Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg,
der Bistümer Hildesheim, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.

6. Jahresbericht 2019

Herausgegeben vom

Diözesandatenschutzbeauftragten
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@datenschutz-katholisch-nord.de

Diesen Tätigkeitsbericht können Sie auch auf unserer Internetseite abrufen unter:
https://www.datenschutz-kirche.de/

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

6. Jahresbericht

des Diözesandatenschutzbeauftragten
des Erzbistums Hamburg,
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

für das Jahr 2019

vorgelegt im Juli 2020

Stand 31.12.2019

Inhaltsverzeichnis

Vorwort

Seit Mai 2018 hat sich die datenschutzrechtliche Landschaft in Europa nachhaltig verändert. Mit der Verabschiedung der Datenschutz-Grundverordnung (DS-GVO) und deren Inkrafttreten im Frühjahr 2018 gibt es in Europa ein unmittelbar geltendes Datenschutzrecht, und in der Folge ein entsprechendes Datenschutzrecht (KDG) für die katholische Kirche in Deutschland.

Die mit der Einführung des kirchlichen Datenschutzrechts in 2018 zunächst verbundenen Verunsicherungen, der Medienrummel und die gesamtkirchlichen Irritationen haben sich im Laufe des Berichtszeitraums 2019 nicht weiter fortgesetzt. Die Beratungsnachfragen sind im Laufe des Jahres nicht wesentlich angestiegen, sondern stagnieren auf einem hohen Niveau. Dabei war eine Zunahme der Beschwerde- und Meldevorgänge gegenüber einer Fortbildungs- und Beratungsnachfrage festzustellen. Unabhängig davon ist die Beratungsnotwendigkeit für die kirchlichen Einrichtungen nach wie vor erkennbar vorhanden.

Die Ergebnisse der anlasslosen Prüfungen in Kindertagesstätten, Kirchengemeinden, Schulen, caritativen Einrichtungen oder Krankenhäusern lassen den Schluss zu, dass das Verständnis und das Bewusstsein für den Datenschutz nicht nur rudimentär vorhanden sind. Das Bemühen der Einrichtungen, die erforderlichen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten zu etablieren, war stets wahrnehmbar und im Ergebnis letztlich positiv festzustellen.

Wenn zudem das Verständnis der Vertreter der Einrichtungen weiter dahingehend verändert wird, dass es nicht um den Schutz der Einrichtung oder Institution geht, sondern um den Schutz des Grundrechts auf informationelle Selbstbestimmung der betroffenen Menschen, und sich diese Erkenntnis festsetzt, ist ein weiterer großer Schritt in die richtige Richtung getan.

Dieses Verständnis könnte auch im Hinblick auf den Umgang mit sozialen Medien im Bereich der Kirche und der caritativen Einrichtungen durch die Verantwortlichen hilfreich sein. Die ohne Zweifel notwendige Öffentlichkeitsarbeit der kirchlichen Einrichtungen unter Hintanstellung der datenschutzrechtlichen Belange der Betroffenen zu etablieren, etwa beim Betreiben von Facebook Fanpages als an-

geblich notwendiges modernes und jugendkompatibles Medium, vernachlässigt bisweilen die Verantwortung der Kirche für die datenschutzrechtlichen Grundrechte der ihr anvertrauten Menschen. Dass Facebook die bei der Nutzung anfallenden (Meta-)Daten möglicherweise zur Erstellung bzw. Anreicherung von Persönlichkeitsprofilen nutzt, in jedem Fall aber über die Erhebung und Nutzung dieser Daten keine rechtskonforme Auskunft erteilt wird, darf den Verantwortlichen nicht egal sein. Ebenso wenig kann es kein Argument sein aus Gründen der „Erreichbarkeit“ mit Messengerdiensten zu kommunizieren, deren datenschutzrechtliche Zulässigkeit schon aus Gründen der unerlaubten Weiterleitung von personenbezogenen Daten an transatlantische Unternehmen zu beanstanden ist. Nicht alles was geht ist auch erlaubt, geschweige denn – und insbesondere von der Kirche – zu verantworten.

In diesem Zusammenhang ist zu berichten, dass die im KDG vorgesehenen Instrumentarien zur Sanktionierung datenschutzrechtlich relevanter Vorkommnisse – bis hin zu der Verhängung von Geldbußen gegenüber der verantwortlichen Stelle – mittlerweile zur ständigen Praxis der kirchlichen Datenschutzaufsicht geworden sind. Dies folgt daraus, dass sich neben der Hilfe und Beratung für die Einrichtungen der Fokus der Datenschutzaufsicht für die norddeutschen Diözesen stärker als zu Beginn der neuen datenschutzrechtlichen Situation in 2018 auf die tatsächliche Umsetzung des Datenschutzes in den kirchlichen Einrichtungen gerichtet hat.

Die Aufgaben der Datenschutzaufsicht sind gesetzlich in § 44 KDG geregelt und entsprechen damit den Bestimmungen aus Kapitel VI DS-GVO. Die für die Bereitstellung einer gemeinsamen Datenschutzaufsicht für den norddeutschen Bereich zuständigen Institutionen sind gehalten, die Datenschutzaufsicht mit den dafür erforderlichen Ressourcen auszustatten.

Die Datenschutzaufsicht für die norddeutschen Diözesen ist zuständig für die Gebiete des Erzbistums Hamburg, die der Bistümer Osnabrück und Hildesheim und das des Offizialatsbezirks Vechta in Oldenburg. Die Leitung der Datenschutzaufsicht obliegt dem Diözesandatenschutzbeauftragten.

Auch im vierten Jahr komme ich gerne der mir durch die (Erz-)Bischöfe von Hamburg, Osnabrück und Hildesheim und dem Leiter des Bischöflich Münster-

schen Offizialats in Vechta übertragenen Aufgaben nach. Für das Vertrauen und die Unterstützung durch die Herren Generalvikare und die Mitarbeiter in den kirchlichen Behörden und Dienststellen bin ich dankbar.

Meinen Tätigkeitsbericht für das Jahr 2019 lege ich nachstehend vor. Wie üblich werde ich 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 in meinem Tätigkeitsbereich sein können.

Bremen, im Juli 2020

Andreas Mündelein
Diözesandatenschutzbeauftragter

1 Die Entwicklung des Datenschutzrechts

1.1 Europarecht

1.1.1 Die Europäische Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO ersetzte die aus dem Jahr 1995 stammende EU-Datenschutzrichtlinie und war am 25. Mai 2018 nach einer Übergangsphase von zwei Jahren wirksam geworden. Auch im aktuellen Berichtzeitraum war sie das allgegenwärtige und prägende Element des Datenschutzrechts.

Die DS-GVO soll regelmäßig bewertet und überprüft werden. Die erste Evaluation erfolgt im Mai 2020 (vgl. Art. 97 Abs.1 DS-GVO). Danach soll alle vier Jahre eine weitere Evaluation stattfinden.

Im Rahmen des Prozesses legt die EU-Kommission dem Europaparlament und dem Europäischen Rat einen Bericht vor, der auch veröffentlicht wird. Falls es notwendig ist, wird die Kommission auf dieser Basis Vorschläge zur Änderung der Verordnung vorlegen. Im Vorfeld findet in Brüssel ein regelmäßiger Austausch zwischen der EU-Kommission und den Mitgliedstaaten statt.

Die Evaluation hat eine hohe Relevanz für die katholische Kirche, auch wenn sie nicht unmittelbar für diesen Bereich Wirkung entfalten kann. Über Art. 91 DS-GVO setzt die Garantie für die Kirchen, ihre eigenen Datenschutzregeln auch weiterhin anwenden zu können nach allgemeiner Meinung voraus, dass das Gesetz über den Kirchlichen Datenschutz (KDG) der DS-GVO in allen wesentlichen Punkten gleichwertig ist. Nicht erforderlich ist eine gleichartige Regelung, wohl aber eine, die den Grundsätzen der Verordnung unter den besonderen Umständen der kirchlichen Datenverarbeitung entspricht.

1.1.2 EU-U.S. Privacy Shield

Als Ersatz für das vom Europäischen Gerichtshof aufgehobene „Safe Harbor Abkommen“ hat die EU mit den USA einen Vertrag zum Datenaustausch zwischen den Einrichtungen und Firmen beider Handelszonen ausgehandelt, welches als „EU-U.S. Privacy Shield“ bezeichnet wird.

Dabei wurde vereinbart, dass dieser Datenschutzschild jährlich überprüft wird, damit sichergestellt werden kann, dass das Schutzniveau für die personenbezogenen Daten auch weiterhin angemessen ist. Aus dem Bericht über die dritte jährliche Überprüfung der Funktionsweise des Privacy Shields der Europäischen Kommission im Oktober 2019 geht hervor, dass die Vereinigten Staaten nach wie vor ein angemessenes Schutzniveau für die personenbezogenen Daten gewährleisten, die aus der EU im Rahmen des Privacy Shields an teilnehmende Unternehmen in den USA übermittelt werden.

1.1.3 Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

Eigentlich sollte gleichzeitig mit der DS-GVO eine Verordnung über elektronische Kommunikation (ePrivacy-Verordnung) in Kraft treten. In der Verordnung sollten Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste mit der Absicht geregelt werden, gleiche Wettbewerbsbedingungen für alle Marktteilnehmer zu gewährleisten. Nach erheblichen Verzögerungen im Rahmen des Gesetzgebungsverfahrens wurde der Abschluss nach der Europawahl 2019 prognostiziert.

Anschließend wurde bekannt, dass es die ePrivacy-Verordnung in ihrer derzeitigen Entwurfsfassung wohl nicht geben wird, nachdem die Mitgliedstaaten sich nicht auf einen Entwurf einigen konnten. Nach den Vorstellungen des zuständigen EU-Kommissars Thierry Breton im Dezember 2019 soll nunmehr ein neuer Entwurf vorgelegt werden. Dieser müsste dann zunächst wieder im EU-Parlament diskutiert werden. Wann mit einem neuen Vorschlag gerechnet werden kann ist unklar.

