Katholische
Datenschutzaufsicht Nord

9. Jahresbericht

2022

www.kdsa-nord.de

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

Der nachfolgende Tätigkeitsbericht schließt an den 8. Jahresbericht an und umfasst den Zeitraum vom 1. Januar 2022 bis zum 31. Dezember 2022.

Noch immer hat auch im aktuellen Berichtsjahr die Pandemie die Menschen im Griff, und das hat die Tätigkeit im Bereich der Katholischen Datenschutzaufsicht Nord natürlich beeinflusst, auch wenn insbesondere über die Sommerzeit der Eindruck zu gewinnen war, als sei die Lage weitgehend entspannt.

Im Gegensatz dazu war in den Betreuungseinrichtungen der Kirche und der Caritas, genau wie in den Krankenhäusern in unserem Zuständigkeitsbereich, ein Zutritt auch weiterhin nur unter den Voraussetzungen eines aktuell gültigen und negativen Testergebnisses möglich. Der gesundheitliche Schutz der Bewohner und Patienten war oberstes Ziel. Auch deshalb haben wir uns, wie schon im letzten Jahr, mit einigen Ausnahmen im Bereich der Kirchengemeinden, auf Querschnitts- und Dokumentenprüfungen eingestellt, und dabei wie angekündigt insbesondere den Bereich der Caritas in den Focus genommen. Das Ergebnis der Prüfung wird in diesem Bericht veröffentlicht.

Fast schon tradiert haben wir unsere Aufgabenwahrnehmung der Situation angepasst und uns neben der telefonischen und schriftlichen Beratung von Betroffenen und Verantwortlichen auch im Bereich der Kommunikation mit unseren Gesprächspartnern immer noch auf Hybrid- oder Videokonferenzen verständigt. Auch wenn tatsächlich ein Teil der für das Berichtsjahr geplanten Sitzungen der Diözesandatenschurzbeauftragten in präsenter Form abgehalten werden konnte, gilt dies grundsätzlich auch für den notwendigen kollegialen Austausch. Es gibt sicher viele Gründe, die für diese Art der technikbasierten Kommunikation sprechen, nicht zuletzt die Fragen im Zusammenhang mit der Verantwortung der Kirche für die Umwelt zum Beispiel durch die Vermeidung von Dienstfahrten, und dieser Trend wird auch nicht mehr umzukehren sein. Ich hoffe aber, dass dabei trotzdem zukünftig der präsente Umgang mit den Gesprächspartnern in einem ausgewogenen Verhältnis erhalten bleibt.

Die Meldung von Datenschutzverletzungen hat sich auf dem vergleichbaren Vorjahresniveau eingependelt und die Anzahl der Beschwerden war leicht rückläufig, was insgesamt als positives Indiz für ein mittlerweile funktionierendes Datenschutzniveau gewertet werden könnte.

Im Hinblick auf die schon mehrfach angesprochene Änderung der rechtlichen Struktur der Katholischen Datenschutzaufsicht Nord gab es Licht am Ende des Tunnels. Der finale Satzungsentwurf für die beabsichtigte Gründung einer Körperschaft des öffentlichen Rechts mit Sitz in Bremen als Träger der Aufsichtsbehörde ist fertiggestellt. Bis zum Jahreswechsel sollen dem Vernehmen nach alle erforderlichen Vertragsentwürfe, die im Zusammenhang mit einem Trägerwechsel erforderlich sind, zur Verfügung stehen. Über die politische Vertretung der Katholischen Kirche in Bremen (Katholisches Büro) soll zum Beginn des neuen Jahres das Errichtungsverfahren mit der Landesregierung eingeleitet werden.

Ein anderer „Dauerbrenner“ bei der Aufgabenwahrnehmung der kirchlichen Aufsichtsbehörde war die Nutzung von Dienstleistungen großer Anbieter im Zusammenhang mit der Verarbeitung personenbezogener Daten in unsicheren Drittstaaten. Zwar wurde berichtet, dass die EU und die USA eine grundsätzliche Einigung darüber erzielt haben, wie ein neues Modell aussehen könnte („Trans-Atlantic Data Privacy Framework“[1]). Damit soll zukünftig wieder eine verlässliche datenschutzrechtliche Basis für den Einsatz von amerikanischen Cloud-Diensten geschaffen werden. Dabei sollen die rechtlichen Schwächen behoben worden sein, an denen der ursprüngliche Privacy Shield beim Europäischen Gerichtshof gescheitert war. Ob damit die Probleme im Hinblick auf Facebook, Google oder Microsoft Cloud etc. eine datenschutzkompatible Lösung erfahren können bleibt aber abzuwarten.

Derzeit raten wir bei Anfragen dringend davon ab, Dienste in Anspruch zu nehmen, die ohne valide Rechtsgrundlage eine Datenverarbeitung in einem unsicheren Drittstaat (Bsp.: USA) vornehmen.

Seit jetzt sieben Jahren nehme ich gerne die mir durch den Erzbischof von Hamburg, und die Bischöfe von Osnabrück und Hildesheim und dem Offizial des Bischöflich Münsterschen Offizialats in Vechta übertragenen Aufgaben als gemeinsamer Diözesandatenschutzbeauftragter war. Es ist und war eine immer spannende und zugleich verantwortungsvolle Aufgabe, die unter der Prämisse des Schutzes

[1] EDPB Statement 01/2022 on the announcement of an agreement in principle on a new Trans- Atlantic Data Privacy Framework / Adopted on 6 April 2022

der personenbezogenen Daten der Menschen im kirchlichen Bereich von Beratung und Anleitung für deren Schutz einerseits und Sanktionierung von Fehlverhalten andererseits geprägt war. Dabei war es meine persönliche Motivation, auch im Sanktionsfall bei den Beteiligten immer das Verständnis für eine Optimierung des Schutzes der Menschen zu erreichen.

Aber unabhängig davon, ob das in jedem Fall gelungen ist, endet mit Ablauf dieses Jahres meine aktive Dienstzeit und ich verabschiede mich in den Ruhestand. Ich freue mich sehr, dass als neuer gemeinsamer Diözesandatenschutzbeauftragter mein Kollege und bisheriger Stellvertreter Herr Andreas Bloms von den Bischöfen für die Fortführung der Aufgaben vorgesehen ist. Für mich persönlich ist es eine große Beruhigung, die Leitung der Behörde in kompetente und erfahrene Hände geben zu können. Ich bin Herrn Bloms sehr dankbar für die bisherige Zusammenarbeit und wünsche Ihm als meinem Nachfolger alles Gute für die anstehenden Aufgaben.

Ich darf mich an dieser Stelle auch bei all denjenigen bedanken, die meine Arbeit und meine Bemühungen um den Datenschutz in der Katholischen Kirche in den zurückliegenden sieben Jahren begleitet und unterstützt haben. Das gilt vor allem für die Herren Generalvikare, die den Aufbau und die Arbeit der Aufsichtsbehörde in Bremen begleitet und die Unabhängigkeit des Diözesandatenschutzbeauftragen im vollen Umfang respektiert und gewährleistet haben. Die Finanzierung des notwendigen Sachbedarfs ist regelmäßig ohne Probleme erfolgt, so dass einer eingehenden und verantwortungsvollen Arbeitsweise nichts entgegengestanden hat. Mein Dank gilt auch den Kollegen, den Datenschutzreferenten, den Justiziaren, den betrieblichen Datenschutzbeauftragten und den IT-Leitern und Technikern der Bistümer, mit denen jederzeit eine vertrauensvolle Zusammenarbeit möglich war.

