Der Diözesandatenschutzbeauftragte

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

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

4. Jahresbericht 2017

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

Tel.: 0421 / 16 30 19 25
Mobil: 0151 / 41 97 57 58
Mail: info@datenschutz-katholisch-nord.de

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

4. Jahresbericht

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

für das Jahr 2017

vorgelegt im März 2018

Stand 31.12.2017

Inhaltsverzeichnis

Vorwort

Der Datenschutz hat in der Kirche eine sehr lange Tradition.

Das seit 1215 n. Chr. im Kirchenrecht verankerte Seelsorge- und Beichtgeheimnis ist eine der ältesten Datenschutzvorschriften. Heute schützt für den Bereich der römisch-katholischen Kirche das weltweit gültige kirchliche Gesetzbuch Codex Iuris Canonici (CIC) das Persönlichkeitsrecht auf Schutz der Intimsphäre in Canon 220.

Auch im außerkirchlichen Bereich sind die Kirchen in Deutschland datenschutzrechtlich gut aufgestellt. Aufgrund des durch die Verfassung bestimmten Selbstbestimmungsrechts der Kirchen in Deutschland gelten die Datenschutzgesetze von Bund und Ländern im Bereich der öffentlich-rechtlichen Kirchen (einschließlich Caritas/Diakonie) zwar nicht unmittelbar. Die Kirchen haben aber ihre Verantwortung wahrgenommen und eigene Regelungen verabschiedet.

In der römisch-katholischen Kirche wurde das Recht bisher durch die Anordnung über den kirchlichen Datenschutz (KDO) und die spezifischen Regelungen für besondere Teilbereiche umgesetzt, welches die Bischöfe der Diözesen in Deutschland erlassen haben.

Die Regelungen haben wie auch im öffentlichen Bereich den Zweck, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Die katholische Kirche nimmt damit bewusst die Verantwortung für die Daten und Informationen war, die Ihr zur Erfüllung der kirchlichen und caritativen Aufgaben zur Verfügung gestellt oder von Ihr erhoben und verarbeitet werden.

Durch die Europäische Datenschutzgrundverordnung (DS-GVO) wird das Datenschutzrecht innerhalb der Europäischen Union vereinheitlicht. Das bezieht auch die katholische Kirche in Deutschland mit ein. Der Art. 91 DS-GVO gibt den Kirchen aber die Möglichkeit, für ihre Einrichtungen eigene Regelungen zu erstellen, die mit der Grundverordnung in Einklang zu bringen sind. Auf diese Weise wird

auch bei der katholischen Kirche die Einheitlichkeit mit dem europäischen Recht hergestellt werden.

Neben dem unmittelbaren Datenschutzrecht ist auch die Organisation des Datenschutzes Teil der Umsetzung der bestehenden und zukünftigen Regelungen des Datenschutzrechtes der katholischen Kirche.

Hierzu gehört neben anderem die unabhängige kirchliche Datenschutzaufsicht. 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.

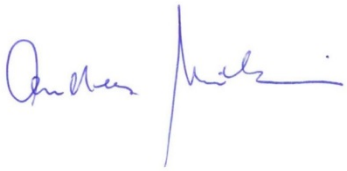
Dieser wacht über die Einhaltung der kirchlichen Datenschutzvorschriften und der anderen Vorschriften über den Datenschutz. Neben der Aufsicht ist die Beratung der bischöflichen Behörden und kirchlichen Dienststellen, aber auch die Weiterbildung von betrieblichen Datenschutzbeauftragten, Aufgabe und Anliegen der Datenschutzaufsicht. Der Austausch und die Zusammenarbeit mit anderen Diözesandatenschutzbeauftragten, den Datenschutzbeauftragten der evangelischen Kirche und den Landesdatenschutzbeauftragten ist nicht nur gesetzlich vorgesehen, sondern auch eine große Hilfe, um die Anwendung eines einheitlichen Datenschutzrechtsniveaus für die Kirchen zu entwickeln. Perspektivisch werden sich die gesetzlichen Aufgaben der Datenschutzaufsicht mit der Anpassung an die Europäische Datenschutzgrundverordnung (DS-GVO) signifikant erweitern.

Seit nunmehr zwei Jahren komme ich gerne der mir durch die (Erz)Bischöfe von Hamburg, Osnabrück und Hildesheim und dem Leiter des Bischöflich Münsterschen Offizialats in Vechta übertragenen Aufgaben nach. Dabei bin ich dankbar für das Vertrauen und die Unterstützung durch die Herren Generalvikare und die Mitarbeiter in den kirchlichen Behörden und Dienststellen.

Meinen Tätigkeitsbericht für das Jahr 2017 lege ich nachstehend vor. Wie bereits im letzten Bericht werde ich neben einer zusammenfassenden Darstellung der Entwicklung des Datenschutzrechtes auf europäischer und kirchlicher Ebene auch exemplarisch auf wesentliche Vorkommnisse in dem Berichtszeitraum hin-

weisen, die von allgemeiner Bedeutung für die Dienststellen in meinem Tätigkeitsbereich sein können.

Bremen, im März 2018



Andreas Mündelein
Diözesandatenschutzbeauftragter

1 Die Entwicklung des Datenschutzrechts

1.1 Europarecht

1.1.1 Die Europäische Datenschutzgrundverordnung

Die DS-GVO, die im Mai 2016 verabschiedet und in Kraft getreten ist, gilt ab dem 25. Mai 2018 (Art. 99 Abs. 1 DS-GVO). Sie gilt dann unmittelbar in den Mitgliedsstaaten der Europäischen Union. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten.

Art. 91 der DS-GVO garantiert das Selbstverwaltungsrecht der Kirchen nach Inkrafttreten der Verordnung unter der Voraussetzung, dass „zum Zeitpunkt des Inkrafttretens der Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung durch die Kirchen angewendet werden." Dies setzt nach allgemeiner Meinung voraus, dass die kirchliche Datenschutzordnung der DS-GVO in allen wesentlichen Punkten gleichwertig ist. Nicht erforderlich ist eine gleichartige Regelung, wohl aber eine, die unter den besonderen Umständen der kirchlichen Datenverarbeitung ein ebenso hohes Datenschutzniveau bietet wie das europäische Datenschutzrecht.

1.1.2 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, das als „Privacy Shield" bezeichnet wird.

Die Vereinbarungen in diesem Vertrag sind jedoch genauso umstritten, wie im aufgehobenen Safe Harbor Abkommen zuvor.

Die Art. 29-Gruppe nimmt in ihrem am 28.11.2017 veröffentlichten Arbeitspapier 255 („EU-U.S. Privacy Shield – First annual Joint Review“) Stellung zum EU-U.S. Privacy Shield.

Zwar bewertet die Art. 29-Gruppe die Anstrengungen der U.S.-Behörden für einen umfassenden Verfahrensrahmen zur Unterstützung des Privacy Shields grundsätzlich positiv, doch überwiegt noch die bisher ungelöste Problemlage im Hinblick auf eine Vielzahl von datenschutzrechtlichen Erfordernissen.

Unter anderem betrifft dies das Fehlen einer Anleitung oder klaren Information bezüglich der Prinzipien des Datenschutzschildes, einer stärkere Kontrolle und Supervision im Hinblick auf die Compliance mit den Prinzipien des Datenschutzschildes durch unabhängige, zertifizierte Unternehmen, die Unterscheidung von Auftragsverarbeitern und Verantwortlichen im Zeitpunkt ihrer Registrierung und Überprüfung, bis hin zur Verbesserung der Zusammenarbeit von U.S.-Behörden untereinander im Rahmen der Anwendung der Regelungen, und insbesondere des noch ungelösten Zugangs von U.S.-Behörden auf die in die USA im Rahmen des Privacy Shields übertragenen Daten.

Die Art. 29-Gruppe hat angekündigt, weitere Schritte, insbesondere die gerichtliche Überprüfung der Angemessenheitsentscheidung der Kommission zu unternehmen, wenn ihre Bedenken nicht berücksichtigt 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)

Neben der DS-GVO als E-Privacy-Richtlinie wurde die Überprüfung der Richtlinie 2002/58/EG („e-Datenschutz-Richtlinie“) angekündigt, um ein hohes Niveau des Schutzes der Privatsphäre für die Nutzer elektronischer Kommunikationsdienste und gleiche Wettbewerbsbedingungen für alle Marktteilnehmer zu gewährleisten.

Die E-Privacy-Richtlinie soll den Schutz von Grundrechten und Grundfreiheiten, insbesondere die Achtung des Privatlebens, Wahrung der Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation, gewährleisten. Außerdem gewährleistet sie den freien Verkehr von elektronischen Kommunikationsdaten, Geräten und Diensten in der Union.