1.2 Bundesrecht

1.2.1 BDSG

Der Deutsche Bundestag hatte im April 2017 das Bundesdatenschutzgesetz (BDSG-neu) als Artikel 1 des DSAnpUG-EU (vollständiger Name: „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680“) beschlossen. Das neue Bundesdatenschutzgesetz ist zusammen mit der DS-GVO in Kraft getreten.

Für die kirchliche Datenschutzaufsicht ist insbesondere die Regelung in § 18 BDSG (neu) von großer Bedeutung. Zu dem dort vorgesehenen Kohärenzverfahren heißt es in § 18 Abs. 1 S. 4 BDSG (neu), dass die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Datenschutzaufsichten von den Aufsichtsbehörden des Bundes und der Länder zu beteiligen sind, wenn diese von der Angelegenheit betroffen sind, mit dem Ziel einer einheitlichen Anwendung der DS-GVO.

Die Pflicht zur Beteiligung der kirchlichen Datenschutzaufsichten ist auf der Bundesebene nicht unumstritten. Unabhängig davon hat sich mittlerweile ein Beteiligungsverfahren entwickelt, bei dem die Kirchen wahrgenommen werden und sich gegebenenfalls selber in die Beratungsprozesse einbringen können.

1.2.2 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU bzw. 2. DSAnpUG-EU)

Wie berichtet hat der Bundestag im Oktober 2018 den Gesetzentwurf der Bundesregierung (BT-Drucksache 19/4674) nach erster Lesung zur federführenden Beratung an den Innenausschuss überwiesen. Nach der 2017 beschlossenen Novellierung des BDSG sollte auch das bereichsspezifische Datenschutzrecht des Bundes an die DS-GVO angepasst werden. Der Gesetzentwurf sah in 154 Fachgesetzen fast aller Ressorts Änderungen vor.

Nach Abschluss der Verfahren ist das Gesetz am 26. November 2019 in Kraft getreten. Neben dem Bundesdatenschutzgesetz 2018 nimmt das sog. Omnibusgesetz Änderungen oder Anpassungen an 154 Gesetzen vor. Hierzu gehört u. a. auch die Anhebung des Schwellenwertes zur verpflichtenden Benennung der betrieblichen Datenschutzbeauftragten. In § 38 Abs. 1 Satz 1 BDSG wird das Wort „zehn“ durch das Wort „zwanzig“ ersetzt, sodass die Schwelle für die Bestellpflicht eines Datenschutzbeauftragten erhöht wurde.

1.3 Datenschutzrecht der Kirche

1.3.1 Das kirchliche Datenschutzgesetz (KDG)

Im Mai 2018 war das Gesetz über den Kirchlichen Datenschutz (KDG) durch die jeweilige gleichlautende Veröffentlichung in den deutschen Diözesen in Kraft getreten. Das Gesetz ist die Grundlage für den Datenschutz im Bereich der katholischen Kirche in Deutschland.

Art. 91 DS-GVO garantiert den Kirchen, eigene Datenschutzregeln nach Inkrafttreten der Verordnung auch weiterhin anwenden zu können, unter der Voraussetzung, dass „zum Zeitpunkt des Inkrafttretens der Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung durch die Kirchen angewendet werden.“ Dieser Vorgabe ist die katholische Kirche in Form des KDG nachgekommen.

Ebenso wie die DS-GVO soll auch das KDG bewertet und überprüft werden. Soweit sich Änderungsnotwendigkeiten im Rahmen der praktischen Anwendung des Gesetzes ergeben, sind diese in dem durch § 58 Abs. 2 KDG geforderten Evaluationsprozess bis zum Mai 2021 zu klären. Dabei wird sich jede Änderung an der europäischen Verordnung orientieren müssen, damit der Einklang mit dieser Regelung und damit die Grundlage für einen eigenen kirchlichen Datenschutz nicht in Frage gestellt wird. Insoweit wird es nicht zu einer grundsätzlichen Veränderung des kirchlichen Datenschutzgesetzes kommen können. Es besteht überdies aber auch keine Notwendigkeit, weil nach diesseitiger Auffassung durch das KDG ein gutes, praktikables und dem europäischen Standard entsprechendes Gesetz vorliegt.

1.3.2 Kirchliche Datenschutzgerichtsordnung (KDSGO)

Mit der im Mai 2018 durch die Veröffentlichung in den Amtsblättern der Diözesen in Deutschland in Kraft gesetzten KDSGO wurde ein zwei Instanzen umfassendes kirchliches Datenschutzgericht etabliert.

Die Gerichte entscheiden in Rechtsstreitigkeiten auf dem Gebiet des kirchlichen Datenschutzrechts (Gesetz über den Kirchlichen Datenschutz (KDG) und weitere kirchliche und staatliche Rechtsvorschriften zum Datenschutz).

Damit hat ***„jede natürliche oder juristische Person unbeschadet des Rechts auf Beschwerde bei der Datenschutzaufsicht (§ 48) das Recht auf einen gerichtlichen Rechtsbehelf gegen einen sie betreffenden Bescheid der Datenschutzaufsicht“*** (vgl. § 49 Abs. 1 KDG).

Im Berichtszeitraum war vor dem erstinstanzlichen Gericht ein Verfahren gegen eine Entscheidung der Datenschutzaufsicht für die norddeutschen Diözesen anhängig. Eine Entscheidung des Gerichts wird für das Frühjahr 2020 erwartet.

1.3.3 KDG-DVO

Zum 1. März 2019 ist die am 19. November 2018 durch die Vollversammlung des Verbandes der Diözesen Deutschlands beschlossene Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in Kraft getreten.

Mit der Durchführungsverordnung wird eine KDG-konforme Verarbeitung personenbezogener Daten sichergestellt, die nach der Einführung des neuen Datenschutzrechts noch bestehende Rechtsunsicherheiten beseitigt und die zu ergreifenden technischen und organisatorischen Maßnahmen für die Verarbeitung personenbezogener Daten definiert und konkretisiert.

In der Praxis hat sich die Verordnung wie bereits ihre Vorgängerin, die „Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)“, die die Anforderungen des KDG Vorgängers „Anordnungen über den Kirchlichen Datenschutz (KDO)“ konkretisiert hat, als ein hilfreiches Instrument

zur Bewältigung der mit dem neuen Datenschutzrecht auf Anwenderseite entstehenden Fragestellungen erwiesen. Auch für die Prüfungssituation durch die Datenschutzaufsicht ist die Verordnung maßgeblich und praktikabel.

2 Die Entwicklung des kirchlichen Datenschutzes

2.1 Betriebliche Datenschutzbeauftragte in den Einrichtungen

Die Verpflichtung der Diözesen, Kirchengemeinden, Kirchenstiftungen und der Kirchengemeindeverbände, ebenso wie die Diözesancaritasverbände und ihre Untergliederungen, einen betrieblichen Datenschutzbeauftragten zu bestellen, ergibt sich aus § 36 Abs. 1 KDG. Dasselbe gilt für Fachverbände, kirchliche Körperschaften und Stiftungen, Anstalten, Werke, Einrichtungen und sonstige kirchliche Rechtsträger (Einrichtungen nach § 3 Abs. 1 lit. b) und c) KDG).

Für die Diözesen und das Bischöflich Münstersche Offizialat in Vechta sind betriebliche Datenschutzbeauftragte benannt und gemeldet worden. Gleiches gilt für die Diözesancaritasverbände.

Die Organisation von betrieblichen Datenschutzbeauftragten für kirchliche Einrichtungen in der Fläche ist im Laufe des Berichtszeitraums von den Diözesen und dem Offizialatsbezirk angenommen und weitestgehend umgesetzt worden. Die Einrichtungen werden zum überwiegenden Teil im Auftrag der Diözesen und des Offizialats durch professionelle externe Datenschutzbeauftragte betreut.

In der Zusammenarbeit mit diesen betrieblichen Datenschutzbeauftragten war es unser Anliegen, eine enge Kommunikationsstruktur zu etablieren. Die zu diesem Zweck eingerichteten regelmäßigen Treffen haben zur Erfüllung des Ziels wesentlich beigetragen und die Effektivität der Umsetzung der datenschutzrechtlichen Belange in den Einrichtungen vor Ort wesentlich gesteigert.

2.2 Kirchliche Datenschutzaufsicht

2.2.1 Die Struktur der Datenschutzaufsicht für die norddeutschen Diözesen

Die kirchliche Datenschutzaufsicht hat die in Kapitel VI der DS-GVO niedergelegten Bedingungen zu erfüllen (Art. 91 Abs. 2 DS-GVO (Art. 51-Art. 59 DS-GVO)), und die katholische Kirche hat dies durch die §§ 42 - 46 KDG sichergestellt. Die Verpflichtung der Diözesen umfasst darüber hinaus die Sicherstellung der perso-

nellen, technischen und finanziellen Ressourcen. (vgl. Art. 52 Abs. 4 i.V.m. Art. 91 Abs. 2 DS-GVO). Die Datenschutzaufsicht für die norddeutschen Diözesen ist rechtlich als unabhängige Stelle eigener Art konfiguriert.

Unabhängig davon soll die kirchliche Datenschutzaufsicht der (Erz-)Diözesen Hamburg, Osnabrück, Hildesheim und des Offizialatsbezirk Vechta i. O. neu strukturiert werden, um den kirchlichen Datenschutz dem staatlichen Recht gegenüber noch wirkungsgleicher gewährleisten zu können.

Es ist geplant, die Datenschutzaufsicht für die norddeutschen Diözesen, ebenso wie die Mehrheit der übrigen kirchlichen Datenschutzaufsichten in der Bundesrepublik, in eine rechtlich selbstständige kirchliche Einrichtung in der Rechtsform einer Körperschaft des öffentlichen Rechts zu überführen. Damit wird die Unabhängigkeit des Diözesandatenschutzbeauftragten garantiert und der kirchliche Datenschutz gegenüber dem staatlichen Recht auf gleichem Niveau ausgestaltet.

