei mit Blick auf die hohe Sensibilität der Daten zu bezweifeln, dass das kirchliche Interesse, die Daten zu anderen (wissenschaftlichen) Zwecken zu nutzen, das Geheimhaltungsinteresse der betroffenen Personen überwiegt.

Fazit

Die Entscheidung des IDSG ist zu begrüßen und ist auch für die Anwendung und Auslegung der Ordnungen und Gesetze zur Regelung von Auskunfts- und Einsichtsrechten zur Aufarbeitung sexualisierter Gewalt von hoher Relevanz. Zum einen sind wichtige Hinweise enthalten, die bei einer – obligatorisch zu prüfenden – Anonymisierung zu beachten sind. Zum anderen lassen sich die Ausführungen zur Interessenabwägung, die auch Grundsätze aus einer vorangegangenen Entscheidung im Kontext der Missbrauchsaufarbeitung[17] einbeziehen, übertragen und geben Anhaltspunkte für die Gewichtung verschiedener zu berücksichtigender Kriterien. Das IDSG lässt erkennen, dass auch im Falle privilegierter wissenschaftlicher Forschung und gleichzeitigem Bestehen eines erheblichen kirchlichen Interesses an der Missbrauchsaufarbeitung der Bistümer das Schutzinteresse der vom Missbrauch betroffenen Person höherrangig sein kann, insbesondere wenn es um höchstpersönliche Informationen aus den Verfahren zur Anerkennung des Leids geht, die streng zweckgebunden erhoben worden sind.

1.3.2.2. Zum Umfang einer Auskunft gemäß § 17 Abs. 1 und 3 KDG

Das IDSG hat sich in der Entscheidung vom 5. April 2024[18] zum Umfang des Auskunftsanspruchs nach § 17 Abs. 1 und 3 KDG geäußert.

Hintergrund

Der Entscheidung vorausgegangen war ein geltend gemachter Auskunftsanspruch eines Vaters gegenüber einer caritativen Beratungsstelle. Sowohl der Vater als auch die Mutter nahmen das Beratungsangebot der Beratungsstelle in gemeinsamen und allein geführten Gesprächen, teilweise unter Beteiligung des Kindes, wahr. Aufgrund eines familiengerichtlichen Verfahrens zwischen den Eltern verlangte der Vater Auskunft über die seine Tochter betreffenden personenbezogenen Daten sowie eine

[17] https://www.dbk.de/fileadmin/redaktion/diverse_downloads/weitere_einrichtungen/Datenschutzgericht/IDSG_16_2021_Beschluss__vom_24.02.2024_anonymisierte_Endfassung_zur_Ver%C3%B6ffentlichung.pdf (letzter Abruf: 01.09.2025)
[18] https://www.dbk.de/fileadmin/user_upload/Beschluss-IDSG-11-2023_v_5.4.2024_anonym.Fassung.pdf (letzter Abruf: 01.09.2025)

Kopie der Unterlagen. Die Beratungsstellte teilte hierauf mit, dass ein Auskunftsanspruch aufgrund der schutzwürdigen Interessen der Mutter, des Kindes sowie der zuständigen Beraterin nicht bestehe. Die Möglichkeit, Inhalte aus der papierhaften Handakte zu schwärzen, bestünde nicht. Hiergegen wendet sich der Vater mit einer datenschutzrechtlichen Beschwerde. Die zuständige Datenschutzaufsicht hat entschieden, dass dem Auskunftsersuchen des Vaters in Bezug auf die personenbezogenen Daten der Tochter nachzukommen sei. Ebenso sei dem Vater eine Kopie der Unterlagen über den Beratungsvorgang zur Tochter auszuhändigen. Hierbei müssten die Erklärungen der Beraterin sowie der Mutter geschwärzt werden, die keinen Bezug zur Tochter hätten. Gegen diesen Bescheid wendet sich die Beratungsstelle mit einem Antrag auf gerichtliche Überprüfung der Entscheidung durch das IDSG. Anschließend stellte die Beratungsstelle dem Vater Teile der Beraterakte zur Verfügung, wobei ein weit überwiegender Teil dieser Kopie geschwärzt war.

Feststellungen des IDSG

Das IDSG stellt zunächst fest, dass der Bescheid der zuständigen Datenschutzaufsicht rechtmäßig ist. Der geltend gemachte Auskunftsanspruch sowie der Anspruch auf Erhalt einer Kopie der personenbezogenen Daten die Tochter betreffend umfasst „*alle Aussagen deskriptiver und wertender Art, die einen Bezug zu der Tochter haben*“. (aao. Rn. 37) Weiter führt das IDSG unter Bezugnahme auf einschlägige Rechtsprechung zur DSGVO aus:

> „*Der Begriff der personenbezogenen Daten ist weit auszulegen. Er umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur, z. B. in Form von Stellungnahmen oder Beurteilungen, wenn es sich um Informationen „über“ die in Rede stehende Person handelt. Diese Voraussetzung ist erfüllt, wenn die Information auf Grund ihres Inhalts, Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist. Diese große Reichweite des Auskunftsrechts ist erforderlich, damit der Betroffene seine Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch wahrnehmen kann.*“
> (aao. Rn 38)

Hieraus folge, dass die zur Verfügung zu stellenden Kopien den Beratungsvorgang die Tochter betreffend annähernd vollständig umfasse. Als Inhaber der elterlichen Sorge, die die gesetzliche Vertretung der Tochter umschließt, umfasst das Recht auf Auskunft des Vaters neben den personenbezogenen zu seiner Person auch die Daten zu seiner Tochter. Diese stehen überwiegend in Bezug zu beiden Elternteilen. Im

Rahmen der erforderlichen Grundrechtsabwägung zwischen dem Auskunftsinteresse des Vaters und dem Geheimhaltungsinteresse der Mutter ergebe sich im Ergebnis nur eine geringfügige Schwärzungspflicht, beschränkt auf Erklärungen zur Mutter, die keinen Bezug zum Kind haben.