Dabei ist mir die Feststellung ein Anliegen, dass ich die der Katholischen Datenschutzaufsicht Nord obliegenden Aufgaben nicht allein hätte erfüllen können, sondern nur in einem motivierten und engagierten Team von Mitarbeitern dazu in der Lage war. Ihnen allen gilt mein ganz besonderer Dank.

Mein Tätigkeitsbericht für das Jahr 2022 wird nachstehend vorgelegt. Wie üblich wird neben einer zusammenfassenden Darstellung der Entwicklung des Datenschutzrechtes auf europäischer, deutscher und kirchlicher Ebene auch exemplarisch auf wesentliche Vorkommnisse in dem Berichtszeitraum hinweisen, die von allgemeiner Bedeutung für die Dienststellen sein können.

Bremen, im Dezember 2022

Andreas Mündelein

Diözesandatenschutzbeauftragter

1. Die Entwicklung des Datenschutzrechts

1.1. Europarecht

1.1.1. „Trans – Atlantic Data Privacy Framework"

Wie berichtet, konnte nach der Entscheidung des EuGH vom 16. Juli 2020 („Schrems II") ein Drittstaatentransfer von personenbezogenem Daten in die USA (Drittland) nicht mehr auf das Datenschutzabkommen („Privacy Shield") gestützt werden, weil das erforderliche Datenschutzniveau der EU durch das Abkommen nicht gewährleistet werden konnte. Um den Datenaustausch zwischen den USA und der EU wieder auf eine sichere rechtliche Grundlage zu stellen, haben die EU und die USA eine grundsätzliche Einigung darüber getroffen, wie ein neues Modell aussehen könnte. Zielvorstellung war es dabei, zukünftig wieder eine verlässliche datenschutzrechtliche Basis für den Einsatz von amerikanischen Cloud-Diensten zu schaffen. Nachdem die Unterzeichnung der zugehörigen Executive Order am 7. Oktober 2022 durch den US-Präsidenten[2,3] erfolgt war, veröffentlichte die Europäische Kommission am 13. Dezember 2022 den Entwurf eines Angemessenheitsbeschlusses.[4]

Die neuen Regelungen sollen den Schutz der personenbezogenen Daten von EU-Bürgern vor dem Zugriff der US-Geheimdienste verbessern.

Die Exekutivanordnung (E.O.) sieht u.a. vor, dass weitere Schutzmaßnahmen vor US-Signalspionageaktivitäten hinzugefügt werden, einschließlich der Anforderung, dass solche Aktivitäten nur in Verfolgung definierter nationaler Sicherheitsziele durchgeführt werden; die Privatsphäre und die bürgerlichen Freiheiten aller Personen, unabhängig von ihrer Nationalität oder ihrem Wohnsitzland, berücksichtigen; und nur durchgeführt werden, wenn es notwendig ist, um eine validierte nachrichtendienstliche Priorität voranzutreiben, und nur in dem Ausmaß und auf eine Weise, die dieser Priorität angemessen ist.

Die E.O. regelt den Umgang mit personenbezogenen Daten, die im Rahmen von nachrichtendienstlichen Aktivitäten erhoben werden, und erweitert die Zuständigkei-

---

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

[3] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045

[4] https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7631

ten von Rechts-, Aufsichts- und Compliance-Beamten, um sicherzustellen, dass geeignete Maßnahmen ergriffen werden, um Verstöße gegen die Vorschriften zu beheben. Deshalb wird durch die E.O. gefordert, dass die Mitglieder der U.S. Intelligence Community, ihre Richtlinien und Verfahren aktualisieren, um die in der Ordnung enthaltenen neuen Schutzmaßnahmen für den Datenschutz und die bürgerlichen Freiheiten zu berücksichtigen.

Darüber hinaus enthält der Erlass einen neuen mehrstufigen Beschwerdemechanismus, mit dessen Hilfe sich EU-Bürger gegen die Sammlung ihrer Daten durch US-Behörden wehren können.

Im Rahmen der ersten Stufe führt der Civil Liberties Protection Officer im Office of the Director of National Intelligence (CLPO) eine erste Untersuchung der eingegangenen qualifizierten Beschwerden durch, um festzustellen, ob die verstärkten Sicherheitsvorkehrungen der E.O. oder andere anwendbare US-Gesetze verletzt wurden, und, falls dies der Fall ist, um geeignete Abhilfemaßnahmen zu bestimmen.

Als zweite Überprüfungsebene ermächtigt und weist die E.O. den Generalstaatsanwalt an, ein Datenschutzüberprüfungsgericht ("DPRC") einzurichten, das auf Antrag der betroffenen Person oder eines Teils der Intelligence Community eine unabhängige und verbindliche Überprüfung der Entscheidungen des CLPO vornimmt.[5]

Auf Basis des neuen Erlasses muss die EU-Kommission eine sogenannte Angemessenheitsentscheidung treffen. Dabei wird festgestellt, dass in einem Drittstaat ein vergleichbares Datenschutzniveau wie in der EU existiert. Es wird nicht mit einer Entscheidung vor dem Frühjahr 2023 gerechnet.

Dem Vernehmen nach ist zudem eine weitere Klage gegen die neue notwendige Angemessenheitsentscheidung nicht ausgeschlossen, vor dem Hintergrund der Kritik, dass eine Massenüberwachung weiterhin uneingeschränkt zulässig sei.

1.1.2. „Weg in die digitale Dekade“

Bei dem strategischen Ziel der EU, den digitalen Wandel im Einklang mit ihren Werten zu erreichen, haben der Rat und das Europäische Parlament eine vorläufige Einigung in Bezug auf das Politikprogramm für 2030 „Weg in die digitale Dekade“ erzielt.

[5] https://community.beck.de/2022/10/07/breaking-news-7102022-president-biden-unterzeichnet-executive-order-zum-eu-us-data-privacy-framework

Der Beschluss soll die digitale Führungsrolle der EU stärken, indem eine inklusive und nachhaltige Digitalpolitik im Dienste der Bürgerinnen und Bürger und der Unternehmen gefördert wird. Zu diesem Zweck werden die konkreten Digitalziele in den Bereichen Kompetenzen, sichere und tragfähige digitale Infrastrukturen, digitaler Umbau von Unternehmen und Digitalisierung öffentlicher Dienste festgelegt, die die Union bis Ende des Jahrzehnts erreichen will. Mit dem Politikprogramm wird eine neue Art der Governance eingeführt, die auf der Zusammenarbeit zwischen den Mitgliedstaaten und der Kommission beruht, um sicherzustellen, dass die Union ihre Ziele als Ganzes erreicht.[6]

Verbunden wird das Ziel mit unterschiedlichen Gesetzesvorhaben, wie etwa:

- Data Governance Act (DGA)

Der Europäische Rat hat am 16. Mai 2022 eine Verordnung zur Daten-Governance verabschiedet. Die Verordnung fördert die Weiterverwendung von Daten öffentlicher Einrichtungen unter anderem zu Forschungszwecken. Ein Datenregister auf EU-Ebene und zentrale Anlaufstellen in den Mitgliedstaaten sollen Interessierte beim Datenzugang unterstützen. Die neuen Regeln treten 15 Monate nach Veröffentlichung der Verordnung in Kraft.[7]

- Digital Markets Act (DMA, Plattformregulierung: Wettbewerbsregulierung) (In Kraft seit 01.01.2022; Übergangsfristen, voll wirksam ab 25.06.2023)[8]
- Digital Services Act (DSA, Plattformregulierung: illegale Inhalte, Missinformation, transparente Werbung) (In Kraft seit 16.11.22, Übergangsfristen, voll wirksam ab 16.02.24)[9]
- Data Act (DA; Datennutzung)[10]