Die personelle und finanzielle Ausstattung der Datenschutzaufsicht für die norddeutschen Diözesen wird dem gesetzlichen Aufgabenbereich und der neuen Struktur angepasst werden müssen. Das Stellentableau umfasst derzeit 3,5 Vollzeitstellen, einschließlich des Sekretariats.

2.2.2 Statistik und Zahlen

Im Laufe des Berichtszeitraums sind die Anfragen zum neuen kirchlichen Datenschutzgesetz deutlich zurückgegangen. Demgegenüber hat die Zahl der laut der internen Statistik erfassten Vorgänge in Bezug auf Beschwerden um 18,75 % im Vergleich zum Vorjahreszeitraum zugenommen und die der gemeldeten Verletzungen des Schutzes personenbezogener Daten um 73,30 %. Der Bereich der Prüfungen wurde um 90,67 % gesteigert.

Die Mitarbeiter der Datenschutzaufsicht haben im Berichtsjahr an 42 externen und internen Arbeitsgruppen teilgenommen und sind insgesamt 14-mal im Rahmen von Vortragsveranstaltungen aktiv geworden.

2.2.3 Methodik für die Durchführung der Prüfungen

Das Vorgehen und die Abläufe bei anlasslosen Vor-Ort-Prüfungen durch die Datenschutzaufsicht wurden im Jahr 2019 weiter standardisiert. (Prüfungs-) Abläufe und Fristen wurden für verschiedene Einrichtungsarten weitergehend festgeschrieben und vereinheitlicht, auch um eine Vergleichbarkeit von Prüfungen sicherstellen zu können. Dabei wurden über die Weiterentwicklung der Prüfungsunterlagen auf Seiten der Datenschutzaufsicht hinaus Fristen zur Einreichung von Dokumenten ebenso wie sonstige Fristen grundsätzlich definiert und auch Eskalationsstufen festgeschrieben.

Die Verpflichtung für die Einhaltung datenschutzrechtlicher Vorgaben liegt einzig bei dem für die Verarbeitung personenbezogener Daten Verantwortlichen.

Mit § 26 Abs. 1 lit. d) fordert das KDG die Einrichtung „ein[es] Verfahren[s] zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“. In diesem Sinne ist in dem Fall, dass bei einer Prüfung Feststellungen zur Nichteinhaltung datenschutzrechtlicher Vorgaben getroffen werden müssen, ein Maßnahmenplan zu erstellen, mit dem die Missstände behoben werden. Die Maßnahmen können dabei von der sofortigen Abschaltung der Verarbeitungstätigkeit, über die Umgestaltung von Abläufen und Minimierung von Risiken bis ggf. hin zur Auslagerung von Verarbeitungstätigkeiten an einen Dienstleister reichen. Mit Ausnahme der erstgenannten Abschaltung werden alle anderen Maßnahmen nach Möglichkeit in Abstimmung mit den geprüften Einrichtungen entwickelt. Dabei sind zu den einzelnen Maßnahmen Umsetzungsfristen und Verantwortlichkeiten anzugeben.

2.2.4 Entwicklung und Vorbereitung Querschnittsprüfungen

Bsp.: Kindertagesstätten

Im ersten Halbjahr 2019 sind vermehrt Meldungen über Datenverluste, hervorgerufen durch gestohlene Laptops und Datenträger in Kindertagesstätten, eingegangen. Die Sachverhaltsklärungen ergaben, dass die Daten auf den Speichermedien nicht ausreichend geschützt gewesen sind. Daraus ergeben sich nicht

nur Haftungsrisiken für die verantwortlichen Träger der Einrichtungen; es besteht zudem die Gefahr, dass zum Teil sensible Daten über die Kinder und die Eltern in den Einrichtungen in falsche Hände geraten und dass hunderte oder tausende Fotografien der Kinder von den Geräten und Speichermedien auch in das Internet gelangen können.

Im August 2019 wurden die Kindertageseinrichtungen in Trägerschaft der Kirchengemeinden über die (Erz)Bischöflichen Generalvikariate sowie das Bischöflich Münstersche Offizialat in Vechta i. O. über diese Entwicklung informiert und sensibilisiert. Ferner wurde angekündigt, dass der Diözesandatenschutzbeauftragte der norddeutschen Bistümer zum Ende des Jahres eine Querschnittsprüfung zur Überprüfung der Umsetzung der Anforderungen in diesem Bereich beginnen würde.

Anfang Dezember wurden ausgewählte Kindertagesstätten aus dem Zuständigkeitsbereich des Diözesandatenschutzbeauftragten der norddeutschen Bistümer zur Teilnahme an einer Online-Umfrage zur Überprüfung der Umsetzung der Anforderungen an die Datensicherheit aufgefordert. Um eine gewisse Prüftiefe zu erreichen, umfassen die in der Umfrage abgedeckten Themenfelder den betrieblichen Datenschutzbeauftragten, Grundlagen zur Datenverarbeitung und organisatorischer Datenschutz, das Löschen von Daten und Verschlüsselung sowie allgemein die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten.

Die zunächst auf einer Selbstauskunft beruhende Erfassung des Umsetzungsstatus rechtlicher Anforderungen vor Ort musste nicht „am Stück“ bearbeitet werden; eine Unterbrechung und Speicherung bereits ermittelter Ergebnisse war jederzeit möglich.

Die Erfassung des Umsetzungsstandes kann auch die Datenschutzaufsicht dabei unterstützen, die gegenwärtige Lage zu erfassen und Handlungsbedarfe zu erkennen. Ergebnisse werden für das laufende Jahr 2020 erwartet.

Bsp.: Schule

Die Datenschutzerklärungen auf den Homepages der katholischen Schulen in Trägerschaft des Erzbistums Hamburg wurden überprüft und Hilfestellung geleistet, um diese den rechtlichen Erfordernissen anzupassen.

2.2.5 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 (Geschäftsordnung). Der jeweils für ein Jahr gewählte Sprecher der Konferenz nimmt dabei neben den sitzungsorganisatorischen Belangen u. a. auch die Kontaktfunktion zur Konferenz der staatlichen Datenschutzbeauftragten wahr.

Die Konferenz hat folgende Beschlüsse veröffentlicht:

- 19.09.2019
  Möglichkeit der Einwilligung in schlechtere technische und organisatorische Maßnahmen
  https://www.datenschutzkirche.de/sites/default/files/file/NEU/Beschluesse_DDSB/Beschluss_Moeglichkeit_der_Einwilligung_in_schlechtere_TOM_2019_09_19_1.pdf

- 04.07.2019
  Muster zur Videoüberwachung
  https://www.datenschutzkirche.de/sites/default/files/file/NEU/Beschluesse_DDSB/Beschluss_Muster_zur_Videoueberwachung_2019_07_04.pdf

- 04.04.2019
  Umgang mit Bildern von Kindern und Jugendlichen
  https://www.datenschutzkirche.de/sites/default/files/file/NEU/Beschluesse_DDSB/2019_04_04_Beschluss_zum_Umgang_mit_Bildern_von_Kindern_und_Jugendlichen.pdf

- 04.04.2019
  Verträge zur Auftragsverarbeitung mit externen Unternehmen
  https://www.datenschutzkirche.de/sites/default/files/file/NEU/Beschluesse_DDSB/Beschluss_Auftragsverarbeitung_mit_externen_Dienstleistern_Aenderung_2019_04_04.pdf

Die von der Konferenz der Diözesandatenschutzbeauftragten getroffenen Beschlüsse für die einheitliche Anwendung des kirchlichen Datenschutzrechts werden auf den jeweiligen Homepages der kirchlichen Datenschutzaufsichten veröffentlicht. Damit soll eine größtmögliche Transparenz und Allgemeinverbindlichkeit in datenschutzrechtlichen Fragen erreicht werden.

2.2.6 Kirchliches Datenschutz Modell (KDM)

Im Berichtszeitraum wurde von den Datenschutzaufsichten der katholischen und evangelischen Kirche der Entschluss gefasst, das Standard-Datenschutzmodell (SDM)[1] zukünftig bei ihrer Arbeit – insbesondere mit dem Ziel der Vereinheitlichung der Prüfungen von kirchlichen Einrichtungen – zu berücksichtigen. Das Standard-Datenschutzmodell soll dazu von einer Projektgruppe an die kirchlichen Gegebenheiten und für die konkrete Anwendung angepasst werden. Ein Mitarbeiter aus dem Büro der Datenschutzaufsicht für die norddeutschen Bistümer ist Teil dieser Projektgruppe.

[1] https://www.datenschutzzentrum.de/sdm/

3 Exemplarische Darstellung von Einzelfragen und Einzelfällen

3.1 Beratungen

3.1.1 Ist WhatsApp auf dienstlichen Handys zulässig, wenn eine MDM-Software eingesetzt wird?

An die Datenschutzaufsicht ist die Anfrage herangetragen worden, ob die Nutzung von WhatsApp auf dienstlichen Smartphones zulässig ist, wenn auf diesem Gerät eine MDM-Software eingesetzt wird.

Aufgrund des Umgangs der WhatsApp-Anwendung mit Kontaktdaten ist im üblichen Setting, bei der der App Zugriff auf die auf dem Smartphone hinterlegten Kontaktdaten gewährt werden, mindestens das Kriterium der Respektierung der Rechte Dritter (siehe Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands, Beurteilung von Messenger- und anderen Social Media-Diensten (26.07.2018, FfM)[2]) nicht erfüllt.

Somit ist die Nutzung von WhatsApp auf dienstlichen Smartphones, auch mit einer MDM-Software, aus datenschutzrechtlicher Sicht nicht zulässig.