Fazit

Das IDSG legt den Begriff der personenbezogenen Daten weit aus und erstreckt diese auf alle Informationen in Bezug auf die unterschiedlichen Beziehungsverhältnisse. Durch die weite Auslegung erlangt die sorgfältige Abwägung der kollidierenden Grundrechte von Dritten besonderes Gewicht. Auch wenn diese umfangreich betroffen sind, kann ein pauschaler Verweis auf die Vertraulichkeit von (Beratungs-)Akten nicht genügen.

Vielmehr muss in jedem Einzelfall geprüft werden, welche Inhalte genau zu schwärzen und welche in jedem Fall zu beauskunften sind. Die Entscheidung ist noch nicht rechtskräftig.

1.3.3. Gemeinsame Stellungnahme

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands hat am 12. November 2024 eine gemeinsame Stellungnahme zu den Unabhängigen Aufarbeitungskommissionen[19] veröffentlicht. Inhaltlich bezieht sich die Stellungnahme auf die Anwendbarkeit des Kirchlichen Datenschutzrechts, die datenschutzrechtliche Verantwortlichkeit der Unabhängigen Aufarbeitungskommissionen sowie die Gewährleistung der Datensicherheit beim Umgang mit personenbezogenen Daten. Die Konferenz der Diözesandatenschutzbeauftragten vertritt die Ansicht, dass die Unabhängigen Aufarbeitungskommissionen dem kirchlichen Datenschutzrecht unterliegen und auch als datenschutzrechtlich Verantwortliche anzusehen sind. Hieraus folgt, dass die Unabhängigen Aufarbeitungskommissionen die datenschutzrechtlichen Pflichten des KDG wie z. B. die Bestellung eines betrieblichen Datenschutzbeauftragten und die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten umzusetzen haben. Auch in Bezug auf die Datensicherheit sind wesentliche Aspekte zu beachten. Hierbei ist zu berücksichtigen, dass die Speicherung der personenbezogenen Daten auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu erfolgen hat. Hierüber lassen sich gut unterschiedliche Zugangs- und Zugriffsrechte darstellen. Ebenso wird hierdurch eine unkontrollierbare

[19] https://www.kdsa-nord.de/Download/Beschluesse/20241114_Gemeinsame_Stellungnahme_UAK.pdf

Vervielfältigung z. B. durch einen Mailversand der personenbezogenen Daten verhindert. Ausführliche Hinweise können der gemeinsamen Stellungnahme entnommen werden.

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.

Der Eingang von datenschutzrechtlichen Beschwerden ist im Vergleich zum Vorjahr stabil geblieben. Die Anzahl der gemeldeten Datenschutzverletzungen hat sich leicht erhöht. Dies ist auch auf eine Datenschutzverletzung zurückzuführen, von der mehrere Einrichtungen betroffen waren. Neben einer Vor-Ort-Prüfung eines Kirchengemeindeverbands hat die Prüfung von Videoüberwachungsanlagen, welche zum Teil in den Schulen zum Einsatz kommen, begonnen.

Im Berichtszeitraum ist ein Bußgeld verhängt worden. Der Bescheid gegen die Einrichtung wird derzeit durch das Interdiözesane Datenschutzgericht (1. Instanz) auf seine Rechtmäßigkeit geprüft.

Insgesamt sind vier neue Verfahren vor dem Interdiözesanen Datenschutzgericht im Jahr 2024 hinzugekommen. Ein Verfahren ist der zweiten Instanz, dem Datenschutzgericht der Deutschen Bischofskonferenz (2. Instanz), zur Prüfung und Entscheidung vorgelegt worden. Zum Abschluss des Jahres 2024 sind damit insgesamt sechs Verfahren vor dem IDSG und ein Verfahren vor dem DSG-DBK anhängig.

Einige der bearbeiteten Fälle und Verfahren sollen im Folgenden in verallgemeinerter Form dargestellt und unsere Einschätzungen hierzu mitgeteilt werden. Aus den beschriebenen Fällen lassen sich allgemeine, nicht abschließende Hinweise für die Verantwortlichen wie auch für diejenigen, deren Daten verarbeitet werden, ableiten.

2.1. Bistümer und Kirchengemeinden

2.1.1. Unzulässige Videoüberwachung

Ein Beschwerdeführer trug im Rahmen eines datenschutzrechtlichen Beschwerdeverfahrens vor, dass im Gemeindehaus eine Videokamera angebracht worden sei. Die Kamera war auch auf den öffentlich zugänglichen Vorhof der Kirche sowie auf ein Fenster des Wohnhauses des Pfarrers ausgerichtet. Ein Hinweisschild für den Betrieb der Videokamera war nicht angebracht worden. Seit wann die Kamera dort angebracht war, war nicht bekannt.

Im Rahmen der Anhörung teilte uns die verantwortliche Kirchengemeinde mit, dass es sich um eine batteriebetriebene Outdoor- und Indoor-Kamera handele, die per App über das Mobiltelefon aktiviert, gesteuert und ausgelesen werden kann. Eine

tatsächliche Inbetriebnahme bzw. eine Aktivierung der Kamera wurden jedoch seitens der Kirchengemeinde bestritten. Als Zweck der Videoüberwachung hat die Kirchengemeinde die Verhinderung und ggf. Dokumentation von Sachbeschädigungen und Vandalismus mitgeteilt. Ein Hinweisschild sei nicht erforderlich gewesen, da die Kamera gut sichtbar im Eingangsbereich angebracht wurde. Im Fall einer Inbetriebnahme hätte ein ehrenamtlicher Mitarbeiter über die App eine Zugriffsmöglichkeit.