„Der Gesetzesentwurf des Data Act sieht Regelungen vor, die klären sollen, wer unter welchen Bedingungen einen Mehrwert aus Daten schaffen kann *[…]*. *[…]* Der

---

[6] https://www.consilium.europa.eu/de/press/press-releases/2022/07/14/policy-programme-path-to-the-digital-decade-the-council-and-the-european-parliament-reach-a-provisional-agreement/

[7] https://www.consilium.europa.eu/de/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925&qid=1671527597637

[9] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2022:277:TOC

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0068&qid=1667848388499

Entwurf wurde im Februar 2022 durch die Europäische Kommission vorgelegt. Das Konsultationsverfahren vor dem Europäischen Wirtschafts- und Sozialausschuss wurde bis Mai 2022 durchgeführt. Derzeit liegt die Verordnung dem Europäischen Parlament und dem Rat vor, wobei der Zeithorizont bis zu einer Entscheidung noch offen ist."[11]

- Artificial Intelligence-Act (AI, KI-Anwendungen)[12]

(Entwurf eines Rechtsrahmen für einen sicheren und gesetzmäßigen Betrieb von KI-Systemen sowie Innovationsförderung[13])

1.2. Bundesrecht

1.2.1. Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Wie berichtet, ist am 1. Dezember 2021 ein Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG) in Kraft getreten.

Mit dem Gesetz soll datenschutzrechtliche Sicherheit im Bereich der Telekommunikation und dem Telemediengesetz geschaffen werden.

Eine Konsequenz aus diesem Gesetz ist die Notwendigkeit der Klärung der Zuständigkeit der Datenschutzaufsichten im Zusammenhang mit Anwendungen, bei denen die Kommunikation im Vordergrund steht, insbesondere Tools im Bereich der Videokommunikation.

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen hat dazu die Auffassung vertreten, dass nach ihrer Ansicht der Bundesbeauftragte für den Datenschutz nach § 29 TTDSG für die datenschutzrechtliche Aufsicht über geschäftsmäßig erbrachte Telekommunikationsdienste zuständig ist und deshalb grundsätzlich auch die Aufsicht über Videokonferenzdienste in seine Zuständigkeit fällt.[14] Die Auffassung wird diesseits, ebenso wie von dem Bayerischen Diözesandatenschutzbe-

[11] https://www.srd-rechtsanwaelte.de/blog/data-act-regelungen/

[12] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

[13] https://svb-muelot.de/neuigkeiten/dafta/

[14] https://www.ldi.nrw.de/handreichung-zu-online-pruefungen-hochschulen

auftragter[15], zumindest für den Bereich der Videokommunikationssysteme in der kirchlichen Anwendung geteilt.

1.3. Datenschutzrecht der Kirche

1.3.1. Evaluation KDG

Das Gesetz sollte innerhalb von drei Jahren überprüft werden (vgl. § 58 Abs. 2 KDG). Bisher ist es aber aus unterschiedlichen Gründen nicht gelungen, den Prozess auf der Ebene des Verbandes der Diözesen Deutschlands zu einem Abschluss zu bringen.

1.3.2. Entscheidungen der Datenschutzgerichte

Eine sehr übersichtliche und kommentierte Zusammenstellung befindet sich im Bericht des Diözesandatenschutzbeauftragten der Bayerischen (Erz-)Diözesen[16]

Im Übrigen wird auf die Zusammenstellung im Rahmen der Entscheidungssammlung der katholischen Datenschutzgerichte unter „Artikel 91. Datenschutz in Kirchen und Religionsgemeinschaften“[17] verwiesen.

1.3.3. Konferenz der Diözesandatenschutzbeauftragten

Die kirchlichen Datenschutzaufsichten haben sich im Rahmen einer „Konferenz der Diözesandatenschutzbeauftragten“ mit dem Ziel zusammengeschlossen, eine möglichst einheitliche Anwendung der kirchlichen Datenschutzbestimmungen zu gewährleisten. Sie entsprechen damit den gesetzlichen Vorgaben nach § 46 KDG. Die Konferenz tagt mehrfach im Jahr nach einem abgestimmten Verfahrensablauf.

Trotz der Pandemieauswirkungen hat die Konferenz viermal in präsenter Form und zweimal als Videokonferenz getagt.

Konferenzen der Diözesandatenschutzbeauftragten fanden statt am:

- 27. Januar 2022 - 1.Konferenz (Videokonferenz)
- 27. April 2022 - Ökumenischer Datenschutztag Berlin

---

[15] Bericht des Gemeinsame Datenschutzaufsicht der Bayerischen (Erz-)Diözesen Diözesandatenschutzbeauftragter vom 1. Oktober 2022, Seite 2; abrufbar unter: https://www.erzbistum-muenchen.de/ordinariat/datenschutzstelle/konferenz-der-dioezesandatenschutz-beauftragten/90605

[16] Bericht des Gemeinsame Datenschutzaufsicht der Bayerischen (Erz-)Diözesen Diözesandatenschutzbeauftragter vom 1. Oktober 2022, Seite 3

[17] https://artikel91.eu/rechtssammlung/roemisch-katholische-kirche/entscheidungssammlung-der-katholischen-datenschutzgerichte/

- 28. April 2022 - 2. Konferenz Berlin
- 15. Juni 2022 - 3. Konferenz (Videokonferenz)
- 14./15. September 2022 - 4. Konferenz Dachau
- 9./10. November 2022 - 5. Konferenz Bremen

Die Konferenz fördert den Datenschutz und verständigt sich auf gemeinsame Positionen. Dies geschieht unter anderen 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. Zum Sprecher für das Jahr 2023 ist Herr Ullrich gewählt worden.

Folgender Beschluss ist durch die Konferenz der Diözesandatenschutzbeauftragten im Berichtsjahr veröffentlicht worden:

- Beschluss Dispositionsrecht zur Einwilligung in die Nichtanwendung von technischen und organisatorischen Maßnahmen, Konferenz vom 15. Juni 2022, dieser Beschluss ersetzt den Beschluss der Konferenz aus September 2019

Sämtliche veröffentlichte Beschlüsse können auf unserer Homepage abgerufen werden.[18]

2. Katholische Datenschutzaufsicht Nord

2.1. Die Struktur der Katholischen Datenschutzaufsicht Nord

Wie schon mehrfach berichtet, hat die kirchliche Datenschutzaufsicht die in Kapitel VI der DS-GVO niedergelegten Bedingungen zu erfüllen (Art. 51, 59 i.V.m. Art. 91 Abs. 2 DS-GVO), und die katholische Kirche hat dies durch die §§ 42-46 KDG sichergestellt. Die Verpflichtung der Diözesen umfasst darüber hinaus die Sicherstellung der personellen, technischen und finanziellen Ressourcen. (vgl. Art. 52 Abs. 4 i.V.m. Art. 91 Abs. 2 DS-GVO). Die KDSA Nord ist rechtlich als unabhängige Stelle eigener Art konfiguriert.

Auf die geplante Umsetzung der rechtlichen Neustrukturierung der Aufsichtsbehörde in eine Körperschaft des öffentlichen Rechts ist in der Konkretisierung auch im letz-

[18] https://www.kdsa-nord.de/beschluesse

ten Jahr noch nicht vollendet worden. Wie bereits erwähnt gibt es aber „Licht am Ende des Tunnels“. Bis zum Jahreswechsel sollen alle erforderlichen Vertragsentwürfe, die im Zusammenhang mit einem Trägerwechsel erforderlich sind, zur Verfügung stehen. Über die politische Vertretung der Katholischen Kirche in Bremen (Katholisches Büro) soll zum Beginn des neuen Jahres das Errichtungsverfahren mit der Landesregierung eingeleitet werden.

