Der Diözesandatenschutzbeauftragte

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

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

3. Jahresbericht 2016

Herausgegeben vom

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

Schwachhauser Heerstraße 67
28211 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/

3. Jahresbericht

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

für das Jahr 2016

vorgelegt im Januar 2017

Stand 31.12.2016

Inhaltsverzeichnis

Vorwort

Datenschutz geht uns alle an.

Es vergeht kaum ein Tag an dem nicht wenigstens eine Meldung im Zusammenhang mit Datenschutzthemen um die Welt geht. Von Whistleblower über Videoüberwachung bis hin zu Hackerangriffen und gezielte Wahlkampfbeeinflussung. Dabei ist das Problem nicht ausschließlich globaler Natur. Auch jeder Einzelne, sei es durch die Teilnahme an der stetig zunehmenden Welt des Internets oder durch die notwendige Inanspruchnahme unterschiedlicher Dienste, ist bewusst oder unbewusst von der Gefährdung seiner Privatsphäre durch das Sammeln und Nutzen seiner personenbezogenen Daten betroffen.

Auf europäischer Ebene ist nach langen Entstehung - und Entscheidungsprozessen durch ein nunmehr für alle Mitgliedstaaten verbindliches Datenschutzrecht dem grundrechtlichem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Rechnung getragen worden (Europäische Datenschutz – Grundverordnung).

Auch die katholische Kirche nimmt die Verantwortung für die Daten und Informationen, die ihr zur Wahrnehmung der kirchlichen und caritativen Aufgaben zur Verfügung gestellt oder von ihr erhoben werden, wahr. Das Bewusstsein im Rahmen dieser Verantwortung zu handeln ist in der katholischen Kirche und ihren Einrichtungen aus dem Schattendasein hervorgetreten und wird zunehmend als wichtiger Faktor im Ablauf ihrer Aufgabenerfüllung gesehen.

Die kirchliche Datenschutzaufsicht wurde mit Beginn des Berichtzeitraums neu strukturiert und hat ihren Sitz in Bremen. Die Zuständigkeit umfasst seitdem die Gebiete des Erzbistums Hamburg, die der Bistümer Osnabrück und Hildesheim und das des Offizialatsbezirk Vechta in Oldenburg.

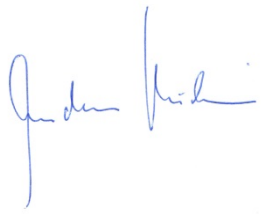
Die Wahrnehmung der Datenschutzaufsicht erfolgt durch den Diözesandatenschutzbeauftragten. Dieser wacht über die Einhaltung der kirchlichen Datenschutzvorschriften und der anderen Vorschriften über den Datenschutz. Neben der Aufsicht ist die Beratung der bischöflichen Behörden

und kirchlichen Dienststellen, aber auch die Weiterbildung von betrieblichen Datenschutzbeauftragten, Aufgabe und Anliegen der Datenschutzaufsicht. Der Austausch und die Zusammenarbeit mit anderen Diözesanbeauftragten, den Datenschutzbeauftragten der evangelischen Kirche und den Landesdatenschutzbeauftragten ist dabei nicht nur eine Verpflichtung, sondern auch eine große Hilfe um ein einheitliches Datenschutzrechtsniveau für die Kirchen zu entwickeln.

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

Nachstehend lege ich meinen Tätigkeitsbericht für das Jahr 2016 vor. Neben einer zusammengefassten Darstellung der Entwicklung des Datenschutzrechtes auf europäischer und kirchlicher Ebene möchte ich exemplarisch auf wesentliche Vorkommnisse in dem Berichtszeitraum hinweisen, die von allgemeiner Bedeutung für die Dienststellen in meinem Tätigkeitsbereich sein können. Mit der Berichterstattung über die aktuelle Entwicklung der Dienststelle in Bremen beschließe ich den Jahresbericht.

Bremen, im Januar 2017



Andreas Mündelein
Diözesandatenschutzbeauftragter

1. Die Entwicklung des Datenschutzrechts

1.1 Europarecht

1.1.1 Die Europäische Datenschutzgrundverordnung

Nach fast vierjähriger Debatte haben sich der Europäische Rat, das Europäische Parlament und die Europäische Kommission über den endgültigen Inhalt der neuen EU-Datenschutz-Grundverordnung geeinigt. In Kraft treten soll die neue Verordnung im Mai 2018 und die bereits seit 1995 geltende EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) ersetzen. Die EU-Datenschutz-Grundverordnung (EU-DSGVO) ist am 14. April 2016 durch das EU-Parlament beschlossen worden. Damit endet die seit 2012 andauernde Gesetzgebungsphase für die EU-DSGVO, die das Datenschutzrecht europaweit reformiert. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten. Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist. Inhaltlich besonders bedeutsam für die Kirche ist Art. 91 (früh. Art.85) EU-DSGVO der neuen Verordnung. Er bestimmt Folgendes:

Artikel 91

Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

1. *Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.*

2. *Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht durch eine unabhängige Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.*

Im Ergebnis führt die Regelung dazu, dass die EU-DSGVO nicht unmittelbar auf kirchliche Stellen anwendbar ist. Den öffentlich-rechtlich organisierten Religionsgesellschaften bleibt ihr durch die Verfassung gewährleistetes Selbstverwaltungsrecht auch in Datenschutzbelangen erhalten. Das gilt nur dann,

wenn die KDO bei Inkrafttreten der Datenschutz-Grundverordnung 2018 „umfassende Regeln“ zum Schutz natürlicher Personen bei der Datenverarbeitung enthalten, die in allen wesentlichen Punkten mit der sehr umfangreichen Datenschutzgrundverordnung der Europäischen Union „gleichwertig“ ist.