3.1.2 Sind die Grundsätze der Nutzung privater IT-Systeme zu dienstlichen Zwecken gemäß § 20 Abs. 2 KDG-DVO auch auf die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken gemäß § 19 KDG-DVO anwendbar?

Uns wurde die Frage gestellt, ob die rechtlichen Vorgaben zum Einsatz von privaten Geräten für den dienstlichen Gebrauch nach § 20 Abs. 2 KDG-DVO auch auf die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken nach § 19 KDG-DVO anwendbar sind.

Zunächst ist anzumerken, dass sowohl die private Nutzung dienstlicher IT-Systeme als auch die Nutzung privater IT-Systeme zu dienstlichen Zwecken grundsätzlich unzulässig und nur im Ausnahmefall vom Verantwortlichen unter

[2] https://www.datenschutz-kirche.de/sites/default/files/file/NEU/Beschluesse_DDSB/2018_07_26_Beurteilung_von_Messengern_und_anderen_Social_Media_Diensten.pdf

Berücksichtigung und unter Beachtung der jeweils geltenden gesetzlichen Regelungen geregelt werden kann.

Dabei sind alle personenbezogenen Daten insbesondere gemäß dem Grundsatz nach § 7 Abs. 1 lit. f) KDG auf eine Weise zu verarbeiten, welche durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

Für den Einsatz von privaten Geräten zu auch dienstlichen Zwecken ist in § 20 Abs. 2 KDG-DVO die Frage nach den geeigneten technischen und organisatorischen Maßnahmen durch die genannten Vorgaben, die unabhängig vom konkreten Einsatzszenario formuliert sind – zumindest im Hinblick auf die mindestens zu treffenden Maßnahmen – bereits beantwortet. Sollten aus Sicht des Verantwortlichen im Sinne des § 26 Abs. 1 KDG weitere Maßnahmen erforderlich sein, so sind diese ebenso umzusetzen. Gleichwohl können die in § 20 Abs. 2 KDG-DVO beschriebenen Mindestmaßnahmen in jedem Fall als sinnvolle Vorschläge für die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken (gemäß § 19 KDG-DVO) aufgefasst werden, ihr Einsatz ist jedoch nicht bindend und sollte auf das Einsatzszenario und in Abhängigkeit vom Schutzbedarf der auf den dienstlichen Geräten verarbeiteten personenbezogenen Daten ausgelegt werden.

3.1.3 Microsoft Office 365

Der datenschutzkonforme Einsatz von Microsoft Office 365 war ebenfalls Gegenstand mehrerer Anfragen, die die Datenschutzaufsicht erreichten.

Der Einsatz von Microsoft Office 365 erfordert hinsichtlich verschiedener Themen eine genaue Betrachtung durch den Verantwortlichen. Exemplarisch genannt seien hier der CLOUD Act, der die Gefahr der unberechtigten Einsichtnahme durch US-Behörden birgt, die Möglichkeit des Wegfallens des EU-U.S. Privacy-Shields als Rechtsgrundlage und grundsätzlich die Möglichkeit der Einsichtnahme durch den Dienstleister. Hier sind die bestehenden Gefährdungen insbesondere in Anbetracht der Sensibilität der verarbeiteten personenbezogenen Daten zu bewerten. Gesondert zu betrachten sind auch die während der Nutzung anfal-

lenden Telemetriedaten. Eine weitere Bedingung für einen rechtskonformen Betrieb ist ferner der Abschluss eines Vertrags zur Auftragsverarbeitung gemäß den Anforderungen aus § 29 KDG.

Auch auf nationaler sowie auf europäischer Ebene war dieses Thema Gegenstand verschiedener Initiativen und Aktivitäten: So hat bspw. der IT-Planungsrat auf seiner Sitzung vom 27. Juni 2019 entschieden, eine länderoffene Arbeitsgruppe mit dem Thema „Daten und Anwendungen der öffentlichen Verwaltung im Cloud-Betrieb“ einzurichten. Diese soll laut Arbeitsauftrag Empfehlungen zu Anforderungen an Softwarehersteller für den Betrieb von Anwendungen in der Cloud und für das weitere Vorgehen hinsichtlich des Umgangs mit entsprechenden Softwareanbietern vorlegen. Der Zwischenbericht sollte im März 2020 vorgelegt werden[3].

Ferner hat das niederländische Ministerie van Justitie en Veiligheid die Ergebnisse einer Datenschutzfolgenabschätzung für Microsoft Office 365 Pro Plus Spring 2019[4] veröffentlicht. Auf europäischer Ebene wurden zudem durch den European Data Protection Supervisor (EDPS) im April 2019 Untersuchungen begonnen, ob die vertraglichen Verhältnisse, die zwischen den EU-Einrichtungen und Microsoft bezgl. der von den EU-Einrichtungen eingesetzten Software geschlossen worden sind, den (datenschutz-) rechtlichen Anforderungen genügen[5]. Weitere Initiativen sind auf dieser Ebene angelaufen, z.B. das „The Hague Forum“[6].

3.2 Datenpannen

3.2.1 Die rechtswidrige Verarbeitung von personenbezogenen Daten in Form von Kinderbildern durch die Aufnahme und die anschließende Veröffentlichung auf dem Onlinedienst Instagram

Ein Praktikant in einer Kindertagesstätte hatte während seiner Arbeitszeit rechtswidrig zwei kurze Sequenzen von spielenden Kindern mittels seines priva-

[3] https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=20
[4] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Office+365+ProPlus+spring+2019+22+July+2019+public+version.pdf
[5] https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-contractual-agreements_en
[6] https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en

ten Handys aufgezeichnet und anschließend auf dem Onlinedienst Instagram hochgeladen, auf denen Kinder der Einrichtung beim Spielen zu erkennen waren. Die Leitung der Kindertagesstätte wurde über den Vorfall durch die Schulleitung der Fachschule (FOS) informiert.

Im Nachgang sind die betroffenen Eltern der abgebildeten Kinder informiert worden und die Handyaufnahmen sind sowohl auf der Instagram-Plattform, als auch auf dem Handy des Praktikanten gelöscht worden.

Durch die nichtgerechtfertigte Aufnahme der Kindergartenkinder und die Anschließende Veröffentlichung auf dem Onlinedienst Instagram lag ein Verstoß gegen § 6 KDG vor, der gem. § 47 Abs. 1 KDG zu beanstanden war.

3.2.2 Das Unterlassen der Meldung der Datenschutzverletzung innerhalb der gesetzlich vorgeschriebenen Frist von 72 Stunden ab Kenntnis der Verletzung

Grundsätzlich hat der Verantwortliche bei der Verletzung des Schutzes personenbezogener Daten die Datenschutzaufsicht unverzüglich von der Verletzung zu unterrichten, wenn die Verletzung voraussichtlich ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (vgl. § 34 Abs. 1 KDG).

Eine Verletzung im Sinne des anzuwendenden Datenschutzrechtes liegt vor, wenn eine Verletzung der Sicherheit, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von personenbezogenen Daten führt (vgl. § 4 Nr. 14 KDG).

Letzteres war der Fall, weil es dem oder der Täter(in) offensichtlich gelungen war, sich durch die Wegnahme einer ungesicherten Kamera in den Besitz von Kinderbildern einer Geburtstagsfeier in einer Kindergartengruppe zu bringen.

Weil nicht ausgeschlossen werden konnte, dass dem oder den Tätern der Zugriff auf in der Kamera gespeicherten Aufnahmen möglich war und zudem nicht ausgeschlossen werden konnte, dass diese Daten zweckentfremdet verwertet werden konnten, ist schon aus Schutzgründen von einem hohen Risiko für die Be-

troffenen auszugeben. Gerade bei Kinderbildern ist im Rahmen der Risikoabwägung in der Regel von einem gesteigerten Schutzbedürfnis zu Gunsten der Kinder auszugehen. Daraus folgt eine Informationspflicht durch den Verantwortlichen. Entsprechend den Ausführungen im Rahmen der Meldung ist letztlich richtigerweise eine Information an die Eltern erfolgt.

Eine tragfähige Begründung, weshalb die gesetzliche Meldefrist von 72 Stunden nicht eingehalten worden ist, war der Meldung der Datenschutzverletzung nicht zu entnehmen.

Auch in Kenntnis dessen, dass die Kirchengemeinde nicht nur mit dem Datenschutz, sondern auch und richtigerweise mit einer Vielzahl anderer Projekte und Aufgaben befasst ist, hätte eine Meldekette an den Leiter der Kirchengemeinde etabliert sein können und müssen.

Die insoweit unentschuldigte Nichteinhaltung der gesetzlichen Meldefrist hat dazu geführt, dass die Datenschutzaufsicht der norddeutschen Diözesen eine Beanstandung auszusprechen hatte.

3.2.3 Die unverschlüsselte Übermittlung von personenbezogenen Daten per E-Mail

Mit der Meldung wurde mitgeteilt, dass eine Excel-Tabelle per unverschlüsselter E-Mail über Outlook an die Abrechnungsstelle eines Bistums übermittelt worden war. Die Liste enthielt neben den Vor- und Nachnamen der betroffenen Personen weitere für die Lohnabrechnung relevante Angaben (Personalnummer, Lohnartencodes und über diese mittelbar die Anzahl von Krankheits- und Urlaubstagen). Nicht enthalten waren besondere Kategorien personenbezogener Daten wie etwa Gesundheitsdaten. Allein die Tatsache, dass die in der Liste enthaltenen Lohnartencodes einen mittelbaren Bezug zu Krankheitstagen aufweisen, führt nicht dazu, dass es sich auch um Gesundheitsdaten handelt. Diagnosen oder der Ausstellende einer AU-Meldung waren ebenfalls nicht erkennbar.

Grundsätzlich sind personenbezogene Daten nach § 26 Abs. 1 S. 2 lit. a) KDG zu verschlüsseln. Dies gilt insbesondere dann, wenn die personenbezogenen Daten per E-Mail verschickt werden sollen.