Das Stellentableau umfasst aktuell vier Vollzeitstellen unter Einbeziehung des Sekretariats. Nach dem altersbedingten Ausscheiden des bisherigen Leiters wird die Stelle eines juristischen Referenten neu zu besetzen sein.

2.2. Statistik und Zahlen

Der Eingang von Beschwerden ist im Vergleich zum Vorjahr leicht rückläufig. Ebenso verhält es sich bei den Beratungsanfragen, wobei bei den Beratungsanfragen ein leichter Trend hin zu komplexeren und umfangreicheren Anfragen verzeichnet werden kann.

Die Meldungen von Verletzungen des Schutzes personenbezogener Daten bewegt sich auf dem Vorjahresniveau. Die im vergangenen Jahr bekanntgewordene Schwachstelle in Exchange-Servern hatte für eine kurzfristige Erhöhung der Meldungen in diesem Bereich gesorgt.

Bei den Prüfungen im Berichtszeitraum haben wir uns auf den Abschluss der Querschnittsprüfung bei den Caritasverbänden beschränkt. Prüfungen vor Ort sind pandemiebedingt erst nach der Sommerzeit bei allgemein rückläufigen Inzidenzen durchgeführt worden. Zwei Kirchengemeinden und ein Dienst der Caritas Nord konnten besucht werden. Für das kommende Jahr werden die Prüfungen hoffentlich wieder planmäßig erfolgen können.

Die Mitarbeiter der KDSA Nord haben im Berichtszeitraum an folgenden Arbeitsgruppen (extern und intern) teilgenommen, die im Wesentlichen als Videokonferenzen durchgeführt wurden.

- Konferenz der DDSB
- Evaluierung KDG
- AK Technik DDSB
- AK Technik DSK

- KDM (ÖPG und UAG KiTa Beispiel)

2.3. Betriebliche Datenschutzbeauftragte in den Einrichtungen

Es ist nicht nur üblich, sondern auch hilfreich, an dieser Stelle des Berichts auf die gesetzlich normierte Notwendigkeit der kirchlichen Einrichtungen zur Bestellung betrieblicher Datenschutzbeauftragter nach § 36 Abs. 1 KDG hinzuweisen und feststellen zu können, dass die Bistümer im Zuständigkeitsbereich der KDSA Nord dieser Verpflichtung nachgekommen sind.

Auf die wesentlichen Vorteile der Professionalisierung im Bereich der Beratung der Einrichtungen im Zusammenhang mit dem kirchlichen Datenschutz wurde schon mehrfach hingewiesen. Dessen ungeachtet ist es mir aber auch in diesem Jahr ein Anliegen, mich bei den Damen und Herren zu bedanken, die mit ihrer Fachkompetenz und Freundlichkeit die kirchlichen Einrichtungen als betriebliche Datenschutzbeauftragte betreuen. Mit meinem Dank verbinde ich die Aufforderung sich auch zukünftig im Rahmen der etablierten Verfahren bei der Aufsichtsbehörde einzubringen.

2.4. Kirchliches Datenschutz Modell (KDM)- aktueller Stand

Auch in diesem Berichtszeitraum hat die ökumenische Projektgruppe aus den Datenschutzaufsichten der katholischen und evangelischen Kirche ihre Arbeiten an dem Kirchlichen Datenschutzmodell (KDM) fortgesetzt. Die Entwicklung des KDM, das seinen Ursprung im Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat, war schon Gegenstand in den vergangenen Tätigkeitsberichten.

Im Rahmen der Aktivitäten der UAG des KDM, die sich mit der beispielhaften Anwendung des KDM auf eine Verarbeitungstätigkeit in einer fiktiven Kindertagesstätte beschäftigt, haben im Februar dieses Jahres zwei Workshops unter dem Titel „Werkstatt Datenschutzmodelle“ stattgefunden, die zum Austausch zwischen der UAG SDM des AK Technik der DSK genutzt wurden. Ferner wurden die Arbeiten an dem Fallbeispiel wie auch an den in diesem Zusammenhang erarbeiteten (Hilfs-)Mitteln fortgesetzt.

2.5. Öffentlichkeitsarbeit

Die KDSA Nord hat die Öffentlichkeitsarbeit auch im Jahr 2022 auf vielfältige Weise fortgesetzt. So wurde u.a. der Aufbau der Internetseite aktualisiert und die Inhalte neu strukturiert.

Ebenso hat die KDSA Nord die Öffentlichkeit über Meldungen auf der Homepage stets über aktuelle und wichtige Themen informiert.

Alle Meldungen können unter folgendem Link noch einmal abgerufen werden: https://www.kdsa-nord.de/meldungen

2.6. Informationsveranstaltungen

Es gehört zu den Aufgaben der KDSA Nord, der Nachfrage nach Informationsbedarf in den kirchlichen Einrichtungen nachzukommen. Die Mitarbeiter der KDSA Nord stehen dafür nach wie vor zur Verfügung. Den unbedingten Wunsch nach einer Präsenzveranstaltung hat es nicht gegeben, so dass alle Anfragen entweder telefonisch oder im Rahmen von Videokonferenzen bearbeitet worden sind. Auch die regelmäßigen Termine wie etwa

- Jour Fixe mit den betrieblichen Datenschutzbeauftragten
- IT Tagungen
- Treffen mit Diözesanjuristen

wurden virtuell durchgeführt.

3. Exemplarische Darstellung von Einzelfragen und Einzelfällen

3.1. Beratungen

3.1.1. Weitergabe von Meldedaten an Zeitungsverlage

Eine Beratungsanfrage erreichte uns von einem Bistum zu der Zulässigkeit der Weitergabe personenbezogener Daten an die Kirchenzeitung. Die Weitergabe der personenbezogenen Daten zum Zwecke der Durchführung der Werbemaßnahme ist hierbei getrennt von der Frage der inhaltlichen Ausrichtung auf die Bereiche Seelsorge und die Verkündigung des Glaubens der Kirchenzeitung zu prüfen. In einer Stellungnahme haben wir dem Bistum sodann mitgeteilt, dass die Weitergabe der beim Bistum vorliegenden Meldedaten an die Kirchenzeitung dann nicht zulässig ist, wenn dies zu dem Zweck erfolgt, die Meldedaten für die Anwerbung von Neukunden zu nutzen. Im Vordergrund steht hierbei das wirtschaftliche Interesse des Zeitungsverlages, die Abonnentenzahl zu erhöhen. Dieses wirtschaftliche Interesse haben wir als nicht vereinbar mit § 42 Abs. 1 Bundesmeldegesetz angesehen, wonach einer öffentlich-rechtlichen Religionsgemeinschaft zur „Erfüllung ihrer Aufgaben“ be-

stimmte Daten zur Verfügung gestellt werden dürfen.

In einem anderen Zusammenhang liegt uns eine Beschwerde zu der Weitergabe der Meldedaten an eine Kirchenzeitung vor. Da hierzu jedoch noch der Eingang von Stellungnahmen der betroffenen Einrichtungen erwartet wird, ist mit einem Abschluss des Beschwerdeverfahren erst in 2023 zu rechnen.