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 Vertrag zuvor. Jetzt hat die Artikel 29-Gruppe der Datenschützer der EU, unter Vorsitz der französischen Datenschutzbeauftragten Isabelle Falque-Pierrotin das Abkommen als mit dem Europäischen Datenschutzrecht vereinbar anerkannt, wobei jedoch in einem Jahr eine weitere Prüfung anhand der bis dahin gemachten Erfahrungen durchgeführt werden soll. In dem Abkommen hat die USA zugesagt, dass Kontrollen nur in sehr engen Grenzen durchgeführt werden sollen. Ab dem 1. August dieses Jahres können sich Firmen bescheinigen lassen, dass sie den Festsetzungen dieses Vertrages Folge leisten werden. Nur mit diesen Unternehmen kann ein rechtssicherer Datenaustausch stattfinden. Problematisch ist allerdings immer noch, dass EU-Bürger praktisch keine Rechte haben, sich gegen eine fehlerhafte Datenverarbeitung zu wehren.

1.2 Bundesrecht

1.2.1 Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

Im Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein.

Die Verordnung enthält Öffnungsklauseln für den nationalen Gesetzgeber und konkrete Regelungsaufträge an die Mitgliedsstaaten. Daraus ergibt sich ein gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht.

Darüber hinaus dient der Entwurf der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Es ist daher erforderlich, das bisherige Bundesdatenschutzgesetz durch ein neues Bundesdatenschutzgesetz abzulösen.

Der Entwurf des Gesetzes befindet sich in der Verbändeanhörung. Die Kabinettbefassung ist noch für den Januar 2017 vorgesehen, damit die Gesetzesänderung noch in der laufenden Legislaturperiode abgeschlossen werden kann.

Für die kirchliche Datenschutzaufsicht von besonderer Bedeutung ist der § 30 Abs. 1 S.4 des Entwurfes des Anpassungsgesetzes. Dieser sieht vor, dass die Aufsichtsbehörden des Bundes und der Länder die kirchlichen Aufsichtsbehörden beteiligen, sofern diese von der Angelegenheit betroffen sind. Die Begründung dazu sieht vor, dass die Stellungnahmen der spezifischen Aufsichtsbehörden (Art. 91 Abs. 2 EU-DSGVO) bei der Festlegung eines gemeinsamen Standpunktes zu berücksichtigen sind. Damit ist auch zukünftig die Beteiligung der kircheneigenen

Datenschutzaufsicht nicht in das Belieben der Akteure gestellt, sondern hat eine klare gesetzliche Regelung.

1.2.2 Änderung im Telekommunikationsgesetz

Am 28.07.2016 ist eine Änderung des Telemediengesetzes (TMG) in Kraft getreten. Danach wird die bisher nur für Festnetzbetreiber oder Hoster unter bestimmten Umständen geltende Haftungsbefreiung auch auf Anbieter freier WLANs ausgeweitet. Nach dem neuen § 8 Abs. 3 TMG gelten die Absätze 1 und 2 (der Norm) auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

Das Haftungsprivileg umfasst dabei alle „fremde Informationen“, deren Übermittlung vom Anbieter nicht veranlasst worden ist und er die Adressdaten der übermittelten Informationen nicht ausgewählt oder gar verändert hat. Somit soll in Zukunft die Einrichtung freier WLANs, die ohne Zugangsbeschränkung von jedermann genutzt werden können, erleichtert werden.

Das TMG schützt aber nicht ausdrücklich vor einer zivilrechtlichen Inanspruchnahme durch Abmahnungen von Seiten der Rechteinhaber, die beim Download von Musikdateien, Filmen oder Fotos ihr Urheberrecht verletzt sehen.

Zwar sieht die Gesetzesbegründung vor, dass die Haftungsprivilegierung des Diensteanbieters nach § 8 Absatz 1 und 2 TMG uneingeschränkt auch die verschuldensunabhängige Haftung im Zivilrecht nach der sog. Störerhaftung umfasst, und daher keine Verurteilung des Vermittlers zur Zahlung von Schadenersatz, und ebenfalls keine Verurteilung zur Tragung der Abmahnkosten und der gerichtlichen Kosten im Zusammenhang mit der von einem Dritten durch die Übermittlung von Informationen begangenen Rechtsverletzung erfolgt.

Im Wortlaut des Gesetzestextes ist diese Auffassung aber nicht umgesetzt worden. Trotzdem haben die Gerichte bei der Auslegung von Gesetzesvorschriften auch die Absichten und Ziele des Gesetzgebers in ihre Entscheidungen mit einzubeziehen (teleologische Auslegung). Es bleibt also abzuwarten, ob die Rechtsprechung der Gesetzesbegründung folgen wird.

1.3 Datenschutzrecht der Kirche

1.3.1 Anordnung über den kirchlichen Datenschutz (KDO)

Bereits mit Datum vom 18. November 2013 hat die 151. Vollversammlung des Verbandes der Diözesen Deutschlands Änderungen der §§ 2a, 3 Abs. 5 und Abs.6, 3a Abs.3, 8 Abs. 2 sowie der §§ 15 ff KDO beschlossen, nachdem schon die Einführung des § 10 a (Beschäftigungsdatenschutz) KDO beschlossen worden war.

Aus Gründen der notwendigen Einheitlichkeit des kirchlichen Datenschutzes haben die Diözesen die aktuelle Version in Kraft gesetzt.

Eine Arbeitsgruppe auf der Ebene des VDD ist derzeit intensiv mit der Anpassung der KDO an die EU – DSGVO befasst. Die Arbeitsgruppe hat den Auftrag, unter Einbeziehung des Katholischen Büros in Berlin die Beratungen hinsichtlich einer an den Regelungen der EU-Datenschutz-Grundverordnung und dem nationalen Anpassungsgesetz orientierten Novellierung der KDO einschließlich Rechtsweg fortzusetzen und im Frühjahr 2017 den Diözesen einen ersten Entwurf zur Beratung vorzulegen.

Die Vorbereitung des Auftrages der genannten Arbeitsgruppe leistet eine sehr engmaschig tagende Unterarbeitsgruppe, die aus Diözesanjuristen, Mitarbeitern der katholisches Büros und Datenschutzbeauftragten besteht. Bis Anfang März soll die Unterarbeitsgruppe ihre Tätigkeit beendet haben.