Nach Prüfung der Stellungnahme ist festgestellt worden, dass die Installation der Videoüberwachung unzulässig war.

Eine Kamera-Attrappe lag im vorliegenden Fall nicht vor. Kamera-Attrappen sind von vornherein nicht für die Verarbeitung von personenbezogenen Daten gedacht bzw. so konzipiert, sodass keine Datenverarbeitung vorliegen kann. Nach Mitteilung der Kirchengemeinde war die Videoüberwachung zwar nicht in Betrieb, hätte jedoch jederzeit über die installierte App aktiviert werden können. Hinzu kommt, dass die verantwortliche Kirchengemeinde keine technischen oder organisatorischen Vorkehrungen getroffen hat, um einen unerlaubten Zugriff zu verhindern. Aus diesem Grund war der vorliegende Einsatz anders zu bewerten als eine Kamera-Attrappe.

Grundsätzlich liegen die Verhinderung und Aufklärung von Straftaten im berechtigten Interesse eines Verantwortlichen. Die Videoüberwachung muss jedoch zur Erreichung des Zwecks erforderlich sein. Dies setzt eine tatsächliche Gefahrenlage voraus, die über das allgemeine Risiko hinausgeht. Eine solche war hier nicht erkennbar.

Ebenso ist gegen die Pflicht verstoßen worden, auf den Umstand der Videoüberwachung zum frühestmöglichen Zeitpunkt hinzuweisen.

Die Beschwerde war damit begründet und führte zur Entfernung der Kamera. Aufgrund des Verstoßes ist eine datenschutzrechtliche Beanstandung ausgesprochen worden.

Hinweis – Was ist zu beachten?

Jeder Verantwortliche muss vorab die Zulässigkeit für den Einsatz einer Videoüberwachung prüfen und dokumentieren. Hierbei sind neben den rechtlichen Aspekten insbesondere auch die technischen und organisatorischen Aspekte wie Möglichkeiten zur Verschlüsselung, Zugriffskontrollen und Festlegung von Nutzungsregeln zu beachten.

Ergänzende Hinweise zum Einsatz einer Videoüberwachung sind in diesem Bericht im Abschnitt 2.5.1 Videoüberwachung an Schulen zu finden.

2.1.2. Anfragen ohne datenschutzrechtlichen Bezug

Aus den Pfarreien erreichten uns auch Anfragen und Beschwerden, die im Ergebnis nicht dem Datenschutzrecht unterliegen. So konnte beispielsweise die Anfechtung einer Gremienwahl wegen Verfahrensfehlern nicht im Rahmen eines datenschutzrechtlichen Beschwerdeverfahrens unterstützt werden.
Auch die Geltendmachung eines Auskunftsanspruches in Bezug auf Geschäftsunterlagen und Sitzungsprotokolle ohne Personenbezug fällt nicht in den Anwendungsbereich des KDG.

2.2. Gesundheitseinrichtungen

2.2.1. Einbruchdiebstahl beim PKW

Aus einer Einrichtung zur Beratung und Unterstützung von Schwangeren und jungen Müttern und Vätern kam die Meldung, dass eine Arbeitstasche aus dem PKW einer Mitarbeiterin der Einrichtung entwendet worden ist. Die Mitarbeiterin befand sich auf dem Weg vom Dienstort ins Homeoffice, um von dort ihre Tätigkeit fortzusetzen. Auf dem Weg nach Hause wurde ein kurzer Halt für einen Spaziergang eingelegt, bei dem die Diensttasche unbeaufsichtigt im PKW verblieb.

Die Tasche enthielt Unterlagen zu Klienten der Einrichtung, in welchen u.a. Stammdaten und Gesundheitsdaten erfasst waren.

Im Rahmen der Aufarbeitung hat sich gezeigt, dass verbindliche und schriftliche Vorgaben oder Dienstanweisungen für den Transport von Klientenunterlagen in der ambulanten Beratung nicht etabliert waren. Es wurde lediglich mitgeteilt, dass bei der Einarbeitung über das Thema gesprochen wird und es jährliche Online-Schulungen gibt, die allgemeine Hinweise zum Umgang mit Akten enthalten. Nach dem Vorfall hat die Einrichtung begonnen, das QM-Handbuch um die Themen mobiles Arbeiten und Umgang mit Akten zu ergänzen.

Hinweis – Was ist zu beachten?

Insbesondere wenn es sich wie hier um besonders sensible personenbezogene Daten wie Gesundheitsdaten handelt, muss die jeweilige Einrichtung konkret und nachweisbar regeln, wie beim Transport mit den Daten umzugehen ist. Das gilt vor allem für Tätigkeiten, die mit regelmäßigen Hausbesuchen und Auswärtstätigkeiten

verbunden sind. Allgemeine Hinweise zum Umgang mit personenbezogenen Daten genügen nicht. Wenn wie im vorliegenden Fall eine Unterbrechung der Fahrt erforderlich sein sollte, dürfen die personenbezogenen Daten nicht unbeaufsichtigt im PKW verbleiben. Ein Diebstahl aus einem PKW ist kein Einzelfall und bei der Risikobewertung zu berücksichtigen.

2.2.2. Mit Unterstützung der Ehefrau

Eine weitere aus einem Krankenhaus gemeldete Datenschutzverletzung beinhaltete einen Verstoß gegen die Schweigepflicht und das Datengeheimnis. Zur Durchführung einer Studie durch einen dort angestellten Arzt sollten mehrere Patienten telefonisch kontaktiert werden, um diese für die Teilnahme an der Studie zu gewinnen. Grundsätzlich hatten diese Patienten eingewilligt, telefonisch zu Studienzwecken von der Klinik kontaktiert zu werden. Insgesamt sollten mehr als 100 Patienten angerufen werden.