3.1.2. Einrichtung eines Kontaktformulars in einer Gesundheitseinrichtung

Ein betrieblicher Datenschutzbeauftragter eines Krankenhauses teilte mit, dass beabsichtigt ist, ein Kontaktformular auf der Webseite zu integrieren. Über dieses Kontaktformular sollten die Patienten ebenfalls die Möglichkeit haben, z.B. Befunde oder Berichte von MRT-Untersuchungen hochzuladen. Die genaue technische Ausgestaltung diese Kontaktformulars war zum Zeitpunkt der Anfrage noch nicht bekannt, sodass lediglich allgemeine Hinweise gegeben werden konnten.

Neben der erforderlichen Rechtsgrundlage für die Erhebung von Gesundheitsdaten sind bei der Auswahl und dem Setup eines Kontaktformulars besondere Aspekte zu beachten. Allgemeine Gefährdungen, die zu einer Kompromittierung der Daten oder zu einem Verstoß gegen datenschutzrechtliche Vorgaben führen können, können folgende sein:

- unzureichende Prüfung von eingegebenen Daten
- unzureichende Prüfung hochgeladener Dateien (bspw. auf Schadcode und Dateiformat)
- sofern eine Authentisierung vor dem Upload erforderlich ist: Möglichkeit unberechtigter Uploads (z.B. kein Brute-Force Schutz gegen das Durchprobieren von Zugangscredentials)
- unzureichendes Sessionmanagement oder unzureichende Authentisierung des Nutzers
- unzureichendes Berechtigungsmanagement im Uploadportal oder der ggf. dahinterliegenden Dateiablage
- unzureichende Verschlüsselung bei der Übermittlung der Daten
- unzureichende Separierung der Systeme

Bei der Auswahl und Konzeption des Dienstes sowie der dahinterliegenden Systeme, sollte immer berücksichtigt werden, dass es sich vorliegend um Gesundheitsdaten handelt und damit um personenbezogene Daten der Datenschutzklasse III ge-

mäß § 13 Abs. 1 KDG.

Daneben müssen ebenfalls die allgemeinen datenschutzrechtlichen Anforderungen, wie die Information der Betroffenen über die Verarbeitung der Daten und die Einhaltung von Speicherfristen (Löschkonzept) berücksichtigt werden.

3.2. Beschwerden

3.2.1. Auskunftsanspruch

Es erreichte uns eine Beschwerde, in der die Beschwerdeführerin mitteilte, ein geltend gemachter Auskunftsanspruch sei nicht erfüllt worden. Hierdurch sollte eine mögliche unrechtmäßige Offenlegung der personenbezogenen Daten geprüft werden. Nach Klärung der Zuständigkeiten ist die Kirchengemeinde als Trägerin der Einrichtung aufgefordert worden, eine Stellungnahme zu dem Vortrag der Beschwerdeführerin einzureichen. Weder aus der Stellungnahme noch aus den sonstigen eingereichten Dokumenten ließ sich eine unbefugte Offenlegung in Bezug auf die personenbezogenen Daten feststellen. Die von der Beschwerdeführerin beantragte Auskunft ist während des Beschwerdeverfahrens erteilt worden. Da es sich vorliegend um eine Kirchengemeinde handelt, ist in diesem Verfahren eine datenschutzrechtliche Beanstandung ausgesprochen worden. Anordnungen wurden keine getroffen, da während des Verfahrens keine grundsätzlichen Mängel festgestellt wurden. Die Beschwerde war somit lediglich hinsichtlich der nicht fristgemäßen Auskunftserteilung erfolgreich.

3.3. Datenpannen

3.3.1. Offenlegung einer Notfallkontaktliste

Uns wurde angezeigt, dass in einer Grundschulklasse anstelle der Klassenliste mit den üblichen Kontaktdaten versehentlich die Liste mit den Notfallkontakten verteilt worden ist. Diese enthielt neben den Kontaktdaten der Erziehungsberechtigten auch weitere, zum Teil vertrauliche Daten wie auch die Daten Dritter und enthüllte darüber hinaus Informationen über die Konstellation innerhalb der Familien. Die Schulleitung hat die Eltern der betroffenen Kinder umgehend informiert und um eine Rückgabe der Listen gebeten; diese ist dann auch erfolgt. Die Listen wurden anschließend datenschutzkonform vernichtet. Der Schaden wurde durch die schnelle Reaktion eingegrenzt. Die Verteilung der Liste stellt eine unbefugte Offenlegung von personenbezogenen Daten und damit einen Verstoß gegen § 7 Abs. 1 lit. f) KDG dar, wonach personenbezogene Daten vor einer unbefugten Verarbeitung geschützt

werden müssen.

Das Problem lag in diesem Fall allerdings an einer anderen Stelle: unzureichende Zugriffsbeschränkungen.

Die Notfalllisten werden im Sekretariat unter Nutzung von bereitgestellten Informationen erstellt und dort während der allgemeinen Schulzeiten für Notfälle bereitgehalten. Außerhalb dieser Zeiten erfolgt eine gesicherte Aufbewahrung.

Die unbefugte Verarbeitung betrifft zum einen die Weiterleitung an die Eltern, zum anderen ist fraglich, aus welchem Grund es der Lehrkraft außerhalb eines Notfallszenarios möglich gewesen ist, auf die Notfalldaten zuzugreifen. Hier waren die Daten nicht hinreichend durch technische oder organisatorische Maßnahmen vor unbefugtem Zugriff gemäß § 6 Abs. 2 lit. c KDG-DVO gesichert gewesen.

3.3.2. Der verlorene USB-Stick

Bei einer weiteren Meldung einer Datenschutzverletzung ist uns mitgeteilt worden, dass ein unverschlüsselter USB-Stick auf dem Weg zum Empfänger abhandengekommen ist. Auf diesem USB-Stick war der Patientenbericht (Arztbericht/Entlassungsbericht) der betroffenen Person gespeichert. Es wurde vermutet, dass der Brief in der Sortiermaschine beschädigt worden ist und der USB-Stick hierdurch abhandenkam. Ein bei der Post in Auftrag gegebener Nachforschungsauftrag war bis zum Abschluss des Verfahrens erfolglos.

Neben einer datenschutzrechtlichen Beanstandung ist angeordnet worden, dass mobile Geräte und Datenträger, zu denen auch USB-Sticks gehören, mit geeigneten Verschlüsselungsverfahren zu verschlüsseln sind. Diese Anordnung folgt aus § 13 Abs. 2 S. 2 lit. a) KDG-DVO, wonach mobile Geräte oder Datenträger, auf denen personenbezogene Daten der Datenschutzklasse III gespeichert werden, zu verschlüsseln sind. Hierbei ist ebenso zu berücksichtigen, dass personenbezogene Daten der Datenschutzklasse III nur dann auf mobilen Geräten gespeichert werden dürfen, wenn dies aus dienstlichen Gründen zwingend erforderlich ist. Die Erforderlichkeit ist im Rahmen der allgemeinen Rechenschaftspflicht nach § 7 Abs. 2 KDG zu dokumentieren.

3.4. Prüfungen

Es ist eine der wesentlichen Aufgaben der Datenschutzaufsicht, über die Einhaltung der Vorschriften des Datenschutzgesetzes und anderer Vorschriften über den Datenschutz zu wachen. Im Hinblick auf die Überprüfung der Vorgaben in der Fläche

ist es erforderlich – anlasslos oder anlassbezogen – notwendige Untersuchungen einzuleiten. Diese können z.B. im Rahmen von Vor-Ort-Terminen, digital oder nach Aktenlage durchgeführt werden. Aufgrund der Gesamtsituation hat es sich neben den durchgeführten Prüfungen vor Ort bewährt, digitale Prüfungen zu etablieren.