Eine enge Abstimmung mit der evangelischen Kirche ist durch eine gegenseitige Beteiligung an einer vergleichbaren Arbeitsgruppe des Kirchenamtes der EKD zur Anpassung des DSG – EKD an die EU-DSGVO gewährleistet.

1.3.2 Durchführungsanordnung zur KDO (KDO-DVO)

Nach der aktualisierten KDO (18.11.2013) treffen die Generalvikare gem. § 22 KDO die zur Durchführung der KDO erforderlichen Regelungen.

In diesem Zusammenhang sind die technischen und organisatorischen Maßnahmen gem. § 6 S. 1 KDO festzulegen, die kirchliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, zu treffen haben, um die Ausführungen der Vorschriften der KDO zu gewährleisten.
Die entsprechenden Maßnahmen sind in den Anlagen zu § 6 KDO in einer jeweils überarbeiteten Form enthalten und in Kraft gesetzt worden (vergleichbare Datenschutzstandards des IT – Grundschutzkataloges des BSI).

Inhaltlich sind dies neben der Anpassung des Einleitungssatzes zu § 3a KDO – DVO - anstelle des bisher geltenden § 19 KDO der seit dem Stand 18.11.2013 geltende § 22 KDO - die angepassten Richtlinien zum Einsatz von Arbeitsplatzcomputern (APC – Richtlinien) und die IT – Richtlinien.

1.3.3 Anordnung über das kirchliche Meldewesen (KMAO)

Nach Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 22.06.2015 zu § 5 der Anordnung über das kirchliche Meldewesen (KMAO) ist auf den Diözesanebenen eine Anpassung bzw. Ergänzung notwendig. Dabei geht es im Wesentlichen um die Schaffung einer Rechtsgrundlage, damit die Bistümer Daten, die Gemeindemitgliederverzeichnisse anderer Bistümer betreffen und die sie seitens einer kommunalen Meldebehörde aus technischen oder organisatorischen Gründen erhalten haben, an die betroffenen Bistümer weiterleiten können. Die Umsetzung ist erfolgt.

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.

Deshalb sind betriebliche Datenschutzbeauftragte für die kirchlichen Einrichtungen, auch in der Fläche, zu berufen. Die Pflicht betriebliche Datenschutzbeauftragte in kirchlichen Einrichtungen zu benennen ergab sich bisher aus § 20 KDO, soweit mehr als 10 Personen mit der automatisierten Erfassung, Verarbeitung oder Nutzung von Daten befasst sind. Die in § 20 KDO genannte „Sollvorschrift“ ist dabei nach einhelliger Ansicht aller Juristen als eine „Mussvorschrift“ zu bewerten. Unabhängig davon war die Erfüllung der Aufgaben eines betrieblichen Datenschutzbeauftragten, wenn weniger als regelmäßig 11 Personen mit der automatisierten Erfassung, Verarbeitung oder Nutzung von Daten befasst sind, in anderer Weis durch die Generalvikare zu regeln (§§ 20 Abs. 9 i.V.m. 22 lit. d KDO)

Mit der EU-DSGVO (Art. 37 EU-DSGVO) ergibt sich die Notwendigkeit betriebliche Datenschutzbeauftragte zu benennen noch einmal unter neuen Gesichtspunkten. Eine Differenzierung nach der Anzahl der mit der automatisierten Erfassung, Verarbeitung oder Nutzung von Daten befassten Personen ist in der Verordnung nicht mehr vorgesehen. Nach Art. 37 Abs. 1. lit. .c ist auf jeden Fall ein betrieblicher Datenschutzbeauftragter zu berufen, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 EU-DSGVO besteht. Dabei handelt es sich um besonders sensible Daten wie religiöse und weltanschauliche Überzeugungen. Der Bedarf an betrieblichen Datenschutzbeauftragten wird durch die EU-DSGVO deshalb nicht geringer, sondern höher.

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.

Im Hinblick auf die Benennung von betrieblichen Datenschutzbeauftragten für kirchliche Einrichtungen in der Fläche ist ein mit den Diözesen und dem Offizialatsbezirk abgestimmtes Verfahren vereinbart worden, das zum Ziel hat den betrieblichen Datenschutz im Laufe des nächsten Berichtszeitraums zu organisieren.

2.2 Kirchliche Datenschutzaufsicht

Die kirchliche Datenschutzbehörde muss nach Art. 91 Abs. 2 EU-DSGVO die in Kapitel IV niedergelegten Bedingungen erfüllen (Art. 51 – Art. 59 EU-DSGVO).
Die Anforderungen an die Unabhängigkeit sind in Art. 52 EU-DSGVO geregelt. Die Berufung des Datenschutzbeauftragten muss in einem transparenten Verfahren erfolgen (Art. Abs. 1 EU-DSGVO).

Art.52 Abs. 4 EU-DSGVO, der über Art 91 Abs. 2 EU-DSGVO auch im kirchlichen Bereich umgesetzt werden muss regelt,

„Jeder Mitgliedstaat stellt sicher, 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.“

Diese Sicherstellungsverpflichtung der Diözesen umfasst somit die personellen, technischen und finanziellen Ressourcen (vgl. Fachet, Jahresbericht 2016).

Die unter Art. 57 EU-DSGVO gelisteten (Mindest)Aufgaben beschreiben einen Großteil der Aufgabengebiete, die auch von der kirchlichen Datenschutzaufsicht zu leisten sind. Das Aufgabenprofil macht es erforderlich, über die personelle Ausstattung der Datenschutzaufsicht konstruktiv nachzudenken.

Das neu errichtete katholische Datenschutzzentrum in Dortmund ist für die nordrhein-westfälischen Bistümer mit insgesamt 10 Vollzeitstellen konfiguriert. Die geplante Datenschutzaufsicht für die südwestlichen Bistümer, die ihren Sitz in Frankfurt haben soll, wird mit 5 Vollzeitstellen geplant. Die bayrische Datenschutzaufsicht, derzeit 3 Vollzeitstellen, soll um weitere 2 Vollzeitstellen aufgestockt werden. Im Bereich der ostdeutschen und norddeutschen Bistümer,

besteht die Datenschutzaufsicht im Wesentlichen aus den Beauftragten und jeweils einer halben Sekretariatskraft, bzw. für den Nordbereich aus einem zusätzlichen Mitarbeiter.