Weil eine Bewertung der europäischen Datenschutzrichtlinie für die elektronische Kommunikation (E-Privacy-Richtlinie 2002/58/EG) allerdings ergeben hat, dass aufgrund der technischen und wirtschaftlichen Entwicklungen eine Neuregelung erforderlich ist (z.B. wg. neuer Internetdienste, die eine interpersonelle Kommunikation ermöglichen, VoIP-Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste), sollen die Grundsätze der DS-GVO im Hinblick auf die "elektronischen Kommunikationsdaten" durch eine Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-Verordnung) ergänzt und präzisiert werden.

Die noch im Gesetzgebungsverfahren befindliche Verordnung sollte ursprünglich ebenfalls am 25. Mai 2018 in Kraft treten und unmittelbar in jedem Mitgliedstaat gelten. Valide Angaben, wann das Verfahren abgeschlossen sein wird, liegen noch nicht vor.

1.2 Bundesrecht

1.2.1 BDSG

Am 27.04.2017 hat der Deutsche Bundestag 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 am 12. Mai 2017 vom Bundesrat gebilligt wurde.

Das derzeitige Bundesdatenschutzgesetz (BDSG-alt) tritt gemäß Art. 8 des DSAnpUG-EU am 25. Mai 2018 außer Kraft.

Mit dem DSAnpUG-EU und dem darin enthaltenen BDSG-neu werden datenschutzrechtliche Regelungen an die DS-GVO angepasst, in ihr enthaltene „Öffnungsklauseln“ genutzt und die Richtlinie (EU) 2016/680 umgesetzt.

Insoweit enthält das BDSG kaum mehr eigenständige Regelungen, sondern überwiegend Ausführung – und Ausnahmebestimmungen zur DS-GVO.

Für die kirchliche Datenschutzaufsicht ist die Regelung in § 18 BDSG (neu) von großer Bedeutung. Zum dort vorgesehenen Kohärenzverfahren heißt es in § 18 Abs. 1 S. 4 BDSG (neu):

> *„Die Aufsichtsbehörden des Bundes und der Länder beteiligen die nach den Artikeln 85 und 91 der Verordnung (EU) 2016/679 eingerichteten spezifischen Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.“*

Die Art und der Umfang der Beteiligung, bspw. der kirchlichen Datenschutzaufsichtsbehörden, sind noch in der Diskussion. Unbestritten wird es aber eine wie auch immer geregelte Beteiligung geben müssen.

1.2.2 Änderung im Telekommunikationsgesetz

Eine von Vielen erwartete Reform, welche die Betreiber öffentlicher WLANs von teuren Haftungsansprüchen freistellt, ist jetzt in Kraft getreten. Mit dem neuen § 8 TMG wurden im Absatz 1 die Sätze 2 und 3 mit folgender Formulierung eingefügt:

> *„Sofern diese Dienstleister nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.“*

Damit dürften nunmehr Abmahnungen von Rechteinhabern und Rechtsanwälten die rechtliche Grundlage entzogen worden sein. Die Geltung des Absatzes 1 wird nach wie vor auch auf Anbieter ausgewendet, die den Internetzugang über ein lokales drahtloses Netzwerk zur Verfügung stellen. Damit ist für alle kirchlichen Einrichtungen, die ihren Kunden ein offenes WLAN zur Verfügung stellen, ein hohes Maß an finanzieller Sicherheit erreicht. Von der Pfarrei, die Jugendlichen ein Netz anbietet, bis zu den Krankenhäusern, die mit einem WLAN für Patienten arbeiten, besteht nicht mehr die Gefahr durch teure Abmahnungen geschädigt zu werden. Sie dürfen allerdings nicht mit dem Nutzer vorsätzlich zusammenarbeiten. Die Beweislast, dass dies geschehen ist, liegt allerdings beim Rechteinhaber und Kläger.

Eine weitere wichtige Änderung ist im § 8 Absatz 4 TMG vorgenommen worden. Danach dürfen Diensteanbieter nicht von einer Behörde verpflichtet werden, vor Gewährung des Zugangs den Nutzer auf Grund persönlicher Daten zu registrieren oder die Eingabe eines Passwortes zu verlangen. Verbraucher sollen hingegen die Möglichkeit haben, überall mobil und unkompliziert ins Internet zu kommen. Diese Regelung dürfte kirchliche Dienststellen auch insoweit entlasten, als

keine besonderen technischen Maßnahmen zum Schutz des Zugangs erforderlich sind.

Mit diesen Änderungen haben jetzt alle Einrichtungen, die ihr Netz in einem gewerblichen Umfeld öffnen möchten, die Möglichkeit dazu, ihr WLAN für fremde Nutzer bereit zu stellen

1.3 Datenschutzrecht der Kirche

1.3.1 Anordnung über den kirchlichen Datenschutz (KDO)

Bisher gilt die mit Datum vom 18. November 2013 durch die 151. Vollversammlung des Verbandes der Diözesen Deutschlands beschlossene Anordnung über kirchlichen Datenschutz (KDO) für die katholischen Diözesen in Deutschland als einheitliches und für alle kirchlichen Stellen verbindliches Recht.

Nachdem sich innerhalb eines annähernd vier Jahre dauernden Zeitraums der Europäische Rat, das Europäische Parlament und die Europäische Kommission auf eine Text der DS-GVO verständigt hatten, wurde die Verordnung im Mai 2016 verabschiedet und am 04.05.2016 im Amtsblatt der Europäischen Union veröffentlicht. Sie gilt ab dem 25.05.2018.

Vor dem Hintergrund des Art. 91 der DS-GVO war es das Ziel bis zum 25.05.2018 die Regelungen über den kirchlichen Datenschutz (KDO) mit den Regelungen der Verordnung in Einklang zu bringen, um den Anforderungen für einen kirchenspezifischen Datenschutz und eine der Verordnung entsprechenden Datenschutzaufsicht zu gewährleisten.

Am 20.11.2017 hat sich die Vollversammlung des Verbandes der Diözesen Deutschlands mit der Novellierung des kirchlichen Datenschutzrechts befasst und einen vorbereiteten Entwurf eines neuen kirchlichen Datenschutzgesetzes (KDG) einstimmig beschlossen; den Diözesen hat die Vollversammlung die Inkraftsetzung zum 24.05.2018 und die entsprechende Veröffentlichung im jeweiligen Amtsblatt der Diözese empfohlen. Die KDO wird zu diesem Datum außer Kraft treten.

1.3.2 Das kirchliche Datenschutzgesetz (KDG)

Durch das Gesetz über den Kirchlichen Datenschutz (KDG) werden die Rechte der Betroffenen wesentlich gestärkt und durch die Einrichtung einer erweiterten

Datenschutzaufsicht im Rahmen der Regelungen des Kapitel VI DS-GVO abgesichert.

Es hat eine Fülle von Änderungen geben, auf die sich unsere Dienststellen und Einrichtungen einstellen müssen.

Unter anderem ergeben sich Veränderungen in folgenden Bereichen:

1.3.2.1 Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB)

Künftig müssen alle kirchlichen Diözesen, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände unabhängig von der Zahl ihrer Mitarbeiter einen eigenen betrieblichen Datenschutzbeauftragten bestellen. Dies sieht § 36 Abs. 1 Satz 1 KDG vor. Andere Einrichtungen, wie die der Caritas müssen nach Satz 2 ebenfalls einen betrieblichen Datenschutzbeauftragten bestellen, wenn sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen, oder ebenfalls solche Einrichtungen, deren Kerntätigkeit in der Verarbeitung besonderer Kategorien von personenbezogenen Daten besteht.

1.3.2.2 Eine Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse

Nach § 3a KDO war schon bisher ein Verfahrensverzeichnis aller automatisierten Datenverarbeitungsprozesse erforderlich. Diese Verpflichtung besteht auch nach dem neuen KDG (§ 31 Abs. 1 bis 5 KDG) für alle Einrichtungen mit 250 oder mehr Beschäftigten und ebenso für kleinere Einrichtungen, wenn ihre Verarbeitung die Rechte der betroffenen Personen gefährdet, die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien beinhaltet.

1.3.2.3 Prüfung der Rechtsgrundlagen

Schon bisher darf eine Datenverarbeitung nur dann erfolgen, wenn kirchliche oder staatliche Rechtsvorschriften sie erlauben oder anordnen, oder die betroffene Person in die Verarbeitung für einen oder mehrere Zwecke eingewilligt hat.

Dieser Grundsatz wird von § 6 KDG übernommen und darüber hinaus noch folgende Fälle der Zulässigkeit ausdrücklich benannt:

- Die Erfüllung eines Vertrages oder Vorvertrages, an dem die betroffene Person beteiligt ist.
- Die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt.
- Erforderlichkeit zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten.
- Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im kirchlichen Interesse liegt oder für die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde.
- Die Verarbeitung ist zur Wahrung der Interessen des Verantwortlichen oder eines Dritten erforderlich, soweit dabei nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Güterabwägung).