Die Ergebnisse der Querschnittsprüfungen der Caritas-Verbände werden nachstehend exemplarisch beschrieben.

3.4.1. Querschnittsprüfung Caritas

Nach erfolgreichem Abschluss der Querschnittsprüfung Kindertagesstätten (s. 8. Jahresbericht der KDSA Nord) war im Jahr 2021 eine weitere Querschnittsprüfung gestartet. Die Prüfung wurde ebenfalls als Online-Prüfung konzipiert und erfolgte auf der Ebene der Caritas-Verbände

Die „Querschnittsprüfung Caritas“ zur Prüfung der in den Caritasverbänden in den norddeutschen (Erz-)Diözesen sowie im Bischöflich Münsterschen Offizialat Vechta umgesetzten datenschutzrechtlichen Vorgaben wie auch der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten wurde im September des Berichtsjahres abgeschlossen. Zusammen mit der Ergebnisdokumentation wurden ggf. auch Hinweise für eine Verbesserung sowie eine Auflistung von Nachbesserungsbedarfen an die verantwortlichen Stellen gesendet.

Wie schon die Überprüfung der Kindertagesstätten, erfolgte auch die Überprüfung der Einhaltung datenschutzrechtlicher Vorgaben in den Caritasverbänden über das Ausfüllen eines einheitlichen elektronischen Fragebogens sowie ggf. über die Beantwortung einrichtungsspezifischer Nachfragen. Die Prüfung erfolgte rein digital und ohne die Durchführung von Vor-Ort-Terminen – auf diese wurde vor dem Hintergrund der sich im Prüfungszeitraum rasant entwickelten Corona-Epidemie weiterhin verzichtet.

Hinsichtlich des Fragebogens war die Prüfung grundsätzlich anders konzipiert als ihre Vorgängerin: weniger als Ankreuzbogen, der vieles abzudecken versucht, sondern vielmehr als Liste offener Fragen, mit denen der Fokus auf speziell ausgewählte Bereiche gelegt wurde.

Trotz der Unterschiede zwischen einer Prüfung vor Ort und einer Online-Prüfung, konnten Hinweise für eine Verbesserung des Datenschutzes gegeben bzw. Nachbesserungsbedarfe (s.u.) identifiziert werden. Beiden Prüfungsarten gemein ist in jedem Fall eine Sensibilisierung für das Thema Datenschutz sowie ggf. seine Priori-

sierung in den geprüften Einrichtungen.

Behandelt wurden die Themenbereiche

- Datengeheimnis
- Rechte der betroffenen Person und Informationspflichten des Verantwortlichen
- Verantwortlicher und Auftragsverarbeiter
- Technische und Organisatorische Maßnahmen (TOM)

Der Prüfungsumfang betrug acht Fragen, mit denen in den jeweiligen Bereichen z. B. exemplarisch der Umgang mit Auskunftsersuchen oder Informationspflichten bei Bewerbungsverfahren erfasst werden sollte. Welche Auskünfte im Einzelnen erwartet wurden, wurde durch entsprechende Hinweise erläutert.

Teilgenommen haben die fünf Caritas-Verbände aus den norddeutschen (Erz-)Diözesen sowie dem Bischöflich Münsterschen Offizialat.

Die einzelnen Prüfpunkte wurden, wie schon bei der Querschnittsprüfung der Kindertagesstätten, dahingehend bewertet, ob bei den abgefragten Sachverhalten eine Abweichung von den datenschutzrechtlichen Vorgaben in Form eines Verbesserungspotenzials (Hinweises) oder eines Nachbesserungsbedarfs vorliegt.

- Ein „Hinweis“ wurde ausgesprochen, wenn die Erfüllung datenschutzrechtlicher Vorgaben möglicherweise noch verbessert werden kann. Eine Umsetzung ist nicht zwingend vorgeschrieben, sollte jedoch geprüft werden. Ggf. wurden diese auch für eine Sensibilisierung für einen bestimmten Sachverhalt genutzt.
- Ein „Nachbesserungsbedarf“ wurde festgestellt, wenn auf Grundlage der übermittelten Antworten die Erfüllung der gesetzlichen Anforderungen nicht gegeben ist und Veränderungen vorgenommen werden müssen.

Sofern Nachbesserungsbedarfe identifiziert worden sind, wurde die Online-Prüfung mit einem Bescheid als „Verwarnung“ abgeschlossen. In dem Fall, dass nur Hinweise ausgesprochen worden sind, wurde die Querschnittsprüfung mit einem Informationsschreiben beendet. Das entsprechende Schreiben wurde der Verantwortlichen Stelle zugesandt.

Einrichtungsübergreifend kann festgestellt werden, dass die Nachbesserungsbedarfe im Bereich der technischen und organisatorischen Maßnahmen (TOM) identifiziert worden sind. Die meisten Hinweise für eine mögliche Verbesserung des Datenschutzes wurden ebenfalls im Bereich TOM und speziell beim Prüfpunkt Berech-

tigungskonzept formuliert.

Insgesamt wurden aufgrund der festgestellten Verbesserungsbedarfe zwei Bescheide (Verwarnungen) und drei Informationsschreiben (einschließlich Hinweise) versandt (s. Abbildung 1). Die Verwarnungen enthielten dabei jeweils einen Nachbesserungsbedarf. In Abbildung 2 ist die durchschnittliche Anzahl der je Einrichtung ausgesprochenen Hinweise und Nachbesserungsbedarfe, sowie deren maximale wie minimale Werte dargestellt.

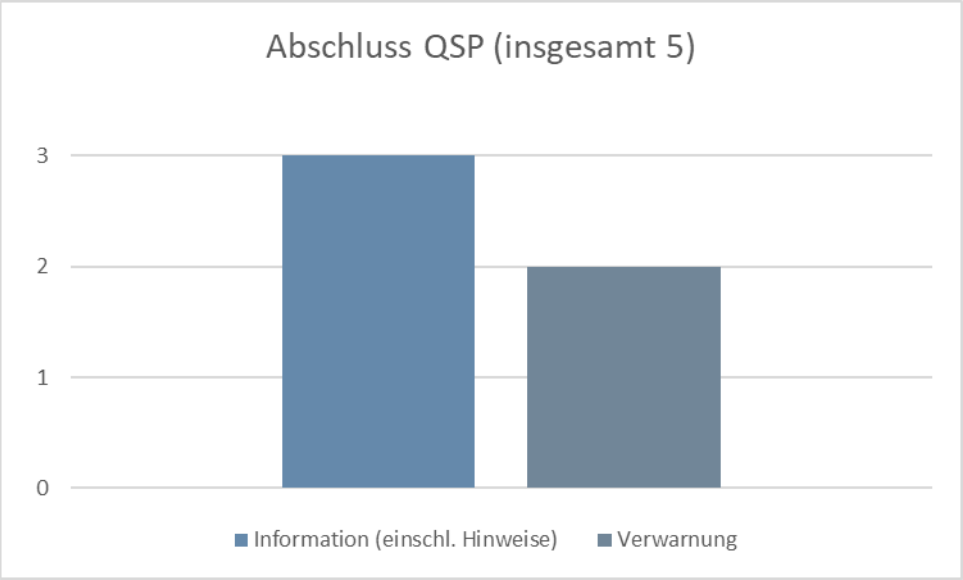

Abbildung 1 Ergebnis der Online-Prüfung im Hinblick auf die versandten Informationsschreiben und Bescheide (Verwarnung).