Angesichts des vorerwähnten Aufgabentableaus wird im Laufe des nächsten Berichtszeitraums mit den Beteiligten über eine angemessene Ausweitung der personellen Situation zu sprechen sein.

3. Exemplarische Darstellung von Einzelfällen

3.1 Beratungen

Im Laufe des Berichtszeitraums wurde die Datenschutzaufsicht mit ca. 120 schriftlichen und teilweise komplexen Anfragen befasst, die einen umfangreichen Schriftverkehr notwendig gemacht haben. Unabhängig davon hat die telefonische Beratung bei dringenden Fragen sowohl von Verantwortlichen als auch von Betroffenen im Laufe des Jahres deutlich zugenommen. Die Sensibilität für den Datenschutz scheint, was als gutes Zeichen werten ist, deutlich zuzunehmen.

Nachstehend werden einige ausgesuchte Beratungsanfragen dargestellt:

3.1.1 Streaming von Gottesdiensten

Das Kunsturhebergesetz erlaubt die Übertragung, auch ohne Einwilligung der Betroffenen, wenn es sich um eine allgemeine Veranstaltung handelt, an der die abgebildete Person teilnimmt. Dabei muss es für alle Teilnehmer erkennbar sein, dass diese Veranstaltung aufgenommen und gestreamt wird. Der Unterschied zu großen Veranstaltungen (Bsp. Kirchentagsgottesdienste) besteht gegenüber einem Gemeindegottesdienst darin, dass diese Tatsache hierbei von den Teilnehmern allgemein erwartet wird und aus diesem Grunde keines besonderen Hinweises bedarf. Bei einzelnen Gemeindegottesdiensten ist die Tatsache der Aufnahme und Übertragung nicht so offensichtlich. Deshalb sollte in diesen Fällen ein deutlicher Hinweis erfolgen.

Ein Hinweis, die Aufnahmen nur auf einen bestimmten Teil der Kirche zu beschränken, ist ein Entgegenkommen an all diejenigen, die mit der Verbreitung ihrer Bilder Probleme haben, aber trotzdem am Gottesdienst teilnehmen wollen. In dem Hinweis kann angegeben werden, dass „Nur der vordere Teil des Mittelschiffs im Aufnahmebereich liegt.“ Diese Handhabung dürfte Beschwerden der Teilnehmer deutlich reduzieren.

3.1.2 Einsatz externer E- Mail Adressen

Sofern die E-Mail-Adressen von einem anderen (Bsp. Arbeitgeber) stammen, ist zu berücksichtigen, dass im Falle einer E-Mail-Weiterleitung oder bei Zugriffsrechten in das Postfach, beispielsweise von Kollegen, Dritte Kenntnis von der Kommunikation nehmen können. Darüber hinaus besteht die Möglichkeit, dass die E-Mails im Archivierungssystem des anderen langfristig gespeichert werden.

Bei der Verwendung von öffentlichen Webmailing-Diensten kann nicht ausgeschlossen werden, dass Dritte (z. B. durch Kenntnis der Zugangsdaten oder bei der Wahl eines unsicheren Passwortes) von den Inhalten der Kommunikation Kenntnis nehmen.

Bei E-Mail-Adressen, die nicht der Domäne des Bistums angehören, sollte ein Hinweis aufgenommen werden, dass es sich hier um externe E-Mail-Adressen handelt, die Datensicherheit nicht durch das BGV zentral administriert wird und eine Vertraulichkeit nicht gewährleistet werden kann.

3.1.3 Umgang (Löschen) mit personenbezogenen Daten in einer Kindertagesstätte

Die Löschung gespeicherter personenbezogener Daten erfolgt, wenn ihre Kenntnis zur Erfüllung des mit der Speicherung verfolgten Zwecks nicht mehr erforderlich ist, oder wenn ihre Speicherung aus sonstigen gesetzlichen Gründen unzulässig ist, es sei denn gesetzliche Aufbewahrungsvorschriften sprechen gegen eine Löschung, dann tritt an Stelle der Löschung eine Sperrung der Daten.

Eine "Löschung" von personenbezogenen Daten in Akten wird in der kirchlichen Datenschutzanordnung nicht geregelt. Akten, bei denen der zugrundeliegende Verwaltungsvorgang endgültig abgeschlossen ist, sind auszusondern und üblicherweise zuverlässig zu vernichten.

Der Träger hat die Aufbewahrungsfristen unter Beachtung der einschlägigen Bestimmungen festzulegen. Zulässig ist es durchaus, verschieden lange Aufbewahrungsfristen festzulegen z. B. für Stammdaten,

Versicherungsunterlagen, Anwesenheitslisten, Gebührenunterlagen. Wenn das Kind den Kindergarten endgültig verlassen hat, kann sich eine unterschiedlich lange Aufbewahrung der verschiedenen Unterlagen zwischen 3 und 10 Jahren datenschutzrechtlich noch rechtfertigen lassen. Ist mit Schadenersatzansprüchen zu rechnen bzw. sind diese zu befürchten, weil es zu einem Unfall kam, kann eine 30jährige Aufbewahrung der Akten datenschutzrechtlich noch unbedenklich sein, weil die allgemeine Verjährungsfrist des § 852 BGB 30 Jahre ist. Ansprüche aus Schadenersatz und Schmerzensgeld verjähren danach nach 30 Jahren, sonst nach 3 Jahren, sobald der Verletzte von dem Schaden und der Person der Ersatzpflichtigen Kenntnis erlangt hat.

Die im Zusammenhang mit der Vereinbarung zur Medikamentengabe erfassten Daten sind ebenfalls personenbezogene Angaben. Die für den Zweck der Medikamentengabe erforderlichen Daten müssen beim Betroffenen selbst erhoben werden. Aufgrund des Alters der die Kindertagestätten besuchenden Kinder handeln in der Regel die Personensorgeberechtigten für das Kind.