1.3.2.4 Besonderer Schutz der Daten von Kindern und Jugendlichen

Das neue Recht schützt besonders Minderjährige vor den Risiken elektronischer Datenverarbeitung. Grundsätzlich ist die Datenverarbeitung bei Anmeldungen oder Bestellungen im Internet, auch bei Erwachsenen nur mit der Einwilligungserklärung der Betroffenen erlaubt. Eine solche Erklärung, so bestimmt § 8 Abs. 8 KDG, kann aber künftig nur von Personen abgegeben werden, die das 16. Lebensjahr vollendet haben. In allen anderen Fällen, ist die Einwilligung der Personensorgeberechtigten erforderlich. Daher haben alle Einrichtungen, die elektronische Angebote bereitstellen, unter Berücksichtigung der zur Verfügung stehenden Technik, alle Anstrengungen zu unternehmen, um dies zu gewährleisten. Diese Verpflichtung gilt unabhängig davon, ob der betreffende junge Mensch zivilrechtlich im Stande ist, wirksame Verträge selbst abzuschließen. Also auch bei der Bestellung einer CD für 10 €, die im Rahmen der Taschengeldregelung rechtswirksam sein mag, ist die Datenverarbeitung bei elektronischer Bestellung nur mit Einwilligung der Sorgeberechtigten wirksam.

Lediglich für kostenfreie Beratungsangebote einer kirchlichen Stelle ist die Einwilligung der Eltern in die Datenverarbeitung nicht erforderlich, wenn das Kind bereits 13 Jahre alt ist. Hierdurch soll gewährleistet werden, dass eine pädagogi-

sche oder psychologische Beratung auch dann erfolgen kann, wenn diese sich auf Schwierigkeiten mit dem Elternhaus bezieht.

1.3.2.5 Rechte der Betroffenen durch transparente Information unterstützen

Betroffene sind in transparenter Weise, das heißt in einer einfachen und klaren Sprache, über die Verarbeitung ihrer Daten präzise, verständlich und in leicht zugänglicher Form zu informieren (§ 14 Abs. 1 bis 6 KDG). Dabei können auch standardisierte Bildsymbole verwendet werden. Besonderes Augenmerk ist dabei auf Informationen an Minderjährige zu legen. Auch für sie muss eine Verständlichkeit erreicht werden. Der Umfang der Informationspflicht ist durch § 15 KDG bei unmittelbarer Datenerhebung und § 16 KDG bei mittelbarer Datenerhebung in weitem Umfange präzisiert worden.

1.3.2.6 Rechte der Betroffenen umsetzen

Die Rechte der Betroffenen werden durch die Vorschriften der §§ 17 bis 25 KDG in Übereinstimmung mit der DS-GVO ausgeweitet. Das gilt vor allem für das Recht auf Löschung, § 19 KDG, und das Recht auf Datenübertragbarkeit, § 22 KDG. So ist eine Löschung der Betroffenendaten auch dann vorzunehmen, wenn die Einwilligung zu ihrer Verarbeitung widerrufen wird und keine andere Rechtsgrundlage für ihre weitere Verwendung besteht. Darüber hinaus besteht ein Widerspruchsrecht bei der Verarbeitung von Daten, die zum Zwecke der Direktwerbung oder für Profiling verwendet werden, § 23 KDG. Neu ist das Recht auf Datenübertagbarkeit in elektronischen Verfahren, bei dem die Person das Recht hat zu verlangen, dass ihre Daten von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden. Das dürfte vor allem in den Fällen von Bedeutung sein, bei denen der Anbieter von Dienstleistungen gewechselt werden soll.

1.3.2.7 Die eigene Dokumentation im Bereich der Datenverarbeitung organisieren

Das KDG sieht an mehreren Stellen Dokumentationspflichten für die datenverarbeitenden Stellen vor:

- § 31 KDG verlangt, dass ein Verzeichnis aller Verarbeitungstätigkeiten geführt wird.
- Bei der Auftragsverarbeitung ist nach § 29 Abs. 4 lit. c) in Verbindung mit § 26 Abs. 1 lit. d) KDG ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen organisatorischen und technischen Maßnahmen durchzuführen und zu ihrem Nachweis zu dokumentieren.
- Nach § 33 KDG sind Datenschutzvorfälle an die Datenschutzaufsicht binnen 72 Stunden zu melden und nach Absatz 5 zu dokumentieren.
- Nach § 40 Abs. 2 KDG sind Übermittlungen in Drittländer, die ohne einen Angemessenheitsbeschluss der Europäischen Kommission erfolgt, aber bei geeigneten Garantien vorgenommen werden, zu dokumentieren.

1.3.2.8 Bestehende Verträge mit Auftragsverarbeitern überprüfen und anpassen

Bestehende Verträge zur Auftragsverarbeitung sind zu überprüfen und gegebenenfalls an die neue Vorschrift des § 29 KDG anzupassen. Zu den bisherigen Verpflichtungen kommen folgende hinzu:

- Der Auftragsverarbeiter darf die Daten nur innerhalb der Europäischen Union verarbeiten. Das trifft auch auf Cloud-Dienste zu.
- Die Verpflichtung des Auftragsverarbeiters, seine Mitarbeiter auf das Datengeheimnis zu verpflichten.
- Haftung des Auftragsverarbeiters für Pflichtverletzungen durch Unterauftragsverarbeiter.
- Die Pflicht zur regelmäßigen Kontrolle über die Einhaltung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters.
- Der Auftragsverarbeiter ist nach § 31 Abs. 2 KDG vertraglich zu verpflichten, ein Verzeichnis aller Tätigkeiten der Verarbeitung zu erstellen, die für den Verantwortlichen ausgeführt werden.

1.3.2.9 Möglichkeit zur Vornahme einer Datenschutz-Folgenabschätzung einrichten

Die Vorschrift des § 35 KDG verpflichtet zur Vornahme einer Datenschutz-Folgenabschätzung durch die verantwortliche Stelle, wenn die Form der Verar-

beitung, insbesondere bei der Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Das Risiko kann sich ergeben aus der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung. Sie ist nach Absatz 4 insbesondere in folgenden Fällen erforderlich:

- Bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf einer automatisierten Verarbeitung, einschließlich Profiling, gründet.
- Bei einer umfangreichen Verarbeitung besonderer Kategorien von Daten nach § 11 Abs. 1 KDG oder Daten strafrechtlicher Verurteilungen.
- Bei der systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche.
- Nach Absatz 5 kann der Diözesandatenschutzbeauftragte zudem eine Liste von Verarbeitungsvorgängen erstellen und veröffentlichen, für die in jedem Fall eine Folgenabschätzung durchzuführen ist. Diese Liste kann auch erstellt werden für Verarbeitungsvorgänge, für die keine Datenschutz-Folgeabsicherung erforderlich ist. Dabei soll er sich an den Listen der Aufsichtsbehörden aus Bund und Ländern orientieren (Abs. 6).

Nach Absatz 7 umfasst die Datenschutz-Folgeabschätzung folgende Punkte:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, einschließlich ihrer Zwecke.
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf die Erreichung des Zwecks.
- Eine Bewertung der Risiken für die betroffenen Personen.
- Eine Darstellung der geplanten Abhilfemaßnahmen zur Bewältigung dieser Risiken. Dabei sind Garantien, Sicherheitsvorkehrungen und Schutzverfahren anzugeben, die den Nachweis zur Einhaltung dieses Gesetzes erbringen.

1.3.2.10 Erweiterte Maßnahmen der Datenschutzaufsicht

Bei der Feststellung von Verstößen gegen das KDG kann der Diözesandatenschutzbeauftragte nach § 47 KDG

- diese beanstanden und eine Frist zur Behebung gegenüber dem Verantwortlichen setzen (Abs. 1);
- bei Nichtbehebung der Mängel die Aufsicht führende Stelle verständigen und sie zu einer Stellungnahme auffordern (Abs. 3);
- Anordnungen erlassen, die geeignet sind, einen rechtmäßigen Zustand wiederherzustellen oder Gefahren für die Betroffenen abwehren (Abs. 5);
- Geldbußen zu verhängen (Abs. 6). Sie müssen im Einzelfall wirksam, verhältnismäßig und abschreckend sein (§ 51 Abs. 2 KDG) und können bis zu 500.000 Euro betragen (§ 51 Abs. 5 KDG).

1.3.2.11 Haftung und Schadensersatz

Erstmals wird nunmehr in § 50 KDG die zivilrechtliche Haftung für das Entstehen materieller und immaterieller Schäden zu Lasten der betroffenen Person geregelt. Eine betragsmäßige Haftungsbeschränkung ist dabei nicht vorgesehen. Mehrere Ersatzpflichtige haften als Gesamtschuldner.