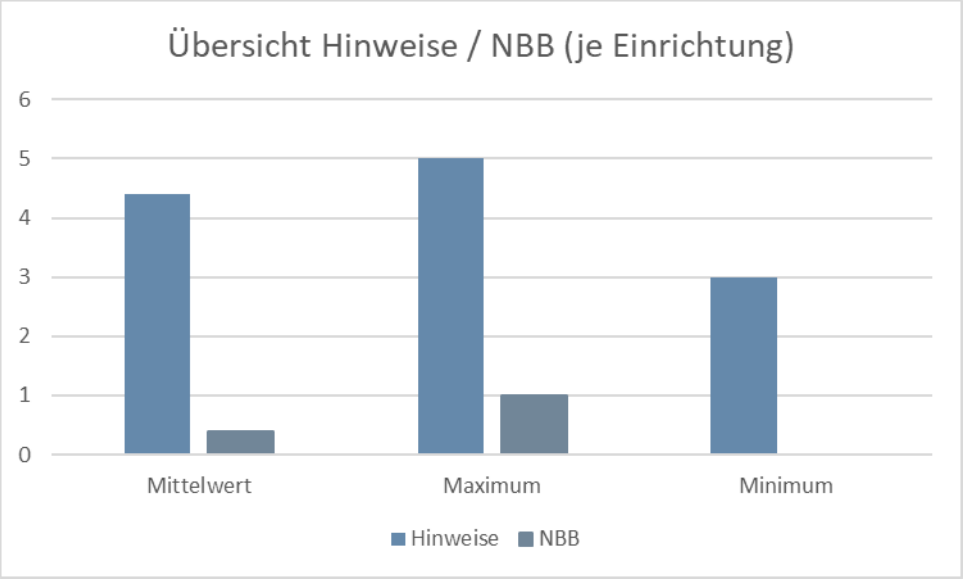

Abbildung 2 Ergebnisse der formulierten Hinweise und identifizierten Nachbesserungsbedarfe (NBB) für die Einrichtungen im Mittel, sowie die maximalen und minimalen Werte,

die in den Einrichtungen vorgekommen sind.

Die Einhaltung datenschutzrechtlicher Vorgaben in den o.g. Themenbereichen Datengeheimnis, Rechte der betroffenen Person und Informationspflichten des Verantwortlichen, Verantwortlicher und Auftragsverarbeiter sowie Technische und Organisatorische Maßnahmen (TOM) wurden anhand verschiedener spezifischer Prüfpunkte untersucht. Tabelle 1 beinhaltet eine Übersicht über die Anzahlen der zu den Themenbereichen/Prüfpunkten formulierten Hinweisen bzw. festgestellten Nachbesserungsbedarfen. Angegeben sind die Zahlen über alle geprüften Einrichtungen.

Tabelle 1 Anzahl der ausgesprochenen Hinweise und identifizierten Nachbesserungsbedarfe aufgeschlüsselt nach Themenbereich und Prüfpunkt. Ausgewertet wurden fünf Fragebögen.

Nr.	Themenbereich	Prüfpunkt	Anzahl Hinweise	Anzahl NBBe
1	Datengeheimnis	Mitarbeiterschulung	3	0
2	Betroffenenrechte & Informationspflichten	Auskunftsersuchen	2	0
3	Betroffenenrechte & Informationspflichten	Informationspflichten bei Bewerbungsverfahren	1	0
3	Verantwortlicher & Auftragsverarbeiter	Verzeichnis von Verarbeitungstätigkeiten	0	0
5	Verantwortlicher & Auftragsverarbeiter	Datenschutzverletzungen	3	0
6	TOM	Berechtigungskonzept	5	0
7	TOM	Löschkonzept	4	1
8	TOM	Patchmanagement	4	1[19]

[19] Der beim Prüfpunkt Patchmanagement festgestellte Nachbesserungsbedarf betrifft eigentlich das Thema "Verarbeitung personenbezogener Daten im Auftrag", ist allerdings bei der Erfassung der Regelungen zum Patchmanagement identifiziert worden.

Eine grafische Darstellung der absoluten Zahlen folgt in Abbildung 3

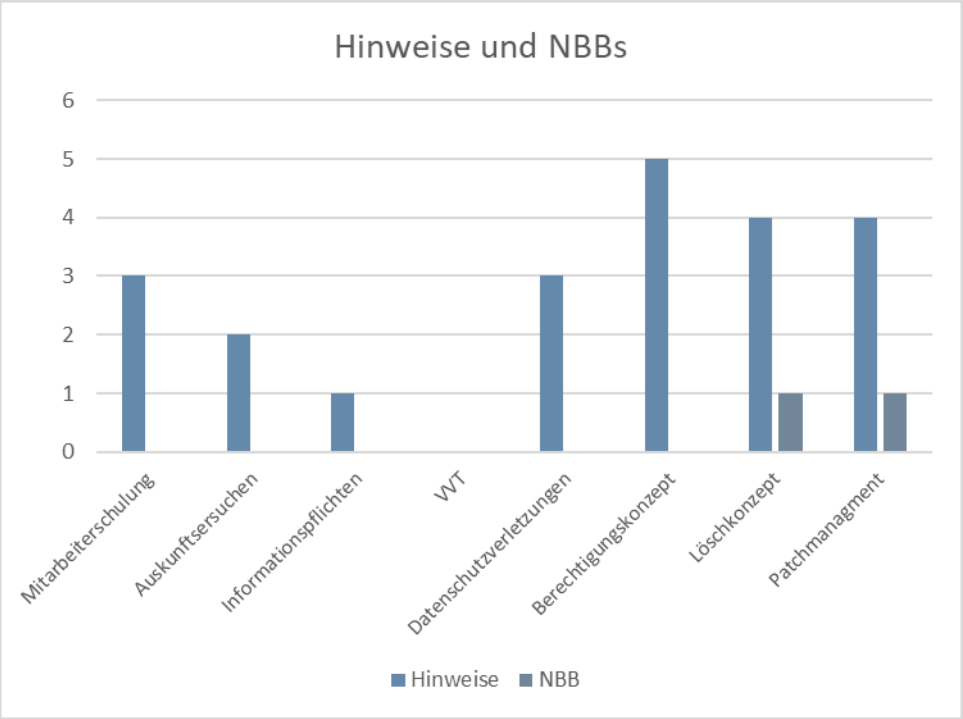

Abbildung 3 Grafische Darstellung der Daten aus Tabelle 1. Die Säulen stellen die Anzahlen der zu den Prüfpunkten ausgesprochenen Hinweise oder festgestellten Nachbesserungsbedarfe dar.

Die Einrichtungen sind aufgefordert, festgestellte Nachbesserungsbedarfe innerhalb einer vorgegebenen Frist zu beheben und dies nachweisen zu können.

4. Über die Dienststelle der Katholischen Datenschutzaufsicht Nord

4.1. Infrastruktur

Das Büro der KDSA Nord ist in der zentralen Innenstadt von Bremen eingerichtet. Die Anschrift lautet:

Unser Lieben Frauen Kirchhof 20, 28195 Bremen.

Das Büro ist regelmäßig von Montag bis Donnerstag in der Zeit von 09:00 bis 16:00 Uhr und am Freitag von 09:00 bis 12:00 Uhr zu erreichen.

Telefon: 0421 330056-0

E-Mail: info@kdsa-nord.de

4.2. Finanzen

Die Personal- und Sachkosten der KDSA 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.

Die für das Kalenderjahr 2022 zur Verfügung stehenden Haushaltsmittel standen bei Abschluss dieses Jahresberichts noch nicht zur Verfügung.