Bei Dritten, z.B. bei einem Arzt, dürfen Daten über das Kind grundsätzlich nur erhoben werden, wenn das Kind oder seine Personensorgeberechtigten ihre Einwilligung in die Datenerhebung geben haben.

Diese Unterlagen sind für den Zeitraum von 30 Jahren zu archivieren. Es empfiehlt sich, diese Dokumente in regelmäßigen Abständen digital zu sichern (z.B. eingescannt auf einem Datenträger).

3.1.4 Veröffentlichung von Pfarrbriefen im Internet

Ein normaler Pfarrbrief darf in der Regel nicht im Internet veröffentlicht werden, weil der Kreis der Nutzer nicht auf den Bereich der Kirchgänger oder Gemeindeangehörigen begrenzt ist, sondern weltweit einsehbar ist. Grundsätzlich sollten personenbezogene Daten, und um die geht es ja in den Pfarrbriefen, möglichst zurückhaltend veröffentlicht werden, und wenn, dann nur mit Zustimmung der betreffenden Personen.

Bei einer im Internet nachlesbaren Veröffentlichung bedarf es zur rechtssicheren Handhabung im Einzelfall deshalb immer einer schriftlich Erklärung, dass der Betroffene mit der Bekanntgabe seines Namens einverstanden ist. Zum Schutz und zur Sicherheit für die Betroffenen dürfen ohne ausdrückliche schriftliche Einwilligung auch keine Anschriften veröffentlicht werden. Die Betroffenen müssen in jedem Fall darum wissen und widersprechen können.

3.1.5 Der Krankenhausbesuchsdienst

Weitergabe von Patientendaten an Ehrenamtliche Klinikbesucher

Der Krankenhausbesuchsdienst ist eindeutig verfassungsrechtlich geregelt.

(Art 140 GG i.V.m. Art. 141 WRV)

Soweit das Bedürfnis nach Gottesdienst und Seelsorge im Heer, in Krankenhäusern, Strafanstalten oder sonstigen öffentlichen Anstalten besteht, sind die Religionsgesellschaften zur Vornahme religiöser Handlungen zuzulassen, wobei jeder Zwang fernzuhalten ist.

Ein Krankenhaus darf (muss) daher die Religionszugehörigkeit des Patienten abfragen, wobei auf die Freiwilligkeit dieser Angabe hinzuweisen ist. Darüber hinaus ist bei dem Patienten eine Einwilligungserklärung für die Weitergabe an den zuständigen Krankenhausseelsorger einzuholen. Hierdurch wird die Verpflichtung „jeden Zwang fernzuhalten“ eingehalten.

Nach dem Niedersachsenkonkordat (Niedersachsenkonkordat (Nds GVBL 1965, S.191), Art.11 ist geregelt:

„In Krankenhäusern,……..werden die zuständigen katholischen Geistlichen im Rahmen der allgemeinen Hausordnung zur Vornahme seelsorglicher Besuche und kirchlicher Handlungen zugelassen“,

Deshalb benennt der Diözesanbischof für die öffentlichen Anstalten (u.a. Krankenhäuser) hauptberufliche Klinikseelsorger.

Dann, wenn die Patienten eine freiwillige Einwilligung gegeben haben, haben diese das Recht den Namen des Patienten, seine Station und gegebenenfalls die

Dauer seines Aufenthaltes zu erfahren. Die Weitergabe erfolgt an die speziell für die Krankenhausseelsorge ausgebildeten Seelsorger. Die Weitergabe von Patientendaten an Dritte, durch die hauptamtlichen Seelsorger, kann gegebenenfalls ein Verstoß gegen die im Krankenhaus geltenden Verschwiegenheitspflichten bedeuten.

Nach der für die katholische Kirche geltenden Anordnung über den kirchlichen Datenschutz ist die Erhebung , Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit diese Anordnung oder eine kirchliche oder staatliche Rechtsvorschrift dies vorsieht – was aber für Patientendaten in öffentlichen Krankenhäusern nicht der Fall ist -, oder, wenn der Betroffene eingewilligt hat.
Die Weitergabe der Daten des Patienten über den Klinikseelsorger an die Pfarrgemeinde des Patienten, und darüber an den ehrenamtlichen Besuchsdienst, ist deshalb nur zulässig, wenn der Patient auch in diese Übermittlung ausdrücklich eingewilligt hat.

Es obliegt der Professionalität der Klinikseelsorger die ehrenamtlichen Besuchsdienste, da wo es vertretbar ist, sinnvoll in die Begleitung der Patienten, die dies wollen, einzubinden. Ein selbständiges Recht eines ehrenamtlichen Besuchsdienstes auf Übermittlung personenbezogener Daten besteht in keiner Weise.

3.1.6 Freies WLAN

Mit der am 28.07.2016 eingetretenen Änderung des Telemediengesetzes (TMG) wird die bisher nur für Festnetzbetreiber oder Hoster unter bestimmten Umständen geltende Haftungsbefreiung auch auf Anbieter freier WLANs ausgeweitet (vgl. § 8 Abs. 3 TMG). Das Haftungsprivileg umfasst dabei alle „fremde Informationen“, deren Übermittlung vom Anbieter nicht veranlasst worden ist und er die Adressdaten der übermittelten Informationen nicht ausgewählt oder gar verändert hat.

Somit soll in Zukunft die Einrichtung freier WLANs, die ohne Zugangsbeschränkung von jedermann genutzt werden können, erleichtert werden.

Die Beschränkung der Haftung umfasst insoweit jede Form der Haftung für rechtswidriges Verhalten jeder Art durch den Nutzer des freien WLAN. Das gilt für die straf-, verwaltungs- und zivilrechtliche Haftung sowie für die unmittelbare und mittelbare Haftung für Handlungen Dritter.

Demgegenüber schützt das TMG den WLAN - Betreiber aber nicht ausdrücklich vor einer zivilrechtlichen Inanspruchnahme durch Abmahnungen von Seiten der Rechteinhaber, die beim Download von Musikdateien, Filmen oder Fotos ihr Urheberrecht verletzt sehen.