Die einzelnen Anrufe bei den Patienten sind jedoch nicht nur von dem Arzt durchgeführt worden. Zur Rekrutierung der Patienten für die Studie bat der Arzt seine Ehefrau privat um Unterstützung. Diese hat etwa 20 Telefonate mit den Patienten geführt und erhielt dafür im Vorfeld die Namen, Telefonnummern und Geburtsdaten der Patienten. Einsicht in die Patientenakte wurde nicht gewährt.

Aufgrund der Sensibilität der hier betroffenen personenbezogenen Daten, die einer Privatperson offengelegt wurden, die selbst nicht Berufsgeheimnisträgerin ist, ist die Benachrichtigung der Patienten angeordnet worden. Die erteilten Einwilligungen konnten nur so verstanden werden, dass sie sich auf eine vertrauliche Kontaktaufnahme durch die Klinik beschränken.

Hinweis – Was ist zu beachten?

Bereits der Kontext, in dem Kontakt- und Geburtsdaten von Patienten offengelegt werden, kann dazu führen, dass es sich um Gesundheitsdaten handelt, auch wenn medizinische Informationen als solche nicht mitgeteilt werden. Im dargestellten Fall waren durch die Kenntnis des Klinikaufenthaltes und die Geeignetheit der Patienten für die Studie des Ehemannes, deren Fachrichtung der Ehefrau bekannt sein dürfte, zweifellos Rückschlüsse auf den Gesundheitszustand der Patienten möglich.

Die ärztliche Schweigepflicht und das Datengeheimnis gelten auch gegenüber Familienangehörigen. Der Aufwand, mehr als 100 ehemalige Patienten anzurufen, um diese für die Teilnahme an einer Studie zu gewinnen, ist sicherlich nicht zu

unterschätzen. Unbeteiligte Familienmitglieder hierfür einzubinden ist aber in keinem Fall eine gute Idee.

2.2.3. Lost Places

Es kommt immer wieder vor, dass personenbezogene Daten von Patienten oder Bewohnern in Einrichtungen verbleiben, welche für immer ihre Türen geschlossen haben.

So ist auch uns ein Einbruch in ein geschlossenes und leerstehendes Altenheim gemeldet worden, in dem sich noch verschiedene Dokumente befanden, die im Haus verstreut worden sind. Glücklicherweise waren die eigentlichen Bewohnerakten bereits vor dem Einbruch in ein anderes Haus des Trägers umgelagert worden. Die herumliegenden Dokumente wurden gesichert und enthielten zum Teil Mitarbeiterdaten und Daten verstorbener Bewohner. Ob Dokumente mit weiteren Daten fehlten, konnte nicht aufgeklärt werden.

Hinweis – Was ist zu beachten?

Verlassene Gebäude können i. d. R. keinen ausreichenden Schutz zur Aufbewahrung von personenbezogenen Daten bieten. Verantwortliche Träger oder ggf. auch Rechtsnachfolger oder Insolvenzverwalter haben eine datenschutzkonforme Aufbewahrung der personenbezogenen Daten sicherzustellen und ein Verfahren zu entwickeln, wie betroffene Personen ihre datenschutzrechtlichen Rechte wahrnehmen können.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte sich im vergangenen Jahr ebenfalls hiermit beschäftigt und dazu eine Entschließung vom 15. Mai 2024 zum Thema „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern“[20] herausgegeben.

2.2.4. Fehlversand wegen Autovervollständigung

Bei einem Versand einer Wunddokumentation per E-Mail an den Hausarzt ist es zu einem Fehlversand gekommen. Bei der Wunddokumentation handelte es sich um ein Bild des Schienbeins mit vollständigem Namen und dem Geburtsdatum des Patienten. Ursächlich für den Fehlversand war die Ähnlichkeit der E-Mail-Adresse des Hausarztes mit einem eingerichteten E-Mail-Verteiler der Einrichtung sowie die Autovervollständigung des Mailprogramms. So hatten 42 Empfänger die Möglichkeit, von der

[20] https://datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf (letzter Abruf: 01.09.2025)

Wunddokumentation des Patienten Kenntnis zu nehmen. Bei den Empfängern handelte es sich teils um interne, teils um externe Empfänger. Nach Bekanntwerden des Fehlversands erfolgte ein Rückruf der E-Mail, welcher zum Teil erfolgreich war. Die weiteren Empfänger wurden informiert, die erhaltene E-Mail zu löschen.

Hinweis – Was ist zu beachten?

Gerade in Fällen, in denen die E-Mail-Adressen automatisch durch das E-Mail-Programm vervollständigt werden, besteht ein erhöhtes Risiko eines Fehlversands. Es mag bequem sein, die E-Mail-Adresse eines Empfängers nicht jedes Mal erneut einzugeben. Mit Blick auf die Risikominimierung sollte der Einsatz einer Autovervollständigung jedoch kritisch geprüft werden.

Zudem ist darauf zu achten, dass ein Hinweis an die unberechtigten Empfänger, die E-Mail zu löschen, nicht immer ausreichend ist. Gerade wenn es sich wie vorliegend um Gesundheitsdaten handelt, sind die Empfänger aufzufordern, die Löschung der E-Mail zu bestätigen.

2.3. Bildung und Kitas

2.3.1. Benachrichtigungspflichten bei Verlust von Kinderfotos

Im Falle von gemeldeten Einbruchdiebstählen wurde es von den Kitas sehr unterschiedlich bewertet, ob beim Verlust von Kinderfotos eine Benachrichtigung der Erziehungsberechtigten erfolgen muss.