Dies ergibt sich auch aus der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO). Nach § 25 Abs. 1 KDG-DVO dürfen „E-Mails, die personenbezogene Daten der Datenschutzklasse II oder III enthalten, […] ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden."

Als bereits ergriffene Maßnahme war mitgeteilt worden, dass zukünftig ein Programm genutzt wird, um einen geschützten Versand von abrechnungsrelevanten Daten zu gewährleisten.

3.2.4 Unbefugte Offenlegung von Gesundheitsdaten

Gemeldet wurde, dass in einem Kuvert neben dem Arztbrief des Patienten auch zwei DVDs mit Patientendokumentationen von zwei weiteren Patienten enthalten waren. Bei den zwei DVDs handelt es sich um Bildaufnahmen ohne Befund- oder Diagnosedaten. Die Bildaufnahmen enthielten die Identifikationsdaten der Patienten (Name, Vorname, Geburtsdatum). Die Bilddaten befanden sich im Dicom-Format auf der DVD und konnten durch die auf der DVD auch vorhandene Leseanwendung zumindest betrachtet werden.

Gemäß § 51 Abs. 1 i.V.m. § 47 Abs. 6 KDG kann die zuständige Datenschutzaufsicht eine Geldbuße verhängen, wenn ein Verantwortlicher oder ein Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen des KDG verstößt. Der Verantwortliche hat vorliegend gegen Grundsätze der Verarbeitung personenbezogener Daten und gegen die Einhaltung der dazu erforderlichen organisatorischen Maßnahmen verstoßen, § 7 Abs. 1 lit. f), § 26 Abs. 1 S. 2 lit. b) KDG. Bei den auf den DVDs gespeicherten Daten handelte es sich um besondere Kategorien personenbezogener Daten nach § 4 Nr. 2 KDG. Insbesondere Gesundheitsdaten sind vor einer unbefugten Offenlegung durch geeignete technische und organisatorische Maßnahmen zu schützen.

Die unbefugte Offenlegung von Gesundheitsdaten stellte einen Verstoß gegen § 7 Abs. 1 lit. f) KDG sowie gegen § 26 Abs. 1 S. 2 lit. b) KDG dar. Hiernach

müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter Verarbeitung. Eine unbefugte Verarbeitung von personenbezogenen Daten liegt u.a. auch dann vor, wenn diese einer Person offengelegt werden, die zur Einsichtnahme nicht berechtigt war.

Aufgrund des fehlerhaften Versands und der damit verbundenen Offenlegung der besonderen Kategorien personenbezogener Daten war eine Geldbuße zu verhängen.

3.2.5 Die Verpflichtung die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können

Grundsätzlich hat der Verantwortliche die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu schaffen, dass die Risiken für die Verletzung des Schutzes personenbezogener Daten minimiert (vgl. § 26 Abs. 1 KDG). Das beinhaltet u. a. auch die Verpflichtung, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können (vgl. § 26 Abs. 1 lit. c) KDG). Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Insbesondere durch – ob unbeabsichtigte oder unrechtmäßige – Vernichtung der personenbezogenen Daten (vgl. § 26 Abs. 2 KDG).

Die Verarbeitung der personenbezogenen Daten erfolgte über ein der Mitarbeiterin überlassenes Notebook auf externen Speichermedien.

Bei den personenbezogenen Daten handelte es sich um solche, die durch eine Mitarbeiterin im Bereich der Beratung von Migranten verarbeitet worden sind. Es war im Hinblick auf die Datensätze nicht auszuschließen, dass sie erforderlich waren, um existentielle Hilfen und Ansprüche der Betroffenen gegenüber den Gebietskörperschaften geltend machen zu können. Dies folgte im Zweifel aus der Übernahme der Beratungstätigkeit für die Landkreise. Entsprechend hätten die Daten gesichert werden müssen. Nach dem Ausscheiden der Mitarbeiterin wurde

verbindlich bestätigt, dass alle dienstlichen Daten auf dem ihr auch zur privaten Nutzung überlassen Notebook gelöscht worden waren und sich keine dienstlichen Daten mehr in ihrem Besitz befanden. Darüber hinaus wurde bestätigt, dass ein dienstlich mit Duldung durch den Verantwortlichen genutzter USB-Stick fachlich adäquat ebenfalls gelöscht worden war. Daraus folgt, dass neben anderen Daten auch alle für die Beratungstätigkeit relevanten personenbezogenen Daten durch das Löschen vernichtet worden sind.

Unabhängig davon, ob die ehemalige Mitarbeiterin die von ihr verarbeiteten personenbezogenen Daten unrechtmäßig gelöscht hat, ist es unter datenschutzrechtlichen Gesichtspunkten die Obliegenheit des Verantwortlichen, durch geeignete technische und organisatorische Maßnahmen die Verfügbarkeit personenbezogener Daten nach einem physischen Zwischenfall rasch wiederherstellen zu können.

Hierfür waren durch den Verantwortlichen keine erkennbaren Vorkehrungen getroffen worden. Es gab weder eine schriftliche Vereinbarung mit der Mitarbeiterin in Bezug auf die Verwendung des Notebooks (zu auch privaten Zwecken), noch ist die Verwendung von externen Speichergeräten im Hinblick auf dienstliche Daten geregelt worden. Der offenbar vorhandene Netz-Laufwerk-Pfad auf dem Server des Verbands ist nicht genutzt worden, um erforderliche Backups verpflichtend durchzuführen.

Die grundsätzliche Nichtachtung der Verpflichtung, die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können, ist ein Verstoß gegen das kirchliche Datenschutzgesetz.

Es wurde angeordnet, innerhalb einer Frist von 2 Monaten durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Verfügbarkeit personenbezogener Daten, auch bei der Nutzung mobiler Datenendgeräte, nach einem physischen oder technischen Zwischenfall rasch wiederherstellt werden kann. Damit bei der künftigen Verarbeitung personenbezogener Daten, auch mittels mobiler Datenendgeräte, die Anforderungen des § 26 KDG erfüllt werden, war die Anordnung erforderlich.

3.3 Beschwerden

3.3.1 Die Veröffentlichung von Namen und Geburtsdatum des Beschwerdeführers im Kirchlichen Amtsblatt des Erzbistums Hamburg im Rahmen einer Jubiläumsmitteilung

Bei den Vor- und Zunamen sowie dem Alter einer Person handelt es sich um personenbezogene Daten. Mit dem Abdrucken im kirchlichen Amtsblatt bzw. der Veröffentlichung der Information im Internet, lag eine Verarbeitung personenbezogener Daten im Sinne des § 6 KDG vor.

Grundsätzlich ist die Verarbeitung personenbezogener Daten unzulässig, es sei denn, eine kirchliche oder staatliche Rechtsvorschrift erlaubt sie, oder die betroffene Person hat in die Verarbeitung eingewilligt.

Eine Veröffentlichung von Jubiläumsdaten i. S. d. Regelungen des § 50 Abs. 2 Bundesmeldegesetz (BMG) scheidet wegen der mangelnden Meldebehördeneigenschaft des Erzbistums aus.

Eine Verarbeitung nach kirchlichen Rechtsgrundlagen im Rahmen einer Offenlegung gegenüber nicht kirchlichen und nicht öffentlichen Stellen (§ 10 KDG) knüpft die Zulässigkeit der Veröffentlichung an die dort geregelten gesetzlichen Voraussetzungen.

Danach ist die Verarbeitung (Veröffentlichung) personenbezogener Daten gem. § 10 i.V.m. § 6 KDG zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der offenlegenden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen gegeben sind, die eine Verarbeitung nach § 6 KDG zulassen würden.

Es war schon zweifelhaft, ob es sich bei der Bekanntgabe der Jubilare um eine kirchliche Aufgabe handelt, für deren Erfüllung das Veröffentlichen im Amtsblatt und im Internet erforderlich ist. Es mag sicher für den einzelnen Jubilar wichtig sein zu erfahren, dass das Erzbistum Hamburg an seinen Ehrentag denkt, bzw. dass man ihn in der Gemeinschaft seiner Mitpriester und Weihedurchgänge auch anlässlich des Jubiläums wahrnimmt, gleichwohl wird durch das Partikularinteresse noch keine „Aufgabe“ des Erzbistums Hamburg generiert. Eine kirchliche Aufgabe bedarf, ebenso wie eine öffentliche Aufgabe im Sinne der Europäischen

Datenschutz-Grundverordnung (DS-GVO), einer entsprechenden Rechtsgrundlage. Eine insoweit geeignete Rechtsgrundlage ist nach den Mitteilungen des Erzbistums im Rahmen der erbetenen Stellungnahme zu dem Beschwerdevortrag nicht benannt worden.

Unbeschadet dessen wäre auch die Frage der Erforderlichkeit der Veröffentlichung nicht ohne Relevanz, weil das Ziel der Wertschätzung und Wahrnehmung der Jubilare auch auf einem anderen, die Persönlichkeitsrechte nicht beeinträchtigendem Weg, erreicht werden könnte, etwa durch Zusendung einer Glückwunschkarte.

Die Praxis des Erzbistums im Hinblick auf die Veröffentlichung von Jubiläumsdaten fußt auf einer sogenannten Widerspruchslösung, die letztmalig im September 2018 (Kirchlichen Amtsblatt Erzbistum Hamburg, September 2018, Art. 96, S. 141) veröffentlicht worden ist. Dabei wird von einer mutmaßlichen Einwilligung der betroffenen in die Veröffentlichung ihrer personenbezogenen Daten ausgegangen, wenn diese der Verarbeitung nicht ausdrücklich widersprechen.

Diese aus der Zeit der Anordnung über den Kirchlichen Datenschutz (KDO) übernommene Regelung hat vor dem Hintergrund des geltenden KDG keinen Bestand mehr.