Eine jüngste Entscheidung des EuGH (Europäischer Gerichtshof) hat nun Auslegungshilfen für diejenigen europäischen Normen getroffen, auf denen auch die deutschen Regelungen im Hinblick auf einen Haftungsausschluss von WLAN – Anbietern im TMG beruhen. Ob eine Umsetzung dieser Grundzüge durch deutsche Gerichte erfolgen wird, bleibt abzuwarten. Eine Inanspruchnahme des WLAN – Betreibers, zumindest dann, wenn er das freie Netz nicht Password geschützt anbietet, im Rahmen von strafbewährten Unterlassens Verfügungen, ist den Kommentierungen nach aber gleichwohl nicht ausgeschlossen.

Es besteht nach Auffassung des Gerichts die Möglichkeit, dass ihm auf Antrag des Geschädigten durch innerstaatliche Gerichte oder Behörden aufgegeben wird, durch Schutzmaßnahmen dafür zu sorgen, solche Rechtsverletzungen künftig zu verhindern. Insoweit können bei einem Verstoß auch Abmahn- und Gerichtskosten geltend gemacht werden.

3.1.7 Weitergabe eines PC Passwortes auf Anforderung der Leitung

Weder muss noch darf ein Passwort weitergeben werden Der Zugang zu einem persönlichen APC Rechner ist ausschließlich personenbezogener Art.

Nach § 6 KDO (Anordnung über den kirchlichen Datenschutz i.d.Fassung v.18.11.2013) haben kirchliche Stellen i. S. d. § 1 Abs. 2 KDO die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften der KDO zum Schutz von personenbezogenen Daten zu gewährleisten.

Die Durchführungsverordnung der KDO (vgl. IV. Anlage 1 zu § 6 KDO – DVO, i.d.F.v. 19.03.2015) stellt dazu klar, dass bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten die innerbetriebliche Organisation so zu gestalten ist, dass sie den Anforderungen des Datenschutzes gerecht wird. Dazu sind u.a. Maßnahmen zu treffen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsmäßige Ausübung seiner Tätigkeit (vgl. Anlage 2, 3.1 zu § 6 KDO – DVO). Die zur Umsetzung von IV. Anlage 2 zu § 6 KDO – DVO erlassene IT – Richtlinie (i.d.F. v. 19.03.2015) regelt unter 2.1 IT – Richtlinie, dass die Anmeldung am APC nur nach Eingabe eines „benutzerdefinierten“ Kennworts möglich sein darf.

Aus der Tatsache, dass der Zugang ausschließlich durch ein benutzerdefiniertes Passwort möglich sein darf, ergibt sich rechtlich zwingend, dass die Weitergabe des Passwortes unzulässig ist, weil nicht ausgeschlossen werden kann, dass das Datenverarbeitungssysteme von Unbefugten oder vermeintlich Befugten genutzt werden könnte. Es ist dabei unerheblich wer das Passwort begehrt, denn zuständig für die Datensicherheit ist jeder Mitarbeiter selbst.

Sollte die Leitung die Notwendigkeit sehen, auf einen APC Zugriff nehmen zu müssen, wäre dies nur über ein Admin - System - Passwort möglich, wobei dann tatsächlich nachweisbar wäre, dass nicht der Rechteinhaber, oder ein Unbefugter mit seinem Passwort, auf seinem Rechner gearbeitet haben, sondern der Administrator des Systems mit besonderen Rechten.

3.1.8 Zulässigkeit einer Videoüberwachung in der Kapelle eines Krankenhauses

Nach Mitteilung des Krankenhauses sind in der Zeit von Dezember 2015 bis aktuell März 2016 diverse Diebstähle vorgekommen, die sich im Wesentlichen auf die am oder auf dem Altar befindlichen Schmuckgegenstände bezogen haben. Daraus ist der Schluss zulässig, dass es sich nicht nur um eine abstrakte oder theoretische Gefahr handelt, sondern die Gefahr weiterer Diebstähle offensichtlich konkret vorhanden ist. Mit der Installation der Videoanlage und de

entsprechenden Hinweis darauf sollen potentielle Diebe abgeschreckt bzw. ermittelt werden.

Eine Überwachung ist (u.a.) nur zulässig, wenn sie zur Wahrnehmung des Hausrechts erforderlich ist. Dies wird jedenfalls für solche Räume angenommen, wo eine konkrete Sicherheitsgefahr besteht, aber auch nur dann, wenn diese mit einem Kameraeinsatz reduziert oder zumindest gebannt werden kann. Die Gefahr muss dabei konkret bestehen und nicht nur abstrakt oder theoretisch vorhanden sein. Darüber hinaus sind die Relation eines Kameraeinsatzes auf der einen Seite und der Wert des zu schützenden Guts auf der anderen Seite (Grundrecht auf freie Religionsausübung) in ein ausgewogenes Verhältnis zu bringen.

Es dürfen keine Anhaltspunkte dafür bestehen, dass die schutzwürdigen Interessen der Betroffenen gegenüber dem Überwachungsinteresse überwiegen. Bei der Abwägung der Interessen muss eine pauschaliert verallgemeinernde Würdigung der zumeist gegenläufigen Interessen erfolgen.

Unter dem Gesichtspunkt des Sicherstellungsinteresses des Hausherrn vor dem Hintergrund der wiederholten Wegnahmen im Bereich der Kapelle könnten nach allgemeinem Verständnis die schutzwürdigen Interessen der Besucher der Kapelle hinter den Überwachungsinteressen zurückstehen.

Gleichwohl wird bei einer Videoüberwachung der Betroffene auch und insbesondere in seinem Grundrecht auf freie Religionsausübung durch die mangelnde Diskretion in Folge der Überwachung beeinträchtigt, bzw. der Betende kann sich beeinträchtigt fühlen. Mithin ist nicht auszuschließen, dass der Zweck des Kirchenraums im Sinne eines ungestörten und persönlichen Gesprächs mit Gott durch Menschen aller Art gestört wird. Infolge dessen sollte keine uneingeschränkte Überwachung eines Kirchenraumes vorgenommen werden, sondern in Abwägung aller Interessen nur dort überwacht werden, wo es zwingend notwendig ist und im Übrigen Räume zu lassen, wo ein unbeobachteter Bereich zum Gebet vorhanden ist.