Eine Benachrichtigung der betroffenen Personen bzw. der Erziehungsberechtigten ist gemäß § 34 Abs. 1 KDG immer dann erforderlich, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen anzunehmen ist.

Aus unserer Sicht ist ein solches hohes Risiko immer gegeben, wenn unverschlüsselte Datenträger mit Kinderfotos entwendet werden. Kinderfotos sind besonders sensibel und bieten ein hohes Missbrauchspotential. Der häufig vorgebrachte Einwand, es habe sich höchstwahrscheinlich um reine Beschaffungskriminalität gehandelt und es ginge den Dieben nicht um die Fotos, führt nicht zu einer Verringerung der Gefährdung. Gerade im Falle von reiner Beschaffungskriminalität kann nämlich davon ausgegangen werden, dass die Geräte zeitnah im Internet, Darknet, ins Ausland etc. verkauft werden, ohne dass die Täter im Vorfeld des Verkaufs eine datenschutzkonforme Löschung der Bilder von den Geräten vornehmen.

Die Bilder sind damit außerhalb jeglicher Kontrolle und es kann nicht nachvollzogen werden, in welche Hände diese schließlich gelangen.

Auch bei vermeintlich harmlosen Fotos, die Kinder in Alltagssituationen in der Kita z. B. beim Spielen, Tanzen oder Malen zeigen, können die Folgen verheerend sein und die Bilder können z. B. in pädokriminelle Foren gelangen oder für computeranimierte Kinderpornografie genutzt werden. Um eine missbräuchliche Nutzung der Bilder zu verhindern, müssen diese auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen oder auf verschlüsselten Datenträgern gespeichert werden. Siehe hierzu auch die ergänzenden Erläuterungen in Abschnitt 3.2.

2.3.2. Verlust eines USB-Sticks

Nachdem der Ausdruck von Dokumenten von einem USB-Stick fehlschlug, hing die Lehrkraft Plakate in der Schule ab und entsorgte diese. Hierbei sind vermutlich nicht nur die Plakate, sondern auch der USB-Stick entsorgt worden, welchen die Lehrkraft noch in der Hand hatte. Auf diesem unverschlüsselten USB-Stick waren neben Zensuren aus den Fächern Mathematik, Deutsch, Englisch, Französisch bzw. Latein auch weitere personenbezogene Daten wie Protokolle aus Elterngesprächen, Dokumentationen aus Lernentwicklungsgesprächen, eine Datei aus der „Sorgenkinderkonferenz“ sowie Gesundheitsdaten gespeichert.

Die Eltern sind über den Verlust der personenbezogenen Daten sowie über die Möglichkeit einer unbefugten Offenlegung informiert worden. Es handelte sich bei den auf dem USB-Stick gespeicherten personenbezogenen Daten um Kopien, sodass die Verfügbarkeit zu keinem Zeitpunkt beeinträchtigt war.

Hinweis – Was ist zu beachten?

Bereits im letzten Jahresbericht ist darauf hingewiesen worden, dass personenbezogene Daten der Datenschutzklasse II und III auf zentralen Systemen in Räumen mit einem gesonderten Zutrittsschutz zu speichern sind. Sofern begründete Ausnahmen vorliegen, ist eine Speicherung auf anderen IT-Systemen, wozu auch USB-Sticks gehören, nur dann zulässig, wenn diese dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechend angemessen geschützt sind.

Zumindest bei Zeugnissen und Lernentwicklungsberichten handelt es sich um personenbezogene Daten der Datenschutzklasse III. Zeugnisse und Lernentwicklungsberichte stellen als Beurteilungen der Leistungen und der Leistungsfähigkeiten eines Schülers besonders schützenwerte Daten dar. Eine unbefugte Offenlegung dieser Daten, sei es innerhalb oder außerhalb der Schule, kann für den betroffenen Schüler erhebliche Nachteile, z. B. Diffamierung, Mobbing, Bloßstellung

oder Diskriminierung, mit sich bringen. Ebenso ist die Tatsache zu berücksichtigen, dass es sich hierbei um personenbezogene Daten von i. d. R. Minderjährigen handelt.

2.4. Caritas und Soziales

2.4.1. Einsatz von KI-Tools

Aus dem Bereich der Kinder- und Jugendhilfe ist mitgeteilt worden, dass eine Mitarbeiterin personenbezogene Daten unter Zuhilfenahme von ChatGPT und DeepL verarbeitet hat. Hierbei ist ein Entwicklungsbericht zunächst mit ChatGPT erstellt worden. Bei der Erstellung ist zwar lediglich der Anfangsbuchstabe des Namens verwendet worden, jedoch unter Benennung der Einrichtung und der Wohngruppe der betroffenen Person. Ergänzt worden sind Gesundheitsdaten, Informationen über geleistete Hilfeformen sowie der pädagogische Unterstützungsbedarf. Um den Bericht noch zu optimieren, ist dieser Bericht anschließend durch DeepL korrigiert worden.

Der Einsatz der genannten Software war nicht durch die Einrichtung genehmigt worden. Die Einrichtung hat aufgrund des Vorfalls sämtliche Mitarbeiter zum datenschutzkonformen Umgang mit KI-Tools sensibilisiert. Ebenso sollen die bereits getroffenen Maßnahmen auf ihre Wirksamkeit geprüft und ggf. angepasst werden.

Hinweis – Was ist zu beachten?