4.3. Vertretung in Konferenzen und Arbeitsgruppen

Der Leiter der KDSA Nord ist persönlich in einer Reihe von ständigen oder temporären Konferenzen oder Arbeitsgruppen vertreten.

- Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche
- IT-Tagung für die Leiter der IT-Abteilungen der (Erz-)Diözesen und des Bischöflich Münsterschen Offizialats in Vechta und die Datenschutzreferenten
- Regelmäßige virtuelle Treffen mit den betrieblichen Datenschutzbeauftragten
- Konferenz der Diözesanjuristen der norddeutschen (Erz-)Diözesen und des Bischöflich Münsterschen Offizialats in Vechta

4.4. Vernetzung

Schon bestehende Kontakte zu unterschiedlichen Stellen und Einrichtungen der Länder und Kirchen sind im Berichtszeitraum weiter gepflegt und ausgebaut worden. Darüber hinaus besteht ein guter Kontakt zu den Beauftragten für den Datenschutz in der evangelischen Kirche Deutschlands sowie zum Datenschutzbeauftragte für Kirche und Diakonie in der evangelischen Kirche, nicht zuletzt durch den mittlerweile schon traditionellen „Ökumenischen Datenschutztag“ und zu anderen kirchlichen Datenschutzbeauftragten oder Datenschutzreferenten.

5. Schlussbemerkung

Es ist auf ganz unterschiedlichen gesellschaftlichen und kirchlichen Ebenen immer wieder wahrzunehmen, dass der Datenschutz an sich zwar irgendwie im Bewusstsein der Beteiligten angekommen ist, aber zunehmend als eher lästig und zukunfts-

behindernd eingeschätzt wird. Unter dem Motto „wen interessieren schon meine Daten“ und „das machen doch alle“ wird gerade im Bereich der Kommunikation und dem Umgang mit dem Internet zunehmend leichtfertig mit der Verarbeitung eigener und fremder personenbezogener Daten agiert. Deshalb sei am Ende meiner Dienstzeit noch einmal die Bemerkung erlaubt, dass auch die normative Kraft des Faktischen im Bereich der grundrechtsrelevanten Rechte keine Rechtfertigung darstellen kann, den erforderlichen Schutz zu relativieren. Es ist und bleibt die Aufgabe der Datenschutzaufsicht, sich für die Rechte und den Schutz der Menschen im Hinblick auf deren personenbezogen Daten einzusetzen. Ich bin dankbar dafür, dass die großen Kirchen auch zukünftig ihren Teil zuverlässig dazu beitragen.

Bremen, im Dezember 2022

Andreas Mündelein

6. Anlagen

6.1. Betriebliche Datenschutzbeauftragte

Liste der betrieblichen Datenschutzbeauftragten auf der Ebene der (Erz-)Bistümer und des Offizialatsbezirks Vechta

Einrichtung	Datenschutzbeauftragte	Anschrift
Bischöfliches Generalvikariat Osnabrück	Herr Thomas Marien datenschutz@bistum-os.de	Hasestraße 40a 49074 Osnabrück
Ehe-/Familien-/Lebens-/Erziehungs-Beratungsstelle	Herr Ludger Lüken l.lueken@bistum-os.de	Domhof 2 49074 Osnabrück
Kirchliche Einrichtungen im Bistum Osnabrück	pco GmbH & Co. KG Herr Philipp Wachhorst datenschutz@bistum-os.de	Hafenstraße 11 49090 Osnabrück
Offizialat Vechta	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Schmidt-Straße 88 28217 Bremen
Kirchliche Einrichtung im Offizialat Vechta	Intersoft consulting services AG Herr Stefan Winkel	Beim Strohause 17 20097 Hamburg
Bischöfliches Generalvikariat Hildesheim	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Kirchliche Einrichtungen im Bistum Hildesheim	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Erzbischöfliches Generalvikariat Hamburg	Itebo GmbH Herr Kim Schoen dsb@itebo.de	Dielinger Straße 40 49074 Osnabrück
Kirchliche Einrichtungen im Erzbistum Hamburg	datenschutz nord GmbH Herr Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen

6.2. Auszug Querschnittsprüfung Caritas (Fragestellungen)

Es folgt der Fragenkatalog der Querschnittsprüfung Caritas strukturiert nach abgefragten Themenbereichen. Ergänzt wurden die Fragen um Hinweise zu den in den Antworten zu beschreibenden Details.

Datengeheimnis

1. Mitarbeiterschulung

   Bitte beschreiben Sie das Vorgehen zur Schulung von Mitarbeitern nach § 2 KDG-DVO.
   Hinweis: Erwartet werden Angaben zu Häufigkeit/Zeitpunkt, Form, Inhalt und Nachweisbarkeit der Schulung. Dies sowohl bezogen auf Bestandsmitarbeiter als auch auf Neueinstellungen.

Rechte der betroffenen Person und Informationspflichten des Verantwortlichen

2. Auskunftsersuchen

   Bitte beschreiben Sie das Verfahren für die Behandlung von Auskunftsersuchen betroffener Personen nach § 17 KDG.
   Hinweis: Es werden Angaben zu dem Ablauf, Zuständigkeiten, Inhalt der Dokumentation, Fristen und Wahrung der Vertraulichkeit erwartet.

3. Informationspflichten Bewerbungsverfahren

   Wie teilen Sie Bewerbern die Informationen nach § 15 KDG im Rahmen eines Bewerbungsverfahren mit?
   Hinweis: Bitte geben Sie kurz Auskunft jeweils bezogen auf die verschiedenen Möglichkeiten der Einreichung von Bewerbungen (Post, E-Mail, Jobbörse, andere).

Verantwortlicher und Auftragsverarbeiter

4. Verzeichnis von Verarbeitungstätigkeiten

   Wie stellen Sie die Aktualität des Verzeichnisses von Verarbeitungstätigkeiten gem. § 31 KDG sicher?
   Hinweis: Es werden auch Angaben dazu erwarten, welche Stelle für die Einhaltung der Aktualität zuständig ist.

5. Datenschutzverletzungen

   Bitte beschreiben Sie den Umgang mit Datenschutzverletzungen nach § 33 KDG.
   Hinweis: Es werden Angaben zu Abläufen, Zuständigkeiten, ggf. Einbindung von Externen, Inhalt der Dokumentation, Fristen und Meldung an die Datenschutzaufsicht erwartet.

Technische und Organisatorische Maßnahmen (TOM)

6. Berechtigungskonzept

   Wie stellen Sie sicher, dass Mitarbeiter nur die erforderlichen Berechtigungen erhalten und ausgeschiedenen Mitarbeitern die gewährten Berechtigungen entzogen werden?
   Hinweis: Erwartet werden Angaben zu Ablauf und Kriterien der Berechtigungsvergabe/-änderung, Zuständigkeiten, Dokumentation, Überprüfung vergebener Berechtigungen sowie deren Häufigkeit.

7. Löschkonzept

   Welche Regeln und Verfahren nutzen Sie, um personenbezogene Daten zu löschen bzw. zu vernichten?
   Hinweis: Erwartet werden Angaben sowohl zu den vorhandenen Löschfristen als auch zu den eingesetzten Methoden des Löschens bzw. des Vernichtens von personenbezogenen Daten.

8. Patchmanagment

   Wie stellen Sie die Aktualität der eingesetzten Systeme und Anwendungen sicher?
   Hinweis: Erwartet werden Angaben zum Umfang der betrachteten Systeme (Betriebssysteme, Anwendungen, Firmware der Infrastrukturkomponenten), Zuständigkeiten, Häufigkeiten und Dokumentation.