Dem Betroffenen kommt außerdem zugute, dass eine Feststellung der Aufsichtsbehörde, eine Datenschutzverletzung habe objektiv vorgelegen, im Prozess vor den Zivilgerichten bindend ist (§ 47 Abs. 2 KDG).

1.3.2.12 Gerichtliche Überprüfung

Erstmals wurde auch die Möglichkeit eines gerichtlichen Rechtsbehelfs gegen eine Entscheidung der Datenschutzaufsicht oder gegen den Verantwortlichen geschaffen. Die Vorschrift des § 49 KDG wird bestimmen, dass hierfür ein kirchliches Gericht in Datenschutzangelegenheiten zuständig ist. Insoweit soll eine „Ordnung für die kirchlichen Gerichte in Datenschutzangelegenheiten (KDSGO) geschaffen werden.

1.3.3 Kirchliche Datenschutzgerichtsordnung (KDSGO)

Das Festhalten an ein eigenes kirchliches Datenschutzrecht hat zur Folge, dass es aus Gründen des „in Einklang bringens“ der kirchlicher Regelungen mit der DS-GVO einen Rechtsschutz für die Betroffenen gegen Entscheidungen, die durch den Diözesandatenschutzbeauftragten oder eines Verantwortlichen ergehen, geben muss. Vor diesem Hintergrund ist der Entwurf einer kirchlichen Datenschutzgerichtsbarkeit entwickelt worden, der am 20.11.2017 durch die Vollversammlung des Verbandes der Diözesen Deutschlands beschlossen wurde. Vorbehaltlich der Entscheidung der Deutschen Bischofskonferenz und den erforderlichen Genehmigungen durch die römischen Behörden wird die Kirchliche Datenschutzgerichtsordnung bis zum 24.05.2018 durch Veröffentlichung in den Amtsblättern der Diözesen in Deutschland in Kraft gesetzt werden und ein zwei Instanzen umfassendes kirchliches Datenschutzgericht entstehen lassen.

2 Die Entwicklung des Datenschutzes in kirchlichen Einrichtungen

2.1 Betriebliche Datenschutzbeauftragte

In ihren Abschlussverhandlungen hat sich die Europäische Union darauf geeinigt, das Erfordernis eines betrieblichen Datenschutzbeauftragten für gewerbliche Unternehmen entfallen zulassen; es bleibt allerdings für Behörden – und zu ihnen zählen auch die kirchlichen Dienststellen – aufrechterhalten.

Künftig müssen deshalb alle kirchlichen Diözesen, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände unabhängig von der Zahl ihrer Mitarbeiter einen eigenen betrieblichen Datenschutzbeauftragten bestellen. Dies sieht § 36 Abs. 1 Satz 1 KDG ausdrücklich vor. Andere Einrichtungen müssen nach Abs. 2 ebenfalls einen betrieblichen Datenschutzbeauftragten bestellen, wenn sich bei ihnen in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen, oder ebenfalls solche Einrichtungen, deren Kerntätigkeit in der Verarbeitung besonderer Kategorien von personenbezogenen Daten besteht.

Für die (erz)bischöflichen Verwaltungen und das Bischöflich Münstersche Offizialats in Vechta sind bis zum Ende des Berichtjahres betriebliche Datenschutzbeauftragte benannt worden. Die Zuständigkeit für die Bereiche der Schulverwaltungen ist dabei gesondert berücksichtigt worden.

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.

Alle Verantwortlichen aus den genannten Bereichen haben sich für den Abschluss von Verträgen mit externen Datenschutzbeauftragten entschieden. In einem gegenseitig abgestimmten Verfahren werden in einem ersten Schritt anhand von jeweils ausgewählten Kirchengemeinden exemplarisch Datenschutzkonzepte und eine Bestandsaufnahme aller durchgeführten Verarbeitungsprozesse erarbeitet, die im Laufe eines festgelegten Zeitraums auf alle kirchliche Einrichtungen übertragen werden können. In einem zweiten Schritt werden die vom Gesetz

vorgesehenen Aufgaben eines betrieblichen Datenschutzbeauftragten im Rahmen einer territorialen Zuordnung für die kirchlichen Einrichtungen umgesetzt.

2.2 Kirchliche Datenschutzaufsicht

Wie bereits im letzten Jahresbericht erwähnt muss die kirchliche Datenschutzbehörde die in Kapitel IV der DS-GVO niedergelegten Bedingungen erfüllen (Art. 91 Abs. 2 DS-GVO (Art. 51 – Art. 59 DS-GVO)).

Art. 52 Abs. 4 DS-GVO, der über Art 91 Abs. 2 DS-GVO auch im kirchlichen Bereich umgesetzt werden muss, regelt dass jeder Mitgliedstaat sicher stellen muss, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und ihre Befugnis auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können.

Die katholische Kirche hat die rechtliche Gleichstellung zur DS-GVO durch die §§ 42 – 46 KDG sichergestellt. Diese Verpflichtung der Diözesen umfasst die Sicherstellung der personellen, technischen und finanziellen Ressourcen.

Für den katholischen Bereich in der Bundesrepublik Deutschland ergibt sich folgendes Bild. Das katholische Datenschutzzentrum in Dortmund ist für die nordrheinwestfälischen Bistümer mit insgesamt 10 Vollzeitstellen konfiguriert. Die geplante Datenschutzaufsicht für die südwestlichen Bistümer, die ihren Sitz in Frankfurt haben wird, ist mit 5 Vollzeitstellen geplant, und wird den Betrieb zum 01.01.2018 aufnehmen. Die bayrische Datenschutzaufsicht, derzeit 3 Vollzeitstellen, wird auf 10 Vollzeitstellen aufgestockt werden. Im Bereich der ostdeutschen Bistümer besteht die Datenschutzaufsicht im Wesentlichen noch aus dem Beauftragten und einer Sekretariatskraft. Ein IT – Fachmann kann gegebenenfalls extern beauftragt werden.

Im Laufe des Berichtsjahrs wurde die personelle und damit verbunden die finanzielle Ausstattung der Datenschutzaufsicht für die norddeutschen Diözesen dem

gesetzlichen Aufgabenbereich angepasst. Das Stellentableau umfasst nunmehr 3 Vollzeitstellen und eine Teilzeitstelle für das Sekretariat.

Die kirchlichen Datenschutzaufsichtsbehörden 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 (§ 18 KDO). 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 von der Konferenz getroffenen Beschlüsse für die einheitliche Anwendung des kirchlichen Datenschutzrechts werden auf den jeweiligen Homepages der Datenschutzbeauftragten veröffentlicht. Damit soll eine größtmögliche Transparenz und Allgemeinverbindlichkeit in datenschutzrechtlichen Fragen erreicht werden.

3 Exemplarische Darstellung von Einzelfällen

3.1 Beratungen

Im Laufe des Berichtszeitraums wurde die Datenschutzaufsicht zunehmend mit telefonischen, schriftlichen und teilweise komplexen Anfragen befasst, die einen umfangreichen Schriftverkehr notwendig gemacht haben. Insgesamt haben die Anfragen laut der internen Statistik um 52% im Vergleich zum Vorjahreszeitraum zugenommen.

Wenn die Verantwortlichen in den kirchlichen Einrichtungen und die Betroffenen die Datenschutzaufsicht in steigendem Umfang als Beratung – und Hilfeeinrichtung wahrnehmen, ist das eine sehr positive Tendenz und zeigt eine zunehmende Sensibilität im Hinblick auf die Akzeptanz des kirchlichen Datenschutzes.

Nachstehend werden einige ausgesuchte Beratungsanfragen dargestellt:

3.1.1 Kirchengemeinden

Darf eine Kirchengemeinde die Namen der Verstorbenen (der vergangenen Woche) in ihrem gedruckten Pfarrbrief / Wochenblatt veröffentlichen?

Eine Veröffentlichung ist nicht zu beanstanden. Zum einen handelt es sich um eine Mitteilung (Nutzung), die zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist. Die Information der Gemeindemitglieder über den Tod eines anderen Mitgliedes mit der seelsorglichen Bitte dem Verstorbenen die ewige Ruhe zu gewähren ist unzweifelhaft eine kirchliche Aufgabe.

Zum anderen erlischt das Recht auf informationelle Selbstbestimmung mit dem Tod der betroffenen Person. Der Schutz personenbezogener Daten setzt immer eine „lebende“ Person voraus. Insoweit kann es auch nicht mehr um die Frage

der Einwilligung des Betroffenen im Hinblick auf die Veröffentlichung der Mitteilung gehen.