Verantwortliche müssen zu jedem Zeitpunkt sicherstellen, dass personenbezogene Daten nicht nur rechtmäßig verarbeitet werden, sondern auch, dass die Verarbeitung ausschließlich mit den vom Verantwortlichen freigegebenen Programmen erfolgt. Die Durchführungsverordnung legt klar fest, dass auf dienstlichen IT-Systemen ausschließlich vom Verantwortlichen autorisierte Programme und Kommunikationstechnologien verwendet werden dürfen. Verantwortliche müssen die Einhaltung dieser Vorgabe durch geeignete technische und organisatorische Maßnahmen sicherstellen. Dies kann beispielsweise durch folgende, nicht abschließende Maßnahmen erreicht werden:

- Sicherstellung, dass Mitarbeitern bei Neueinstellungen das Verbot bekanntgemacht wird (z.B. Aufnahme des Verbots in einem Merkblatt, Beschreibung des Verbots bei der Erstinformation zum Datenschutz)
- Erstellung einer Mitarbeiterrichtlinie
- regelmäßige Sensibilisierungsmaßnahmen
- Nachbelehrung sämtlicher Mitarbeiter

- Trennung von Anwender- und Administratorenrechten
- regelmäßige Überprüfung und ggf. Anpassung der getroffenen Maßnahmen

Insbesondere dann, wenn es sich um „allseits bekannte“ Probleme handelt, wie hier die eigenmächtige Nutzung von leicht zugänglichen KI-Tools, gelten erhöhte Anforderungen an die zu treffenden organisatorischen Maßnahmen.

2.4.2. Zugriffsrechte in Wohneinrichtung

Bei einer Routinekontrolle in einer Wohneinrichtung ist aufgefallen, dass ein Mitarbeiter der Haustechnik einen regulären Zugriff auf personenbezogene Daten der Bewohner hatte. Es handelte sich um einen Zugriff auf eine Datenbank, in der neben aktuellen Themen und außerhäuslichen Terminen auch medizinische Informationen zu einzelnen Bewohnern notiert werden. Die interne Überprüfung des Zugriffserfordernisses unter Einbeziehung des Stellenprofils ergab, dass die Kenntnis der notierten Termine ggf. benötigt werden, da es zu den Aufgaben des Mitarbeiters gehört, die Bewohner zu Auswärtsterminen zu begleiten. Eine Kenntnis von persönlichen, insbesondere medizinischen Daten war jedoch nicht erforderlich. Um die Begleitung zu einzelnen Terminen zu organisieren, genügt eine bedarfsgerechte und mündliche Information an den Mitarbeiter. Daher ist der Zugriff des Mitarbeiters auf diese Datenbank entzogen worden. Aufgrund des Vorfalls sind zudem die weiteren Berechtigungen unter Berücksichtigung des Need-to-know-Prinzips geprüft und ggf. angepasst worden.

Da der Zugriff auf die personenbezogenen Daten bereits entzogen wurde, war eine dahingehende Anordnung entbehrlich.

Hinweis – Was ist zu beachten?

Grundsätzlich dürfen Mitarbeiter auf die personenbezogenen Daten zugreifen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Dieser Zugriff muss jedoch gerade dann, wenn es sich um Gesundheitsdaten handelt, auf das absolut erforderliche beschränkt werden. Ebenso sind das Berechtigungskonzept sowie die tatsächlich vergebenen Berechtigungen regelmäßig kritisch zu prüfen.

2.5. Prüfungen 2024

2.5.1. Videoüberwachung an Schulen

Alle Schulabteilungen bzw. Schulstiftungen sind in einem ersten Schritt gebeten worden, diejenigen Schulen mitzuteilen, welche Videoüberwachungsanlagen auf dem Schulgelände installiert haben. Die Abfrage ergab, dass an insgesamt 17 Schulen

verteilt über das Zuständigkeitsgebiet der Katholischen Datenschutzaufsicht Videoüberwachungsanlagen installiert und in Betrieb sind. Die jeweilige Anzahl der installierten Kameras variiert stark. Einige Schulen haben lediglich eine Kamera installiert. Spitzenreiter im Hinblick auf die Anzahl der Kameras ist eine Schule, bei der 14 Kameras installiert sind. An insgesamt sechs Schulen findet in 2025 eine Prüfung vor Ort statt

Im Rahmen der Prüfung zur Rechtmäßigkeit der Videoüberwachung müssen Verantwortliche u.a. folgende Fragen beantworten können:

- Zu welchem Zweck ist die Videoüberwachung erforderlich?
- An welchen Orten sind die Videokameras angebracht worden? Hierbei sollte auch beschrieben werden, welche Bereiche von den Kameras erfasst werden. Dazu ist eine Skizze mit Lage und Erfassungsbereichen der Kameras einzureichen.
- Wird auf die Videoüberwachung hingewiesen? Hierbei sollte auch beschrieben werden, wo eventuelle Hinweisschilder angebracht sind. Gegebenenfalls sind eine Kopie des Hinweisschildes einzureichen sowie die Standorte der Hinweisschilder auf der Lageplan-Skizze zu markieren.
- Wie lange werden die Videoaufnahmen gespeichert?
- Ist der Einsatz der Videokamera im Verzeichnis von Verarbeitungstätigkeiten dokumentiert worden? Hierzu sollte ein Auszug des Verzeichnisses von Verarbeitungstätigkeiten eingereicht werden.
- Sofern eine Datenschutz-Folgenabschätzung durchgeführt worden ist, sollte auch hiervon eine Kopie vorgelegt werden können.
- Zur eingesetzten Technik sollten u. a. folgende Fragen beantwortet werden können:
    - Welche Kameramodelle werden eingesetzt? Die entsprechenden Datenblätter sind einzureichen.
    - Wo und auf welchen Systemen erfolgt die Speicherung der Videodaten? Wie sind die Aufnahmen auf diesen Systemen vor unbefugtem Zugriff geschützt?
    - Welche Zugriffsmöglichkeiten bestehen auf die Videobilder? Können diese etwa über mobile Endgeräte (z. B. Smartphone) abgerufen werden? Wenn ja, wer verfügt über die Möglichkeit dieses Zugriffs? Wie werden die Bilddaten übertragen und wie sind diese dabei vor unbefugten Zugriffen geschützt?