Wenn also nur der Altarraum überwacht und gegebenenfalls außerhalb der Gottesdienste noch mit einer Absperrung versehen wird, somit also Räume zum

unbeobachteten Gebet bleiben, kann die Videoüberwachung zur Wahrung des Hausrechtes außerhalb der Gottesdienstzeiten zulässig sein.

Es ist eine Vorabkontrolle nach § 3 Abs. 5 und 6 KDO durchzuführen. Eine Inbetriebnahme der Überwachungsanlage ist erst nach ihrer Durchführung erlaubt. Die Datenspeicherung darf 74 Stunden nicht überschreiten. Die Zugangsrechte zu den Aufzeichnungen müssen beschrieben werden.

Zudem ist eine periodische Risikoanalyse erforderlich. Mit ihr sollen die tatsächlich vor der Überwachung eingetretenen Schäden mit denen, die seit Installation und Inbetriebnahme der Anlage passiert sind, verglichen werden. Von ihrem Ergebnis ist die Entscheidung, ob eine Videoüberwachung fortgesetzt wird, abhängig zu machen. Eine solche Bewertung sollte etwa ein Mal im Jahr stattfinden. Nur dann ist die Fortsetzung gerechtfertigt, wenn sie zum Erreichen des verfolgten Zwecks erheblich beiträgt (§ 5a Abs. 3 KDO). Dabei sind auch alle Anhaltspunkte, die zur Verletzung der schutzwürdigen Interessen der Betroffenen beitragen in jedem Fall zu beachten und dürfen das berechtigte Interesse der Einrichtung am Erfolg der Maßnahme nicht überwiegen.

3.1.9 Prüfungen

Nach § 18 Abs. 1 KDO wacht der Diözesandatenschutzbeauftragte über die Einhaltung dieser Anordnung sowie anderer Vorschriften über den Datenschutz. Dazu kann es erforderlich sein, dass die Datenschutzaufsicht auch ohne einen konkreten Anlass vor Ort in den Einrichtungen die Einhaltung der kirchlichen Datenschutzanordnung und anderer relevanten Regelungen überprüft.

Aus diesem Grund wurden zunächst für den Bereich der Kirchengemeinden, den Krankenhäusern sowie den Bildungseinrichtungen (Schulen) Prüfungsschemata entwickelt, die auch den Bereich der technischen und organisatorischen Maßnahmen (§ KDO/ KDO- DVO) beinhalten. Mit Hilfe der Schemata ist es nun möglich ein allgemein verbindliches Datenschutzniveau für alle zu prüfenden Einrichtungen zu Grunde zu legen und Vergleichsmaßstäbe für die Unterstützung der Einrichtungen auf dem Weg zur Datensicherheit zu gewinnen.

3.1.10 Schulen

Im Berichtszeitraum konnten zwei Schulen, nach Abstimmung mit der zuständigen Schulabteilung, besucht werden.

In beiden Einrichtungen war festzustellen, dass grundsätzlich eine hohe Datenschutzsensibilität vorhanden ist und die Bereitschaft besteht, die erforderlichen Maßnahmen zum Schutz der personenbezogenen Daten der Schüler, Eltern und Lehrer treffen zu wollen. Eher unterschiedlich waren die bisher umgesetzten Maßnahmen zum Schutz der entsprechenden Daten. Die bisherige Auswertung hat unter anderem ergeben, dass es dringend erforderlich ist den Schulen einen betrieblichen Datenschutzbeauftragten zur Seite zu stellen, der die verantwortliche Schulleitung unterstützt. Nur so kann gewährleistet werden, dass bei der Aufgabenvielfalt der Verantwortlichen trotz aller Vorsätze der erforderliche Datenschutz nicht ins Hintertreffen gerät. Der Schulträger hat bereits reagiert und einen für seine Schulen zuständigen betrieblichen Datenschutzbeauftragten benannt.

In Abstimmung mit diesem ist die Entwicklung eines Datenschutzkonzeptes für die Schulen des Schulträgers bis Mitte des nächsten Jahres vorgesehen. Im Anschluss kann eine erneute Überprüfung durch die Datenschutzaufsicht erfolgen.

3.1.11 Krankenhäuser

Aufgrund der Erfahrungen aus Prüfungen und Beratungen der letzten Jahre hat sich gezeigt, dass die Nutzung externer Dienstleister im Krankenhaus zunimmt was gleichzeitig eine Vielzahl von Problemen aus Datenschutzsicht aufwirft.

Werden externe Dienstleister an der Verwaltung von Patientenakten beteiligt (z.B. Digitalisierung, Archivierung, Entsorgung, Betrieb von IT-Systemen) so handelt es sich in der Regel um eine Auftragsdatenverarbeitung, für die nach § 8 KDO strenge Regeln vorgesehen sind. Weiterhin ist zu berücksichtigen, dass alle Patientendaten, die im Rahmen der Behandlung dem Arzt anvertraut worden sind, der Schweigepflicht nach § 203 StGB unterliegen.

Deshalb sind sie auch vor einer Beschlagnahme durch Strafverfolgungsbehörden nach § 97 StPO geschützt, aber nur solange, wie sie sich im Gewahrsam des Krankenhauses befinden.

Eine durch Krankenhäuser veranlasste Auftragsdatenverarbeitung muss also immer daran gemessen werden, ob durch sie die ärztliche Verschwiegenheit gewahrt wird.

Um einen Überblick über die Auftragsdatenverarbeitung in kirchlichen Krankenhäusern in katholischer Trägerschaft zu gewinnen, wurde darum gebeten einen eigens entwickelten Fragenbogen zu beantworten damit eine zentrale Auswertung durch die Datenschutzaufsicht erfolgen kann.

Von den 40 in katholischer Trägerschaft angeschriebenen Einrichtungen haben sich bis zum Jahresende 27 zurückgemeldet und die erforderlichen Unterlagen zur Verfügung gestellt. Die Einrichtungen, die bisher keine Reaktion gezeigt haben, werden noch einmal an die Rückgabe der notwendigen Unterlagen erinnert.