Die Einwilligung nach dem KDG zur Verarbeitung von personenbezogenen Daten ist regelmäßig schriftlich zu erteilen und zu dokumentieren, um der Nachweispflicht Genüge zu tun. Sie entspricht einer freiwilligen und für einen bestimmten Fall in informierter Weise und unmissverständlich abgegebenen Willenserklärung, mit der die betreffende Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (§ 4 Nr. 13 KDG). Eine Einwilligung darf keinen pauschalen Charakter tragen. Die Veröffentlichung von personenbezogenen Daten im Amtsblatt des Erzbistums Hamburg entspricht nicht den vorgenannten Anforderungen und ist somit datenschutzrechtlich zu beanstanden.

Es wurde angeordnet, die Veröffentlichungen der Namen und Geburtsdaten der Priester und ständigen Diakone mit dem Gesetz über den Kirchlichen Datenschutz innerhalb einer Frist von drei Monaten durch Schaffung einer Rechts-

grundlage oder durch zukünftige Einwilligung der betroffenen Person in Einklang zu bringen.

3.3.2 Die Offenlegung von personenbezogenen Daten gegenüber einer privaten Abrechnungsstelle für ärztliche Leistungen

Der Beschwerdeführer hatte sich gegen die Weitergabe seiner personenbezogenen Daten an eine private Abrechnungsstelle gewendet. Er hatte eine Rechnung der privaten Abrechnungsstelle über die Abrechnung von Laborleistungen erhalten, die durch seinen behandelnden Arzt bei dem Laborinstitut in Trägerschaft der Beschwerdegegnerin in Auftrag gegeben worden waren. Die Beschwerdegegnerin hatte die Abrechnung des Labormediziners über die private Abrechnungsstelle veranlasst.

Der Beschwerdeführer hatte weder eine Einwilligung für die Inanspruchnahme der privaten Abrechnungsstelle erteilt, noch hatte die Beschwerdegegnerin eine Rechtsgrundlage für die Inanspruchnahme der Verrechnungsstelle dargelegt.

Sie verwies lediglich darauf, dass mit der privaten Abrechnungsstelle ein Auftragsverarbeitungsvertrag vorliegen würde und aus diesem Grund keine Einwilligung zur Weitergabe der personenbezogenen Daten erforderlich sei. Zudem vertrat sie die Auffassung der Sachverhalt sei wie in den Urteilen des BGH vom 14. Januar 2010 zu beurteilen (III ZR173/09 und III ZR 188/09).

Entgegen der Ansicht der Beschwerdegegnerin war es erforderlich, bei der betroffenen Person eine Einwilligung für den Fall einzuholen, dass die Abrechnung der medizinischen Leistung durch eine private Abrechnungsstelle erfolgt. Insoweit war der Beschwerde stattzugeben.

Zwar stellte die Beschwerdegegnerin zutreffend dar, dass der niedergelassene Arzt stellvertretend für den Patienten einen Behandlungsvertrag mit dem Institut für Laboratoriums Medizin in Trägerschaft der Beschwerdegegnerin abgeschlossen habe (so auch der BGH in den von der Beschwerdegegnerin zitierten v.g. Entscheidungen), aber die „Abrechnung“ der medizinischer Leistungen durch eine privaten Abrechnungsstelle ist nach diesseitiger Auffassung nicht vom Behandlungsvertrag mit dem Labor (Träger) umfasst. Diese Auffassung stützt sich

auf eine Entscheidung des BGH (BGH, Urteil vom 10. Oktober 2019, III ZR 325/12), der bei einer Inanspruchnahme einer privaten Abrechnungsstelle eine Einwilligung der betroffenen Person voraussetzt.

3.3.3 Beschwerde gegen eine beabsichtigte Versetzung als betrieblicher Datenschutzbeauftragter

Die Beschwerde richtete sich gegen einen Schulträger als Beschwerdegegnerin. In der Beschwerde wurde vorgetragen, dass eine beabsichtigte Versetzung des Beschwerdeführers (Lehrer) an einen anderen Schulstandort als den bisherigen im unmittelbaren Zusammenhang mit der Tätigkeit des Beschwerdeführers als betrieblichen Datenschutzbeauftragten für die Schulen des Schulträgers stehe. Im Rahmen seiner Aufgabe als betrieblicher Datenschutzbeauftragter habe es mehrfach Diskrepanzen zwischen Leitungsfunktionsträgern und seiner Person gegeben, was nach seiner Auffassung nunmehr zur Versetzung an einen weitabgelegenen Schulstandort geführt habe.

Demgegenüber hat die Beschwerdegegnerin auf Nachfrage vorgetragen, dass die Versetzungsentscheidung in keinem Zusammenhang mit der Wahrnehmung der Aufgabe als betrieblicher Datenschutzbeauftragter stehe, sondern allein der schulorganisatorischen Verantwortung des Schulträgers geschuldet sei.

Im Ergebnis war die Beschwerde zurückzuweisen.

Nach § 37 Abs. 1 S. 2 KDG darf der betriebliche Datenschutzbeauftragte „wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden“. Das Benachteiligungsverbot umfasst jede Form der direkten oder indirekten Benachteiligung. Dazu gehören auch Sanktionen oder Diskriminierung als Reaktion auf Maßnahmen oder Stellungnahmen des Datenschutzbeauftragten in Wahrnehmung seiner Aufgaben (Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DS-GVO Art. 38 Rn. 15).

Aus dem Vortrag des Beschwerdeführers ergeben sich unter Berücksichtigung der Stellungnahme der Beschwerdegegnerin keine Anhaltspunkte dafür, dass die beabsichtigte Versetzung im Zusammenhang mit der Tätigkeit des Beschwerdeführers als betrieblicher Datenschutzbeauftragter steht.

Zutreffend ist, dass die Versetzung den Arbeitsweg deutlich verlängern würde. Jedoch ist der Beschwerdeführer nicht in seiner Tätigkeit als betrieblicher Datenschutzbeauftragter eingeschränkt. Nach wie vor besteht die Möglichkeit des Beschwerdeführers, als Ansprechpartner sämtlicher Schulen des Trägers verfügbar zu sein. Anhaltspunkte dafür, dass die Verfügbarkeit im Vergleich zu bisherigen Situation reduziert werden soll, ergeben sich nicht.

Die Beratung der einzelnen Schulen ist im Fall einer Versetzung an einen anderen Schulstandort ebenfalls nicht beeinträchtigt.

3.4 Prüfungen

3.4.1 Ablauf einer Datenschutzprüfung am Beispiel einer Katholischen Kirchengemeinde

I. Terminabstimmung

II. Anforderung Dokumentation zur datenschutzrechtlichen Prüfung.

Die Einrichtung wird aufgefordert in der Regel bis spätestens 10 Tage vor dem genannten Prüfungstermin nachstehende Unterlagen zur Verfügung zu stellen:

- Verzeichnis der Verarbeitungstätigkeiten (§ 31 KDG)
- Datenschutzkonzept (§ 15 KDG-DVO)
- Datensicherungskonzept (§ 16 KDG-DVO)
- Musterverträge zur Auftragsverarbeitung (§ 29 KDG)
- Ggf. Ausnahmeregelungen z.B. gem. §§ 19, 20 KDG-DVO

III. Prüfung

Gegenstand der anlasslosen Prüfungen sind die datenschutzrechtlich relevanten Abläufe im Zusammenhang mit der Organisation und dem Betrieb einer Katholischen Kirchengemeinde. Das Ergebnis wird der Gemeinde in einem umfangreichen Prüfungsbericht mitgeteilt und gilt für die untersuchten Sachverhalte.

Mit der Möglichkeit zur Stellungnahme zum Bericht hat die Kirchengemeinde einen Maßnahmenplan zur Umsetzung der im Bericht getroffenen Feststellungen zu entwickeln und der Datenschutzaufsicht vorzulegen. Anschließend wird der Maßnahmenplan kommentiert an die Kirchengemeinde mit dem Hinweis auf die Verbindlichkeit des kommentierten Maßnahmenplans zurückgeben, soweit nicht innerhalb einer zweiwöchigen Frist Einwände erhoben werden.

Die nicht erfolgte Einhaltung des Gesetzes über den kirchlichen Datenschutz und anderer Vorschriften über den Datenschutz im Zusammenhang mit der Organisation und dem Betrieb der Kirchengemeinde werden beanstandet. Zudem wird angeordnet, die Feststellungen im Maßnahmenplan innerhalb einer gesetzten Frist umzusetzen. Das zu diesem Zweck im Vorfeld von der Kirchengemeinde entwickelte und mit der Datenschutzaufsicht in Form des kommentierten Maßnahmenplans abgestimmte Verfahren sieht seitens der Kirchengemeinde Fristen vor, bis zu welchem Zeitpunkt die Feststellungen, die laut Maßnahmenplan noch zu bearbeiteten sind, abzuschließen sind. Die Fristsetzung berücksichtigt auch die Leistungsmöglichkeit der Kirchengemeinde.

3.4.2 Exemplarische Feststellungen aus den Prüfberichten

Bei den durchgeführten Prüfungen in den Einrichtungen konnte insgesamt ein positiver Eindruck gewonnen werden. Die Teilnehmer vermittelten eine hohe Akzeptanz im Hinblick auf den kirchlichen Datenschutz. Wenn auch nicht sämtliche Erfordernisse erfüllt waren, konnte sich die Datenschutzaufsicht für die norddeutschen Diözesen gleichwohl davon überzeugen, dass die Bereitschaft zur Umsetzung der gesetzlichen Vorgaben im hohen Maße vorhanden ist. Nachstehend werden einige Feststellungen aus den Prüfungsberichten aufgelistet, die eine hohe Übereinstimmung in den Prüfverfahren zeigen:

- Es sind nicht sämtliche Mitarbeiter auf das Datengeheimnis verpflichtet.