- Welche weiteren Funktionen hat die Kamera (z. B. steuerbare Zoomobjekte, Audiofunktion, Bewegungsdetektion, Gesichtserkennung)?

Bei den genannten Fragen handelt es sich nicht um einen abschließenden Prüfkatalog. Sonderfälle (wie z. B. der Fall einer verdeckten Videoüberwachung zur Aufdeckung von Straftaten im Beschäftigtenverhältnis) können weitere Angaben erforderlich machen.

Ein Bericht der Prüfungsergebnisse erfolgt im nächsten Tätigkeitsbericht.

2.5.2. Anlasslose Prüfung

Im vergangenen Jahr fand ebenso eine Prüfung eines Kirchengemeindeverbands statt. Insgesamt war der Kirchengemeindeverband in datenschutzrechtlicher Hinsicht gut aufgestellt. An wenigen Stellen sind Anordnungen getroffen worden. Die meisten Anordnungen sind bereits im Anhörungsverfahren zum Bescheid umgesetzt worden.

Problematisch war u. a. die Konstellation im Serverraum: Personenbezogene Daten der Datenschutzklasse II müssen gemäß § 12 Abs. 2 lit. c) KDG-DVO grundsätzlich auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen gespeichert werden. Um dies sicherzustellen, werden in den Einrichtungen als Standort bevorzugt u. a. Keller- oder Haustechnik-Räume gewählt. Zu beachten ist in solchen Umgebungen, dass ggf. weitere in diesen Räumen befindliche Anlagen wie etwa Heizungen oder andere Versorgungsanlagen selbst eine Gefährdung für die Verfügbarkeit der Systeme und der darauf gespeicherten Daten darstellen können; z. B. wenn der Serverschrank direkt unter wasserführenden Leitungen positioniert wird. In solchen Konstellationen sollten Maßnahmen getroffen werden, die diesen Gefährdungen entgegenwirken, sodass diese nicht direkt auf die Systeme wirken können.

2.6. Zusammenarbeit und Veranstaltungen

2.6.1. Ökumenischer Datenschutztag

Auch im Jahr 2024 fand der Ökumenische Datenschutztag als Gemeinschaftsveranstaltung der Vertreter der evangelischen und katholischen Datenschutzaufsichten statt. Veranstaltungsort der zweitägigen Veranstaltung war diesmal die Stadt Erfurt. Der Schwerpunkt der Veranstaltung lag auf dem Thema Künstliche Intelligenz.

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 2024 war Frau Ursula Becker-Rathmair, Diözesandatenschutzbeauftragte und Leiterin des Katholischen Datenschutzzentrums Frankfurt/M. KdöR, Sprecherin der Konferenz. Zum Sprecher für das Jahr 2025 ist Herr Dominikus Zettl, Diözesandatenschutzbeauftragter und Leiter des Katholischen Datenschutzzentrums Bayern (KdöR), 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 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 2024 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 und damit bei der Beratung berücksichtigt werden.

2.6.5. Umgang mit Datenschutzverletzungen

Zusammen mit dem Katholischen Datenschutzzentrum Frankfurt/M. ist eine gemeinsame Sensibilisierungskampagne zum Umgang mit Datenschutzverletzungen in den kirchlichen Einrichtungen gestartet. Die entsprechende Meldung steht auf unserer Webseite zur Verfügung.[21] Die Kampagne ist als Online-Umfrage gestartet und betrifft mehr als 100 Einrichtungen aus den Bereichen Alten- und Pflegeheime, Behinderten- und Jugendeinrichtungen, Orts-Caritasverbände/soziale Einrichtungen, Kirchengemeinden sowie Kindertagesstätten. Die Ergebnisse werden voraussichtlich im nächsten Tätigkeitsbericht veröffentlicht.

[21] https://www.kdsa-nord.de/20240715

3. Weitere Themen

3.1. Umgang mit Fotos – Unsicherheiten in Bezug auf „Besucherfotos“

Beratungsanfragen zum Umgang mit Fotos in Kitas und Schulen haben gezeigt, dass in der Praxis immer wieder die Frage aufkommt, wie die Einrichtung damit umzugehen hat, wenn Besucher/Erziehungsberechtigte bei gemeinsamen Veranstaltungen (Sommerfest, gemeinsamer Gottesdienst, Theateraufführung etc.) mit ihren Smartphones Bilder oder Videos erstellen. Ist es möglich, dies zu untersagen und sicherzustellen, dass nicht erteilte Einwilligungen nicht durch private „Elternfotos“ umgangen werden? Muss im Falle eines ausgesprochenen Verbotes kontrolliert werden, ob sich alle Anwesenden an das Verbot halten? Was ist zu tun, wenn sich im Nachgang herausstellt, dass Eltern trotz eines Verbotes Bilder gemacht und veröffentlicht haben? Wie ist in diesen Fällen mit Betroffenenanfragen umzugehen?

Auch wenn die Einrichtung für das eigenmächtige Erstellen und Veröffentlichen von Bildern oder Videos durch Besucher grundsätzlich nicht datenschutzrechtlich verantwortlich ist, sollte diese als Organisator der Veranstaltung dennoch gewisse Rahmenbedingungen festlegen.

Insbesondere mit Blick auf die Fürsorgepflichten sollten Kita- und Schulveranstaltungen in ihrer Ganzheit so organisiert werden, dass seitens der Einrichtung alle ihr möglichen Maßnahmen ergriffen werden, um den Schutz der betroffenen Kinder und Jugendlichen sicherzustellen.