Demgegenüber gibt es ein postmortales Persönlichkeitsrecht das von den Angehörigen geltend gemacht werden kann. In der Regel besteht aber im Vorfeld einer Beerdigung ein intensiver Kontakt zwischen der Gemeinde und den jeweiligen Angehörigen. Bei dieser Gelegenheit können daher auch die Modalitäten einer Veröffentlichung/Bekanntgabe im Pfarrbrief mit den Beteiligten unmittelbar besprochen werden. Aus diesem Anlass sollte darauf hingewiesen werden, dass es in der Gemeinde üblich und auch aus theologischer Sicht wünschenswert bzw. notwendig sei, die Gemeinde über die geplante Beerdigung bzw. den Tod des Gemeindemitgliedes zu informieren. Dabei ist auch darauf hinzuweisen, in welcher Form dies geschieht. Von den Beteiligten hat dann jeder die Möglichkeit, sich hierzu zu äußern. Will sich jemand tatsächlich ausschließen, muss dies allerdings respektiert werden.

Darf eine Kirchengemeinde sämtliche Pfarrbriefe / Wochenblätter auf ihrer eigenen Homepage / im Internet veröffentlichen?

Es kommt darauf an, ob durch die Veröffentlichung auch personenbezogene Daten aus dem Pfarrbrief in das Internet gestellt werden.

Wenn ja, dann ist die Übermittlung personenbezogener Daten an nicht kirchliche Stellen nach § 12 KDO an bestimmte Voraussetzungen gebunden. Im vorliegenden Falle kommt erschwerend hinzu, dass eine Veröffentlichung im Internet an einen nicht feststehenden und daher nicht bestimmbaren Empfängerkreis erfolgt. Eine solche Bekanntgabe ist daher in der Regel zur Erfüllung der Aufgaben der Pfarrgemeinde nicht erforderlich und erfolgt nicht für die Zwecke, für die die Daten erhoben worden sind. Sie können daher nur mit Einwilligung der Betroffenen eingestellt werden (§ 3 Abs.1 Nr. 2 KDO). Eine allgemein gehaltene Zustimmung wäre hierfür nicht ausreichend. § 3 Abs. 2 KDO verpflichtet die veröffentlichende Stelle, den Betroffenen auf den Zweck der Nutzung hinzuweisen und sich auf der Grundlage der Freiwilligkeit schriftlich bestätigen zu lassen, dass die Betroffenen hiermit einverstanden sind.

Nachfrage eines „erwachsenen Kindes“ nach dem Verbleib seiner leiblichen Mutter nach dessen Adoption.

Das „Kind“ hat um die Mitteilung der Anschrift seiner möglichen leiblichen Mutter aus dem Bestand der Meldedaten einer katholischen Kirchengemeinde gebeten

Nach § 5 Abs. 5 KMAO hat jedes Pfarramt zu gewährleisten, dass die melderechtlichen Sperrvermerke entsprechend ihrem Zweck beachtet werden.

Selbstverständlich ist das Adoptionsgeheimnis aus §§ 61 ff Personenstandsgesetz (PStG), § 1758 Bürgerliches Gesetzbuch (BGB) zu schützen.
Gemäß § 1758 I BGB ist es sowohl Privatpersonen als auch Behörden, und insoweit auch den Kirchengemeinden, grundsätzlich untersagt, Tatsachen, die geeignet sind, eine Adoption und ihre Umstände aufzudecken, zu offenbaren oder auszuforschen.

In Fällen, in denen inzwischen erwachsene „Kinder“ die Personen ihrer leiblichen Eltern ausfindig machen wollen, sind diese an die zuständigen Standesämter zu verweisen. Solche Ermittlungen gehören nicht zum Aufgabenbereich der Kirche.

Veröffentlichung der Namen ehrenamtlichen Helfer auf der Homepage einer Kirchengemeinde

Jede Pfarrei ist auf die Mitarbeit Ehrenamtlicher angewiesen. So gibt es Messdiener, Lektoren, Kommunionhelfer und weitere Helfer, deren Mitarbeit in Plänen koordiniert werden muss. Diese Pläne enthalten personenbezogene Daten.

Es ist darauf zu achten, dass die Pläne nur denjenigen zugänglich gemacht werden, die die darin enthaltenen Informationen für ihren Dienst benötigen. Für die Veröffentlichung solcher Informationen im Pfarrbrief bestehen keine Notwendigkeit und auch keine Rechtsgrundlage. Dies trifft umso mehr zu, wenn der Pfarrbrief online gestellt wird und somit über das Internet einer unüberschaubaren Vielzahl von fremden Personen personenbezogene Daten zugänglich gemacht werden.

Neben einer postalischen Zustellung der Pläne besteht die Möglichkeit, diese in einen geschützten Bereich auf der Homepage der Pfarrei einzustellen, auf den nur Berechtigte einen Zugriff haben.

Sollen solche Pläne trotz datenschutzrechtlicher Bedenken im Internet oder im Pfarrbrief veröffentlicht werden, ist die Einwilligung jedes Betroffenen erforderlich. Bei Kindern und Jugendlichen ist neben der Einwilligungserklärung der Eltern auch die der Kinder und Jugendlichen einzuholen, wenn sie über die notwendige Einsichtsfähigkeit verfügen. Dies dürfte spätestens ab dem 16. Lebensjahr der Fall sein.

Eine Veröffentlichung ohne die erforderliche Einwilligung ist rechtswidrig.

Anfrage zu einer Videoüberwachung einer Kindertagesstätte auf der Grundlage der Präventionsordnung

Datenschutzrechtlich ist die Videoüberwachung in der Vorschrift des § 5a der Anordnung über den kirchlichen Datenschutz (KDO) geregelt.

Der Eingangsbereich eines Kindergartens ist ein öffentlich zugänglicher Raum, der von einer Vielzahl von Personen betreten werden kann. Von den Mitarbeiterinnen, den Kindern, Sorgeberechtigten, aber auch von Postboten, Handwerkern und vielen anderen.

Die Videoüberwachung, und das wird von Vielen nicht erkannt, bedeutet einen schwerwiegenden Eingriff in das Persönlichkeitsrecht unbeteiligter und unverdächtiger Menschen. Sie kann daher nur in Ausnahmefällen zulässig sein, wenn schwerwiegende Gründe gegeben sind, die in einer Abwägung der Rechte das Persönlichkeitsrecht der Betroffenen deutlich überwiegen.

Nur dann, wenn in der Vergangenheit Fälle von Kindesmissbrauch vorgekommen sind und nur hierdurch verhindert werden kann, dass sich solche Fälle wiederholen, besteht Veranlassung über eine Videoüberwachung nachzudenken.

In diesen Fällen muss aber jede andere Möglichkeit des Schutzes, die das Persönlichkeitsrecht der Betroffenen weniger beeinträchtigt, der Vorzug gegeben werden. Diese Verpflichtung ergibt sich aus der Forderung gern. § 5a Abs. 1 Nr. 2 KDO nach einer Erforderlichkeit der Maßnahme. Ein Abschließen der Tür und eine Türklingel könnten das Ziel in der Regel genauso erreichen.

Die Präventionsordnung an sich ist keine Rechtsgrundlage für die Durchführung von Videoüberwachungen. Es müssen handgreifliche und anders nicht abwendbare Gründe für die Installation vorliegen. Nach § 3 Abs. 5 KDO ist daher zuvor eine Vorabkontrolle durchzuführten, in der diese Gründe dargelegt und mit bisher aufgetretenen Fällen, möglichst unter Angabe von Aktenzeichen durchgeführter Strafverfahren, belegt werden. Ohne die Durchführung einer genehmigenden Vorabkontrolle darf das System nicht in Betrieb genommen werden.

3.1.2 Bildungseinrichtungen

Verwendung von im Internet recherchierten E Mail Anschriften, um Flyer (Newsletter) zu verschicken.

Die Verwendung von recherchierten E-Mail Anschriften für Werbezwecke ist nicht frei von rechtlichen Bedenken.

Es ist nach den datenschutzrechtlichen Verlautbarungen zunehmend zu beobachten, dass Versender wegen unverlangt zugesandter Werbe-Emails/News abgemahnt werden. Die Adressaten solcher Mitteilungen sind nicht mehr damit zufrieden, die unerwünschten elektronischen „Werbenachrichten“ einfach zu löschen. Stattdessen greifen sowohl Privatleute als auch Unternehmer immer öfter zum Mittel der Abmahnung, um den Absendern solcher E-Mail-Newsletter beizukommen.

Der Empfänger einer unverlangt zugesandten Werbe-E-Mail kann vom Absender nach dem bürgerlichen Recht das Unterlassen verlangen. Privatpersonen können sich dabei auf ihr allgemeines Persönlichkeitsrecht berufen, das durch die Zusendung unverlangter Werbung beeinträchtigt wird. Den Unternehmern steht der Anspruch wegen eines widerrechtlichen Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb zu. Zudem stellt das Versenden unverlangter Werbe-E-Mails auch eine unlautere Wettbewerbshandlung dar und kann daher auch nach dem Gesetz über den unlauteren Wettbewerb abgemahnt werden.