- Eine Schulung der Mitarbeiter nach § 38 S. 2 c) KDG ist bisher noch nicht erfolgt.
- Die Nutzung privater IT-Systeme zu dienstlichen Zwecken ist gem. § 20 KDG-DVO nicht geregelt.
- Es fehlen die notwendigen Informationen im Zusammenhang mit der unmittelbaren Datenerhebung.
- Eine Dokumentation (Richtlinie/Merkblatt) zur Umsetzung der Informationspflichten nach dem KDG bei Datenerhebung liegt nicht vor.
- Ein Verfahren zur Umsetzung von Betroffenenanfragen liegt nicht vor.
- Ein Verfahren, wie mit Datenpannen und den sich daraus ergebenden gesetzlichen Verpflichtungen (§§ 33 ff. KDG) im Tagesablauf der Kirchengemeinde umzugehen ist, ist noch nicht implementiert.
- Es liegen keine Auftragsverarbeitungsverträge nach § 29 KDG vor.
- Es liegt kein Konzept zur Löschung der personenbezogenen Daten vor.
- Es existiert kein Prozess für die Nutzer- und Berechtigungsverwaltung, insbesondere für den Weggang von Personal und den Entzug von Berechtigungen, z. B. in Form von Laufzetteln o.ä.
- Eine passwortgeschützte, sich selbst aktivierende Bildschirmsperre ist nicht eingerichtet.
- Ein Boot-Schutz der Systeme ist nicht eingerichtet. Dieser soll durch ein komplexes Passwort geschützt werden.
- Den Mitarbeitern sollen an zentraler Stelle die Informationen zum Vorgehen beim Versand von personenbezogenen Informationen via E-Mail (Vorgehen zur Verschlüsselung, Passwortversand über 2. Kanal (SMS oder Telefonat), Vorgaben zur Passwortkomplexität etc.) zur Verfügung gestellt werden.
- Die an den Systemen im Rahmen von Administrationsdienstleistungen vorgenommene Änderungen oder durchgeführte Tätigkeiten sind nicht nachvollziehbar.
- Eine nachweislich erfolgte Schulung der Mitarbeiter im Hinblick auf die Gefahren der Nutzung der IT-Systeme gem. § 15 Abs. 3 KDG-DVO ist nicht erfolgt.
- Eine Überprüfung der Dienstleister gemäß § 15 Abs. 5 KDG-DVO ist nicht erfolgt.

- Ein Datensicherungskonzept gemäß § 16 Abs. 1 KDG-DVO existiert nicht. Zu berücksichtigen ist ggf. auch die Datensicherung, die im Rahmen einer Dienstleistung erstellt werden.
- Es ist sicherzustellen, dass nur autorisierte Programme genutzt werden.
- Die Hinterlegung von Passwortlisten der Systemverwaltung ist bisher nicht festgelegt.

3.4.3 Rechtliche Grundlagen der Datenschutzprüfung

Es obliegt der Datenschutzaufsicht über die Einhaltung des Gesetzes über den kirchlichen Datenschutz und anderer Vorschriften über den Datenschutz zu wachen. Hierzu kann die Datenschutzaufsicht Untersuchungen in Form von Datenschutzüberprüfungen vornehmen, die von den kirchlichen Einrichtungen (vgl. § 3 Abs.1 KDG) zuzulassen sind (vgl. § 44 Abs. 1, Abs. 2 lit. c) KDG). Die im Rahmen der Prüfung getroffenen Feststellungen in Form eines Prüfungsberichts dokumentieren die Abweichungen von den für die kirchliche Einrichtung verbindlichen Vorschriften über den Datenschutz. Gem. § 47 Abs. 1 KDG sind die identifizierten Abweichungen (Verstöße) aktenkundig zu machen und zu beanstanden.

Gem. § 47 Abs. 5 lit. a) KDG kann die Datenschutzaufsicht Anordnungen treffen, um einen rechtmäßigen Zustand herzustellen. Insbesondere kann angeordnet werden, Verarbeitungsvorgänge auf bestimmte Weise und unter Fristsetzung mit dem Gesetz in Einklang zu bringen.

3.5 Informationsveranstaltungen

Die Mitarbeiter der Datenschutzaufsicht kommen der Nachfrage nach Informationsbedarf in den kirchlichen Einrichtungen gerne nach. In diesem Zusammenhang wird ohne Anspruch auf Vollständigkeit und nur zur Dokumentation der Bandbreite auf die nachstehenden Veranstaltungen hingewiesen.

- Vortrag Schulleiterkonferenz
- Vortrag Fachtag Kirchengemeinden und Kindertagesstätten
- Vortrag QM Zirkel Ludmillenstift

- Vortrag auf der faith + funds
- Vortrag Kirchengemeinde St. Antonius für Pfarrsekretärinnen
- Mehrfach Jour Fixe mit den betrieblichen Datenschutzbeauftragten
- Vortrag ALKO/DiCV
- IT Tagungen

Unabhängig davon besteht auch die Möglichkeit, sich über den kirchlichen Datenschutz im Rahmen der ständig aktualisierten und erweiterten Homepage der kirchlichen Datenschutzaufsicht zu informieren. In insgesamt zwölf Informationen (News) auf der Homepage wurde während des Berichtzeitraums auf aktuelle Gefährdungen oder datenschutzrechtliche Notwendigkeiten hingewiesen. Die Nachfrage nach den Newslettern der Datenschutzaufsicht für die norddeutschen Diözesen ist zudem erfreulich groß. Der Newsletter kann über die Homepage abonniert werden.

4 Über die Dienststelle des DDSB/Nord-Bremen

4.1 Infrastruktur

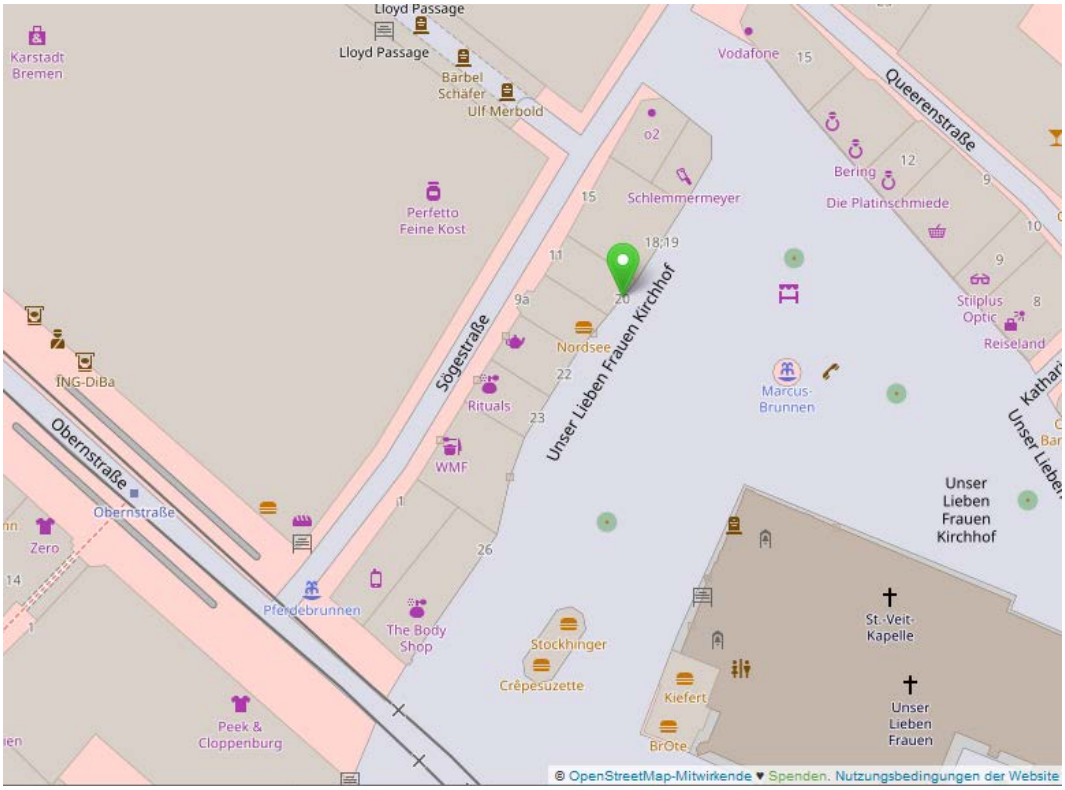
Das Büro der Datenschutzaufsicht ist in der zentralen Innenstadt von Bremen eingerichtet. Die Anschrift lautet:

Unser Lieben Frauen Kirchhof 20, 28195 Bremen.

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

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

Um die Anforderungen und Aufgaben im Bereich des kirchlichen Datenschutzes auch technisch effektiver wahrnehmen zu können, wurde Anfang des Jahres eine elektronische Aktenverwaltung mit eingebundenem Dokumentenmanagement-system eingeführt.