Eine Möglichkeit ist das Aussprechen eines Verbotes der Erstellung und Weiterverwendung von privaten Fotos aufgrund des Hausrechts und stattdessen das einrichtungsorganisierte Fotografieren und zweckgebundene Bereitstellen an die Erziehungsberechtigten unter Beachtung der erteilten Einwilligungen. Je nach Veranstaltung kann es auch eine Lösung sein, eine „Fotoecke“ einzurichten, die für private Fotografie zu nutzen ist.

Auf offensichtliche Verstöße sollte reagiert werden. Wenn im Nachgang Beschwerden oder Löschbegehren von betroffenen Personen an die Einrichtung herangetragen werden, ist aus unserer Sicht soweit wie möglich eine Mitwirkung geboten, beispielsweise durch Kontaktaufnahme mit den verantwortlichen Personen.

Hinweis – Was ist zu beachten?

Einrichtungen sollten ihre Veranstaltungen möglichst so organisieren, dass ihnen gegenüber erteilte bzw. nicht erteilte Einwilligungen zur Erstellung und

Veröffentlichung von Bildern auch von Dritten beachtet werden. Das Hausrecht ermöglicht es ihnen, ein Verbot privater Fotografie auszusprechen oder gewisse Regeln für das Fotografieren aufzustellen, um dieses Ziel zu erreichen.

3.2. Einbruchdiebstähle bei Kitas

Nach wie vor melden insbesondere Kindertagesstätten vermehrt Einbrüche in ihre Einrichtungen und hiermit verbunden den Diebstahl von Kameras, Laptops und sonstigen mobilen Speichergeräten. Leider sind immer noch zahlreiche mobile Datenträger nicht verschlüsselt, sodass nach einem Diebstahl ein Zugriff auf die dort gespeicherten personenbezogenen Daten ungehindert möglich ist und diese missbräuchlich verwendet werden können. Eine Speicherung der personenbezogenen Daten auf zentralen Systemen erfolgt häufig ebenfalls nicht.

Jede Einrichtung, die personenbezogene Daten der Datenschutzklasse II und höher verarbeitet, ist grundsätzlich verpflichtet, die Daten auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern. Die Datenschutzklasse II ist bereits dann gegeben, wenn ein Geburtsdatum verarbeitet wird. Ebenso sind Bilder von Kindern mindestens der Datenschutzklasse II zuzuordnen. Eine dezentrale Speicherung ist lediglich in begründeten Ausnahmefällen erlaubt. Bei der Erstellung von Bildern mit einer Kamera ist sicherzustellen, dass diese zeitnah auf ein zentrales System gespeichert und von der Kamera gelöscht werden. Alternativ zum Einsatz von Kameras kann der Einsatz von verschlüsselten mobilen Geräten wie Smartphones oder Tablets, die im Hinblick auf die Kommunikation mit externen Diensten und bestehender Schnittstellen entsprechend abgesichert werden müssten, geprüft werden.

3.3. Mangelnde Transparenz bei der Datenschutzinformation

Eine Datenschutzinformation soll informieren und nicht verwirren. Immer dann, wenn ein Verantwortlicher personenbezogene Daten einer betroffenen Person erhebt, muss er diese ausführlich über die Datenverarbeitung informieren. Welche Informationen mitzuteilen sind, ergibt sich unmittelbar aus den §§ 15 und 16 KDG. Die Information dient der Transparenz und soll die betroffene Person in die Lage versetzen, die tatsächliche Verarbeitung ihrer personenbezogenen Daten nachzuvollziehen – ein wesentlicher Baustein des Grundrechts auf informationelle Selbstbestimmung.

Für Einrichtungen gibt es verschiedene Möglichkeiten, dies umzusetzen. In jedem Fall ist vorab eine Analyse der Verarbeitungsprozesse erforderlich. So wird ermittelt, welche Verarbeitungen in der Einrichtung stattfinden und welche Personen(gruppen)

jeweils betroffen sind. Es hat sich gezeigt, dass häufig bereits dieser wichtige Schritt übersprungen und eine Datenschutzinformation bereitgestellt wird, in der jegliche in Betracht kommende Datenverarbeitungen aufgelistet sind, unabhängig davon, ob sie in der Einrichtung tatsächlich stattfinden oder ob sie für die betroffene Person überhaupt relevant sind. Als Beispiel kann die Datenschutzerklärung auf einer Webseite genannt werden, die z. B. über verschiedenste Tracking-Tools informiert, obwohl im Ergebnis nur eines davon im Einsatz ist. Um sicherzugehen, dass alle erforderlichen Informationen enthalten sind, werden beim Generieren der Datenschutzerklärung „vorsichtshalber“ alle Optionen ausgewählt. Ein anderes Beispiel ist die Aushändigung eines einheitlichen, völlig überladenen Dokuments an Bewerber, Besucher und Klienten, das sämtliche potentielle Datenverarbeitungen enthält, die die Einrichtung betreffen könnten.

Das KDG sieht jedoch ausdrücklich vor, dass die Datenschutzinformation in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ bereitzustellen ist. Das setzt vor allem voraus:

- Beschränkung auf die tatsächlich stattfindenden Datenverarbeitungen
- Fokussierung auf die jeweilige Zielgruppe
- Übersichtlichkeit in der Darstellung

Zusammengefasst: Die Datenschutzinformation muss so gestaltet sein, dass die Inhalte zutreffen und die betroffene Person diese verstehen kann.

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, insbesondere:

- 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

Zur Erfüllung der Aufgaben wird dem Diözesandatenschutzbeauftragten angemessene Personal- und Sachausstattung zur Verfügung gestellt. Im Berichtsjahr 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 2024 wurden Haushaltsmittel in Höhe von 378.372 EUR aufgewendet.

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