Das Verfahren der Abmahnung, zumal wenn es über eine Anwaltskanzlei betrieben wird, ist mit nicht unerheblichen Kosten verbunden, die vom Absender zu erstatten sind.

Wer E-Mails mit werbendem Inhalt an Dritte versenden will, bedarf grundsätzlich der Einwilligung des jeweiligen Adressaten. Wird die Einwilligung des Adressaten in elektronischer Form eingeholt, muss die Einwilligung gemäß § 13 Abs. 2 TMG ihrerseits folgende Voraussetzungen erfüllen:

- Die Einwilligung muss durch eine ausdrückliche Handlung des Adressaten (bewusst und eindeutig) erfolgen (z.B. mittels Opt-In Checkbox oder Bestellbutton).
- Die Einwilligung des Adressaten muss protokolliert werden (Logfiles).
- Der Inhalt der Einwilligungserklärung muss jederzeit für den Adressaten abrufbar sein (Datenschutzerklärung).

Zudem muss der Adressat nach § 13 Abs. 3 TMG vor Erklärung seiner Einwilligung auf die jederzeitige Widerrufsmöglichkeit (Abbestellmöglichkeit) hingewiesen werden.

Dabei ist der Anbieter für das Vorliegen einer Einwilligung des Adressaten beweispflichtig. Wenn er den Nachweis mangels ordnungsgemäßer Dokumentation nicht führen kann, droht ihm eine kostenpflichtige Abmahnung wegen wettbewerbswidrigen Verhaltens.

Es besteht demgegenüber die Möglichkeit, auf der eigenen Website eine Kontaktmöglichkeit zu schaffen, mittels derer Interessierte Newsletter abonnieren können. Die Bestellungsmail ist zu dokumentieren.

3.1.3 Krankenhäuser

Umgang mit Patientendaten (Auszug aus einer Dienstanweisung einer Krankenhausgesellschaft)

In Abstimmung mit dem Diözesandatenschutzbeauftragten ist nachstehende Dienstanweisung entstanden, die exemplarisch in den Jahresbericht aufgenommen wird.

> *„Patienteninformationen (Befunde, Arztbriefe, Bilder etc.), in denen die persönlichen Daten des jeweiligen Patienten ersichtlich sind, dürfen nicht per Mail, Fax oder gar per WhatsApp, Facebook oder andere Medien versendet werden. Diese Versandarten haben den Charakter einer Postkarte und mit einem Versenden wird grob fahrlässig gegen aktuelles Datenschutzrecht verstoßen.*

Sofern entsprechende Dokumente aus dringenden Gründen per Mail oder per Fax verschickt werden sollen, hat der Versender dafür zu sorgen, dass entweder die Dokumente verschlüsselt versendet werden oder dass die persönlichen Daten des Patienten (Name, Vorname, Geburtsdatum etc.) unkenntlich gemacht werden.

Beim Versenden per Mail können die Dokumente in eine Zip-Datei umgewandelt und müssen verschlüsselt werden. Der Ersteller der Datei vergibt ein Passwort, mit dem der Empfänger der Nachricht die Zip-Datei dann wieder öffnen kann Es ist zu beachten, dass das Passwort zum Öffnen der Datei nicht mit der Mail versendet wird, sondern separat per Telefon dem Adressaten mitgeteilt wird.

Beim Versenden per Fax sind die Regelungen der Fax-Richtlinie „Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte“ - veröffentlicht im Kirchlichen Amtsblatt für die Diözese Osnabrück, Band 48, Nr. 42, Art. 377, Seite 282 - zu beachten. Wegen der besonderen Schutzbedürftigkeit der Patientendaten ist es gemäß Ziffer 7 der Fax-Richtlinie u. a. geboten, unmittelbar vor der Sendung eine telefonische Vereinbarung möglichst auch über persönliche Entgegennahme der Sendung zu treffen.

Die Nutzung von WhatsApp, Twitter, Facebook oder andere Medien für dienstliche Zwecke sind gar nicht gestattet.

Patientenunterlagen dürfen das Krankenhaus nicht verlassen. So ist beispielsweise die Mitnahme von Patientenakten nach Hause zum Diktieren von Arztbriefen nicht zulässig und verstößt gegen das Datengeheimnis. Sofern dies aus betrieblichen Gründen notwendig sein sollte, muss der Patient hierzu befragt werden und schriftlich einwilligen. Ferner muss der jeweilige Chefarzt darüber informiert werden und die Mitnahme der Akten muss dokumentiert werden, damit immer nachvollziehbar ist, wo sich die jeweilige Akte befindet (Sicherstellung der Verfügbarkeit der Patientendaten).“

Aktenverwaltung in kirchlichen Krankenhäusern

Im August 2016 wurde eine Befragung aller 35 Krankenhäuser der katholischen Kirche in den Norddiözesen in Angriff genommen, die im März 2017 abgeschlossen wurde. Die dabei gemachten Angaben sind nunmehr in einem „Leitfaden zur Aktenverwaltung in Krankenhäusern von Trägern der katholischen Kirche im Erzbistum Hamburg, den Bistümern Hildesheim und Osnabrück und dem Bischöflich Münsterschen Offizialat in Vechta i.O." zusammengefasst worden. Der Leitfaden versteht sich als Hilfestellung für alle datenschutzrechtlich verantwortlichen Mitarbeiter der beteiligten Krankenhäuser. Er gibt wichtige Hinweise zu einer ordnungsgemäßen Organisation der Aktenverwaltung.

Der Leitfaden kann unter folgendem Link heruntergeladen werden:

datenschutz-kirche.de/krankenhaus

3.1.4 Prüfungen

Die datenschutzrechtlich relevanten Abläufe im Zusammenhang mit der Organisation und dem Betrieb einer Fachklinik

Die Fachklinik ist spezialisiert auf die Therapie und Rehabilitation abhängigkeitskranker Frauen. Die Klinik besteht seit 1975 und verfügt über 80 vollstationäre und 5 ganztägig ambulante Behandlungsplätze. Ein besonderes Angebot stellt die spezifische Behandlung psychischer Störungen dar.

Im Rahmen eines Vor-Ort-Audits wurde die Feststellung der Konformität der Verarbeitung personenbezogener Daten mit den Vorgaben aus den Regelwerken

- Anordnung über den kirchlichen Datenschutz (KDO) in der Diözese Münster (Kirchliches Amtsblatt für die Diözese Münster vom 15.04.2014, Nr. 8, Art. 12, Seite 152 ff.)
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO), insbesondere IV. Zu § 6 KDO Anlagen 1 und 2 und die zugehörigen IT-Richtlinien.
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern,

überprüft.

Dazu wurden ein

- Datenschutzkonzept nach Anlage 2 zu § 6 KDO – DVO (Stand 10. Oktober 2017),
- ein Verfahrensverzeichnis (Stand Oktober 2017), sowie
- ein Auszug aus dem QM-Handbuch Datenverwaltung / Datenschutz (Stand August 2017)
- Schlüsselkonzept
- Besucherbuch

vorgelegt. Die Feststellungen zur rechtlichen/technischen Prüfung orientieren sich im Wesentlichen an der Chronologie des vorgelegten Konzepts und des Verfahrensverzeichnis.

Im Ergebnis ist festzuhalten:

Die auf Nachfrage der Einrichtung durchgeführte Prüfung war durch die Geschäftsleitung gut vorbereitet. Die beteiligten Mitarbeiter der Fachklinik standen für Erklärungen und Nachfragen im Rahmen des Prüfungsablaufs jederzeit zur Verfügung. Die Einrichtung ist im Hinblick auf die Gewährleistung des erforderlichen Datenschutzes, soweit dieser wie aus dem Audit ersichtlich geprüft worden ist, auf einem guten Weg.

Unabhängig davon sind die im Laufe des Audits getroffenen Feststellungen zu berücksichtigen und die noch fehlende Dokumentation zeitnah nachzureichen.

Es wurde festgestellt, dass die Patientendaten mit einem verschlüsselten Verfahren an den bei einem Dienstleister vorhandenen Server transportiert werden. Auf dem dortigen Server werden die Daten in unverschlüsselter Form gespeichert und einem möglichen Zugriff der dortigen Administratoren ausgesetzt. Es ist erforderlich, die aus der ärztlichen Schweigepflicht (§ 203 StGB) resultierende Geheimhaltungsverpflichtung der Patientendaten durch eine vertragliche Einbeziehung des Dienstleisters in den Verpflichtungskreis des Arztes zu realisieren (derz. Stand der Rechtslage).