- openstreetmap.org
- opendatacommons.org

4.2 Finanzen

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

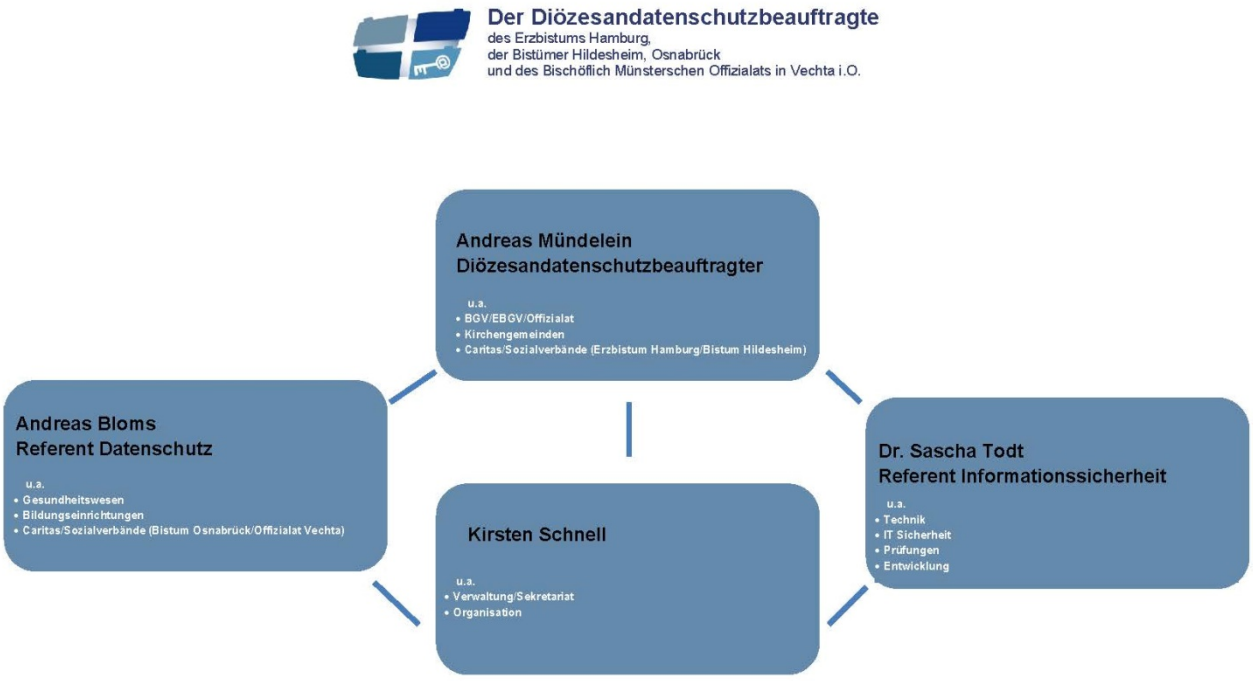
Die Finanz- und Budgethoheit liegt beim Diözesandatenschutzbeauftragten. Die Abwicklung des Haushaltes erfolgt über die Finanzabteilung des bischöflichen Generalvikariates Osnabrück als Belegenheitsbistum für die Stadt Bremen.

Für das Kalenderjahr 2019 standen Haushaltsmittel in Höhe von 371.400,00 Euro zur Verfügung.

4.3 Personal

Das Stellentableau umfasste im Berichtszeitraum 3,5 Vollzeitstellen, einschließlich des Sekretariats.

Die sachlichen Zuständigkeiten der Mitarbeiter sind in dem nachstehenden Organigramm dargestellt.



4.4 Vertretung in Konferenzen und Arbeitsgruppen

Der Leiter der Datenschutzaufsicht für die norddeutschen Diözesen ist persönlich in einer Reihe von ständigen oder temporären Konferenzen oder Arbeitsgruppen vertreten.

- Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche
- Referentenkonferenz für Datenschutz, Meldewesen und Kirchenmitgliedschaftsrecht der evangelischen Kirche
- AK „Anwendung der KAO“
- IT-Tagung für die Leiter der IT-Abteilungen der (Erz-) Diözesen und des Bischöflich Münsterschen Offizialats in Vechta und die Datenschutzreferenten
- Konferenz der Diözesanjuristen der norddeutschen (Erz-)Diözesen und des Bischöflich Münsterschen Offizialats in Vechta
- Tagung der Mitglieder des Virtuellen Datenschutzbüros
- Regelmäßige Treffen mit den betrieblichen Datenschutzbeauftragten

4.5 Vernetzung

Im Berichtszeitraum sind Kontakte aufgebaut und Gespräche mit den Landesbeauftragten für den Datenschutz und Informationsfreiheit geführt worden. Auf Einladung des Landesbeauftragten der Freien und Hansestadt Hamburg bestand zudem die Möglichkeit, an einer Arbeitsgruppe mit den Kirchen und der Aufsichtsbehörde teilnehmen zu können.

Zudem besteht ein guter Kontakt zum Beauftragten für den Datenschutz in der evangelischen Kirche Deutschlands und anderen kirchlichen Datenschutzbeauftragten oder Datenschutzreferenten.

4.6 Öffentlichkeitsarbeit

Der Internetauftritt der Datenschutzaufsicht Nord „www.datenschutz-kirche.de“ wird bundesweit genutzt und geschätzt. Es wird auch deshalb zukünftig das Ziel sein müssen, die Internetseite wie bisher zu pflegen und sie jeweils dem neuesten Stand des kirchlichen, und gegebenenfalls auch weltlichen, Datenschutzrechts anzupassen.

Erforderliche Anpassungen, wie etwa die elektronische Meldung von betrieblichen Datenschutzbeauftragten, Datenschutzpannen oder Beschwerden sind umgesetzt worden. Jeder Besucher der Homepage hat nun neben der schriftlichen oder telefonischen Meldung auch die Möglichkeit, seine Anliegen über ein entsprechendes Portal an die Datenschutzaufsicht zu melden.

Die vorgehaltenen Informationen, Arbeitshilfen, Praxishilfen und Mitteilungen dienen dazu, die Einrichtungsleiter und Mitarbeiter der kirchlichen Dienststellen gleichermaßen zu informieren und sie für das Recht auf informationelle Selbstbestimmung für sich und andere zu sensibilisieren.

5 Schlussbemerkung

Durch die Europäische Datenschutz-Grundverordnung und durch das im Zusammenhang damit entstandene kirchliche Datenschutzgesetz hat sich die datenschutzrechtliche Lage für den Bereich der Kirchen deutlich verändert. Nach diesseitiger Auffassung hin zu einem besseren Zustand, weil mit dem KDG ein gutes, praktikables und dem europäischen Standard entsprechendes Gesetz vorliegt. Ergänzt und konkretisiert wird dieses nunmehr durch die zugehörige Durchführungsverordnung.

Das Gesetz stellt die Rechte des Einzelnen im Zusammenhang mit dem Datenschutz in den Mittelpunkt und schützt umfangreich das Recht auf informationelle Selbstbestimmung des jeweils Betroffenen. Es hilft dadurch den Verantwortlichen unabhängig von der jeweils unterschiedlichen Motivlage bei der Verarbeitung personenbezogener Daten, die richtige Balance zwischen den Eigeninteressen und dem Recht des Betroffenen, über seine eigenen Daten selbst bestimmen zu können, einzuhalten.

Die Datenschutzaufsicht hat die Aufgabe die Balance immer wieder herzustellen und gegebenenfalls zu gewährleisten. Die erforderlichen Mittel, bis hin zur Sanktionierung, stehen zur Verfügung, bzw. werden angepasst oder entwickelt.

Der Fokus liegt dabei immer wieder auf der Beratung der kirchlichen Einrichtungen und erst letztlich bei der Sanktionierung eines datenschutzrechtlichen Fehlverhaltens. Wir kommen dieser Aufgabe unabhängig und frei von geleiteten Interessen nach und realisieren auch damit den Auftrag der Kirche, sich für die Belange der Einzelnen einzusetzen und das Grundecht auf informationelle Selbstbestimmung sicherzustellen.

Die Datenschutzaufsicht für die norddeutschen Diözesen wird diesen Weg auch weiterhin beschreiten und auch zukünftig dafür Sorge tragen, dass die Menschen im Zusammenhang mit ihren personenbezogenen Daten wahrgenommen und beachtet werden.

Der Diözesandatenschutzbeauftragte
des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28211 Bremen

Telefon.: 0421 330056-0
E-Mail: info@datenschutz-katholisch-nord.de
Internet: https://datenschutz-kirche.de

6 Anlagen

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

Einrichtung	Datenschutzbeauftragte	Anschrift
Bischöfliches Generalvikariat Osnabrück Ehe-/Familien-/Lebens-/Erziehungs-Beratungsstellen	Thomas Marien datenschutz@bistum-os.de Ludger Lüken l.lueken@bistum-os.de	Hasestraße 40a 49074 Osnabrück Domhof 2 49074 Osnabrück
Kirchliche Einrichtungen im Bistum Osnabrück	Itebo GmbH Kim Schoen datenschutz@bistum-osnabrück.de	Dielinger Straße 40 49074 Osnabrück
Offizialat Vechta	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Kirchliche Einrichtungen im Offizialat Vechta	intersoft consultig services AG Herr Stefan Winkel	Beim Strohause 17 20097 Hamburg
Bischöfliches Generalvikariat Hildesheim	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Kirchliche Einrichtungen im Bistum Hildesheim	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen
Erzbischöfliches Generalvikariat Hamburg	Itebo GmbH Kim Schoen dsb@itebo.de	Dielinger Straße 40 49074 Osnabrück
Kirchliche Einrichtungen im Erzbistum Hamburg	datenschutz nord GmbH Dr. Uwe Schläger kirche@datenschutz-nord.de	Konsul-Smidt-Straße 88 28217 Bremen

6.2 Flyer Information Datenpannen

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Hinweis zur Meldepflicht bei Datenpannen

Personenbezogene Daten müssen geschützt werden. Dies regelt das „Gesetz über den Kirchlichen Datenschutz“ (KDG).

Datenpannen sind meldepflichtig!

Datenpannen sind:

- Diebstahl von Laptops, Kameras etc. aus Einrichtungen
- der Verlust von USB-Sticks, wenn darauf personenbezogene Daten (z.B. Fotos) gespeichert waren
- Ungewollte Veröffentlichung von personenbezogenen Daten
- Versendung einer E-Mail mit offenem Adressverteiler
- Versand personenbezogener Daten an falsche Empfänger
- Nutzung von Daten für andere als die ursprünglichen Zwecke

Wenn Ihnen eine Datenpanne unterlaufen sollte oder diese bemerken, wenden Sie sich bitte an Ihre Einrichtungsleitung. Diese setzt sich mit dem betrieblichen Datenschutzbeauftragten in Verbindung.

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Andreas Mündelein
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

Internet: www.datenschutz-kirche.de

Meldeplattform:

https://www.datenschutz-kirche.de/datenpanne_melden