Unabhängig davon gilt, dass dann, wenn Patientendaten in eine Cloud gestellt werden, diese nur verschlüsselt gespeichert und übertragen werden dürfen. Die Vorgabe korrespondiert mit einer Entscheidung der DSK der Landesdatenschutzbeauftragten.

3.1.5 Fortbildungen

Neben der ständigen Aktualisierung und Erweiterung der angebotenen Arbeitshilfen für unterschiedliche Bereiche wurden im Laufe des Berichtszeitraums acht Praxishilfen (von 17) erstellt und eine weitere zur Veröffentlichung vorbereitet. Auf Nachfrage von Krankenhäusern, caritativen Einrichtungen und Kirchengemeinden, sowie der MAV wurden insgesamt 8 Fortbildungsveranstaltungen am jeweiligen Standort der Einrichtung geplant und durchgeführt. Die Nachfrage nach Fortbildungen ist im Laufe des Jahres erheblich gestiegen, was im Zusammenhang mit dem neuen kirchlichen Datenschutzgesetz zu sehen ist. Soweit wie möglich werden aufgrund dessen für das nächste Jahr primär solche Information/Fortbildungsmaßnahmen geplant, bei denen eine große Zahl von Multiplikatoren erreicht werden kann.

3.1.6 Beschwerden

Anschreiben an Katholische Erstwähler bei einer Landtagswahl

Im Mai 2017 wurde dem Datenschutzbeauftragten im Auftrag des Ministeriums für Inneres und Bundesangelegenheiten des Landes Schleswig–Holstein eine Anfrage zugeleitet, die auf die Verwendung von Meldedaten abzielt, die das Erzbistum Hamburg nach den Vorschriften des Bundesmeldegesetzes aus den Schleswig-Holsteinischen Melderegistern zur Erfüllung seiner Aufgaben erhalten hat. Der Bezug war ein Erstwählerbrief, den der Erzbischof im Rahmen der letzten Landtagswahl an die katholischen Erstwähler in der Diözese versandt hat.

Nach Prüfung der Sach- und Rechtslage konnte festgestellt werden, dass eine befürchtete unzulässige Verwendung von Meldedaten nicht gegeben war.

Nach § 42 Abs. 1 S. 1 BMG (Bundesmeldegesetz) darf die Meldebehörde einer öffentlich–rechtlichen Religionsgemeinschaft u.a. definierte Daten unter der Voraussetzung zur Verfügung stellen, dass die Religionsgemeinschaft diese Daten zur Erfüllung ihrer Aufgaben nutzt.

Die Verwendung von Meldedaten zum Anschreiben der katholischen Erstwähler im Land Schleswig–Holstein war im vorliegenden Fall gerechtfertigt, weil es der kirchlichen Aufgabenerfüllung dient, wenn der Erzbischof mit „seinen“ katholischen Erstwählern in einen Kommunikationsprozess eintreten will, zu dem er die Angeschriebenen ausdrücklich auffordert. Es gehört dabei fraglos zu den Aufgaben der katholischen Kirche, Wertvorstellungen und Überzeugungen in die Öffentlichkeit einzubringen und so an der öffentlichen Meinung mitzuwirken. Der Bischof betont in seinem Schreiben die christlichen Werte, die den jungen Kirchenmitgliedern, die zum ersten Mal wählen dürfen, bei ihren persönlichen Entscheidungen als Leitfaden dienen können, und fordert sie auf, ihm Rückmeldungen über ihre Erfahrungen als Erstwähler mitzuteilen.

Nach dem verfassungsrechtlich geschützten kirchlichen Selbstverständnis ist die Kirche frei, Ihre Aufgaben zu definieren, wenn damit ein Stück des Auftrages der Kirche in dieser Welt wahrgenommen und erfüllt wird.

Für das kirchliche Anliegen des Erzbischofs, die katholischen Erstwähler für die Wahl zu motivieren, darum zu bitten sich zu informieren und für die Ausübung

des Wahlrechtes zu werben, war das Anschreiben erforderlich. Andere Kommunikationsformen standen insoweit nicht zur Verfügung.

Das Schreiben des Erzbischofs an katholische Erstwähler war zudem eine für die kirchliche Aufgabe geeignete Form, die definierte Zielgruppe anzusprechen. Bei der bekanntermaßen eher geringen Anzahl derer, die regelmäßig an einem Sonntagsgottesdienst teilnehmen (ca. 10% in Schleswig–Holstein), war der Zweck nicht über andere kirchenübliche Verlautbarungsformen zu erreichen. Deshalb war das postalische Versenden an die jeweiligen Anschriften der Zielgruppenmitglieder allein geeignet, das kirchliche Anliegen des Erzbischofs zu realisieren.

Es ist in der Bundesrepublik Deutschland üblich, dass sich Bischöfe vor einer Wahl öffentlich äußern und sich, insbesondere für die Ausübung des Wahlrechts, werbend einsetzen. Nichts anderes hat der Erzbischof von Hamburg heruntergebrochen auf die katholischen Erstwähler getan. Er fordert zur Wahrnehmung des Wahlrechtes auf und bittet die Jugendlichen darum, sich zu informieren. Das der Erzbischof dabei absolut kirchliche Themenbereiche als Anregung und Hilfestellung benennt ist folgerichtig und entspricht dem kirchlichen Selbstverständnis.

Zugehörigkeit zu einer katholischen Kirchengemeinde, Bekanntgabe der über den Beschwerdeführer gespeicherten Daten

Die Anfrage vom Juni 2017 wurde über das Bistum Hamburg an den Datenschutzbeauftragten weitergeleitet.

Der Beschwerdeführer gab an bereits in den 90er-Jahren aus der kath. Kirche ausgetreten zu sein, und bat um Mitteilung, wie er zu der kath. Kirchengemeinde laut einem Einladungsschreiben "gehören" kann und wie sein Name/Anschrift in die Datenbank der Kirchengemeinde gelangen konnte.

Ferner bat er um vollständige Mitteilung seiner gespeicherten Daten nach §34.

Darüber hinaus begehrte der Beschwerdeführer die Mitteilung, woher die gespeicherten Daten stammen, an welche Empfänger die Daten weitergegeben wurden und zu welchen Zwecken die Daten gespeichert werden.

Nach der kircheneigenen datenschutzrechtlichen Bestimmung ist der Diözesandatenschutzbeauftragte einzuschalten, wenn ein Sachverhalt vorgetragen wird, der geeignet sein könnte, dass bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch kirchliche Stellen gegen kirchliche Datenschutzbestimmungen verstoßen worden ist (vgl. § 15 Abs. 1 KDO)

Die Anordnung über den kirchlichen Datenschutz (KDO) ist die für den Bereich der römisch-katholischen Kirche in Deutschland geltende Datenschutz-Regelung. Die Kirchen in Deutschland haben das Recht, aufgrund des kirchlichen Selbstbestimmungsrechts in Art. 137 Absatz 3 der Weimarer Reichsverfassung in Verbindung mit Art. 140 des Grundgesetzes, eigene Rechtsordnungen für ihren Bereich zu erlassen. Aufgrund der Europäischen Datenschutzrichtlinie 1995/46/EG sind sie verpflichtet, Regeln zum Datenschutz aufzustellen.

Letzteres hat die katholische Kirchen getan und der Erzbischof von Hamburg hat für seine Diözese die Anordnung über den kirchlichen Datenschutz (KDO) im Erzbistum Hamburg vom 07. März 2014 (vgl. Kirchliches Amtsblatt des Erzbistums Hamburg vom 18.03.2014, Nr. 3, Art.36, Seite 45 ff.) in Kraft gesetzt.

Insoweit dient das kirchliche Datenschutzrecht als Grundlage für die Beantwortung der Fragen.

Nach der Prüfung des Sachverhalts war der Beschwerdeführer aus einem kirchlichen Anlass angeschrieben worden, da er als Gemeindemitglied im Gemeindemitgliederverzeichnis aufgeführt war.

Das Gemeindemitgliederverzeichnis ist die wirksame und gleichzeitig notwendige Grundlage für eine ordnungsgemäße pastorale Versorgung in den Kirchengemeinden (Zweck).

Nach deutschem Recht erhalten die Kirchen diese Daten durch staatliche Übermittlung. Geregelt ist dies durch das Bundesmeldegesetz (BMG) vom 03. Mai

2013, zuletzt geändert am 20.10.2015 und in Kraft getreten am 01.11.2015. Nach § 42 Abs. 1 BMG hat die katholische Kirche, als öffentliche Religionsgesellschaft gegenüber den Einwohnermeldeämtern Anspruch auf Übermittlung der Daten ihrer Mitglieder.

Die Datenübermittlung erfolgt durch die Meldebehörden als kommunaler Datensatz an die kirchliche Meldestelle im Generalvikariat. Von dort aus werden sie in einem kirchlichen Rechenzentrum verarbeitet und als Gemeindemitgliederverzeichnis den Pfarrgemeinden zur Verfügung gestellt.

Nach den der katholischen Kirche im Erzbistum Hamburg auf der rechtlichen Grundlage des BMG zu übermittelten Daten war der Beschwerdeführer seit seinem Zuzug in Hamburg mit der Konfession r.k. (römisch-katholisch) gemeldet, ebenso wie auch in seinem Wegzugort. Ein von ihm vollzogener Kirchenaustritt war offensichtlich melderechtlich nicht bekannt. Ansonsten hätte die Kirchengemeinde seine Daten nicht in dem Gemeindemitgliederverzeichnis aufgeführt.

Ein Austritt aus der katholischen Kirche ist immer zu dokumentieren und der kommunalen Meldebehörde bekannt zu geben. Aus welchen Gründen der vom Beschwerdeführer in den „neunziger Jahren“ vollzogene Kirchenaustritt nicht registriert und melderechtlich behandelt worden ist, war nicht zu ermitteln.

Nach den kirchlichen Datenschutzregelungen hat der Beschwerdeführer selbstverständlich das Recht Auskunft über die zu seiner Person gespeicherten Daten zu erhalten (vgl. § 13 KDO). Ihm wurde zu diesem Zweck ein Ausdruck aus dem Meldewesenprogramm zur Verfügung gestellt. Diese Daten sind der katholischen Kirche in Hamburg durch das Einwohnermeldeamt zur Verfügung gestellt worden. Sie bilden die Grundlage für das Gemeindemitgliederverzeichnis, dass der Kirchengemeinde zum Zweck der ordnungsgemäßen pastorale Versorgung zur Verfügung steht.

Eine Weitergabe der Daten an Dritte erfolgt nicht.

4 Über die Dienststelle des DDSB/Nord–Bremen

4.1 Infrastruktur

Mit Datum vom 01.10.2017 wurde das Büro der Datenschutzaufsicht von der Schwachhauser Heerstr. 67 in 28211 Bremen in ein Gebäude in der zentralen Innenstadt verlegt. Die neue Anschrift lautet: Unser Lieben Frauen Kirchhof 20, 28195 Bremen.

Das Büro ist über die Straßenbahnlinien 4 und 6 (2 Stationen, Schüsselkorb) vom HBF in Richtung Arsten/Flughafen / bzw. Bahnhof schnell zu erreichen. Die fußläufige Entfernung beträgt ca. 10 Min.

Das Büro ist regelmäßig von Montag bis Donnerstag in der Zeit von 09:00 – 17:00 Uhr und am Freitag von 09:00 bis 14:00 zu erreichen.

Telefon: 0421 16301925
E-Mail: info@datenschutz-katholisch-nord.de

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.

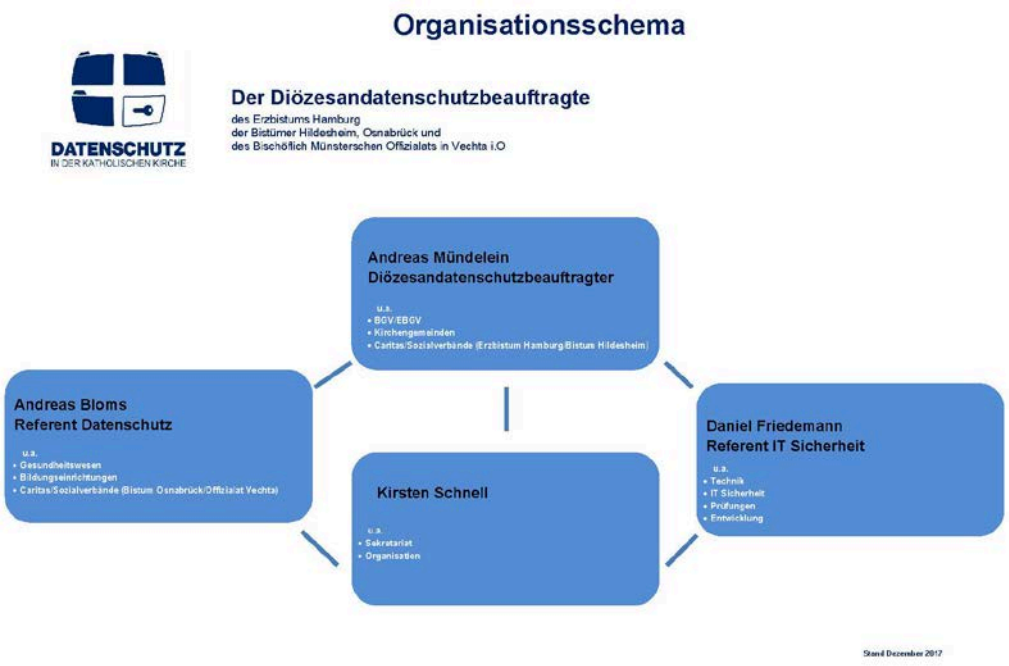
Die Finanz- und Budgethoheit liegt beim Diözesandatenschutzbeauftragten. Die Abwicklung des Haushaltes erfolgt über die Finanzabteilung des bischöflichen Generalvikariates Osnabrück als Belegenheitsbistum für die Stadt Bremen.

Der Haushalt des Diözesandatenschutzbeauftragten ist im Bistumshaushalt des Bistums Osnabrück als eigene Haushaltsstelle veranschlagt.

4.3 Personal

Neben dem Beauftragten stehen seit Herbst des vergangenen Jahres ein weiterer Volljurist, ein IT – Techniker und eine Sekretariatskraft (derzeit 19,5 Stunden) zur Verfügung. Bis zum Jahresbeginn 2018 war befristet ein Volljurist im Büro der Datenschutzaufsicht tätig.

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



4.4 Vertretung in Konferenzen und Arbeitsgruppen

Der Leiter der Datenschutzaufsicht Nord 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.
- AG Datenschutz und Meldewesen des Verbandes der Diözesen Deutschlands (ab Januar 2018)
- Unterarbeitsgruppe der AG Datenschutz des VDD zur Entwicklung der KDO
- AK "Anwendung der KAO"
- IT – Workshop für betriebliche Datenschutzbeauftragte, 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

4.5 Vernetzung

Im Berichtszeitraum sind Kontakte aufgebaut und Gespräche mit den Landesbeauftragten für den Datenschutz und Informationsfreiheit in Bremen, Niedersachsen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein 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 für das neue Berichtsjahr geplant und in Vorbereitung.

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

Der kirchliche Datenschutz ist im Umbruch.

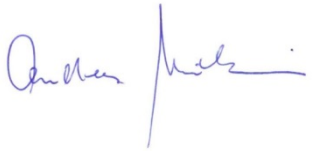
Das neue KDG ist beschlossen und wird zu Beginn des nächsten Jahres von den (Erz-)Bischöfen der norddeutschen Diözesen in Kraft gesetzt und in den jeweiligen Amtsblättern veröffentlicht.

Die Aussicht darauf führt schon jetzt zu vielen Anfragen, Bedenken und teilweise auch zu Beunruhigungen bei den kirchlichen und caritativen Einrichtungen.

Gemeinsam mit den Verantwortlichen in den Diözesen ist die Datenschutzaufsicht bemüht, den Sorgen und Bedenken der Einrichtungen und deren Mitarbeiter Rechnung zu tragen. Mit der strukturellen Anpassung des Datenschutzes in der Fläche der Bistümer (Einsatz von betrieblichen Datenschutzbeauftragten) und der Unterstützung, Information und Hilfestellung durch die Aufsichtsbehörde im Rahmen ihrer gesetzlichen Aufgabenstellung, werden konkrete Schritte unternommen, die Verantwortlichen und Mitarbeiter in den Einrichtungen auf das neue Gesetz bis Mai 2018, und darüber hinaus, vorzubereiten und mitzunehmen.

Die erforderlichen Rahmenbedingungen sind geschaffen oder in der Vorbereitung. Das bischöfliche Gesetz einzuhalten ist eine Selbstverständlichkeit. Bei Beachtung der notwendigen Sensibilität für das Recht auf informationelle Selbstbestimmung derjenigen, deren personenbezogene Daten im kirchlichen Kontext verarbeitet werden, besteht grundsätzlich kein Anlass, mit Sorge auf die Einführung des neuen kirchlichen Datenschutzgesetzes zu blicken.

Bremen, 15. März 2017



Andreas Mündelein

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

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

Tel.: 0421 / 16 30 19 25
Mobil: 0151 / 41 97 57 58
Mail: info@datenschutz-katholisch-nord.de
Internet: https://datenschutz-kirche.de