Die Gesamtauswertung der Unterlagen erfolgt sodann. Das Ergebnis wird im nächsten Jahresbericht veröffentlicht.

3.1.12 Fortbildungen

Neben der Aktualisierung und Erweiterung der angebotenen Arbeitshilfen für unterschiedliche Bereiche wurden in der Zeit von Mai bis Dezember des letzten Jahres auf Nachfrage von Krankenhäusern und caritativen Einrichtungen insgesamt neun Fortbildungsveranstaltungen am jeweiligen Standort der Einrichtung geplant und durchgeführt. Dabei hat sich herausgestellt, dass der Fortbildungsbedarf im Bereich des Datenschutzes insgesamt als sehr hoch eingeschätzt wird. Zukünftig könnte deshalb in diesem Bereich eine Schwerpunktbildung erfolgen, wenn entsprechende Personalressourcen dafür zur Verfügung stehen.

3.1.13 Beschwerden

Weitergabe eines Gemeindemitgliederverzeichnisses für eine personalisierte Wahlwerbung

Die Beschwerde erreichte die kirchliche Datenschutzaufsicht nach Klärung der Zuständigkeit durch die Landesbeauftragte für den Datenschutz in Niedersachsen. Die verantwortliche Stelle einer Kirchengemeinde hatte einem verdienten Gemeindemitglied die Daten zur Verfügung gestellt, damit er sich persönlich um Stimmen für seine Partei im Kommunalwahlkampf bei „seinen“ Kirchenmitgliedern bemühen konnte. um letztlich im kommunalpolitischem Raum auch die Interessen der katholischen Kirche vertreten zu können.

Dabei ist der Verantwortliche davon ausgegangen, dass letzteres, nämlich die Interessenvertretung im kommunalpolitischen Bereich durch das Gemeindemitglied einen kirchlichen Zweck darstellt, der eine Weitergabe von Adressdateien durch die Kirchengemeinde rechtfertigt.

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

Zweifelsfrei gehört es nicht zu den eigenen Aufgaben einer katholischen Kirchengemeinde einen Kandidaten im Wahlkampf aktiv zu unterstützen. Dies würde im Übrigen auch das grundgesetzliche Prinzip der Trennung von Staat und Kirche betreffen.

Entgegen den Vorstellungen des Verantwortlichen ist die Verwendung der Adressdaten in der dargestellten Form in keiner Weise von einem kirchlichen Zweck getragen, sondern diente allein dem Wahlinteresse des Kandidaten mit seiner Bitte um Unterstützung bei der Kommunalwahl. Weder hat der Kandidat die Daten insoweit für Gemeindezwecke zur Verfügung gestellt bekommen, noch hat er diese im Gemeindeauftrag genutzt. Auch wenn er die Absicht bekundet hat (auch) die Interessen der katholischen Kirchengemeinde vertreten zu wollen, ist dies kein kirchlicher Zweck, geschweige denn eine kirchliche Aufgabe, und daher als Rechtfertigung für die Weitergabe ersichtlich irrelevant.

Nach § 42 Abs. 5 BMG ist die Datenübermittlung an eine Religionsgemeinschaft nur zulässig, wenn beim Datenempfänger ausreichende Maßnahmen zum Datenschutz getroffen sind. Die katholische Kirche hat (auch) deshalb eine umfassende Regelung zur Sicherstellung des Datenschutzes getroffen (KDO – Anordnung über den kirchlichen Datenschutz).

Eine Datenübermittlung an nichtkirchliche und nicht öffentliche Stellen oder Personen ist nur unter bestimmten rechtlichen Bedingungen zulässig (vgl. § 12 KDO) die im Wesentlichen in § 10 Abs. 2 KDO geregelt sind. Nach dem oben genannten war die Weitergabe der Daten ersichtlich nicht zur Erfüllung einer Aufgabe der katholischen Kirchengemeinde erforderlich, so dass durch die unberechtigte Weitergabe ein Verstoß gegen die Anordnung über den kirchlichen Datenschutz zu sehen ist. Die Weitergabe stellt einen erheblichen Verstoß gegen die Datenschutzbestimmungen der Kirche dar. Die Maßnahme wurde entsprechend beanstandet. Der Dienstgeber hat seinerseits auf die Situation reagiert.

Fotografie von Neugeborenen im Krankenhaus

Die Beschwerde erreichte die Datenschutzaufsicht über die Landesbeauftragte für den Datenschutz in Bremen. Diese war von der Fraktion einer Bürgerschaftspartei angeschrieben worden.

Inhaltlich ging es um die Weitergabe der Information über die Geburt eines Kindes und die Weitergabe der Zimmernummer an eine Fotografin. Unter rechtlichen Gesichtspunkten um die Übermittlung von Patientendaten an eine Stelle außerhalb des Krankenhauses , die nur mit Einwilligung der Betroffenen zulässig gewesen wäre.

Die Landesdatenschutzbeauftragte hatte bereits 2011 für die städtischen Krankenhäuser eine Einwilligungserklärung bei den Fotoaufnahmen von Neugeborenen vereinbart. Dabei wurde darauf hingewiesen, dass die datenschutzrechtlichen Vorschriften für eine wirksame Einwilligungserklärung verlangen, dass der Adressat die Erklärung versteht. Ist dies aufgrund sprachlicher Barrieren nicht möglich, wäre die Erklärung unwirksam, mit der

Folge, dass entweder die Erklärung übersetzt werden müsste, oder die Daten nicht an einen Fotografen weitergegeben werden dürfen.

Nach der eingeholten Stellungnahme handelte es sich um eine nicht des deutschen mächtige slawische Patientin, die im Zuge der „kostenlosen“ Aufnahmen ihres Neugeborenen gleich drei Kinderalben mitbestellt haben soll.
Die Frage im Hinblick auf eine „verstandene“ Einwilligungserklärung konnte wegen des mittlerweile eingetretenen Zeitablaufs nicht mehr hinreichend sicher geklärt werden.

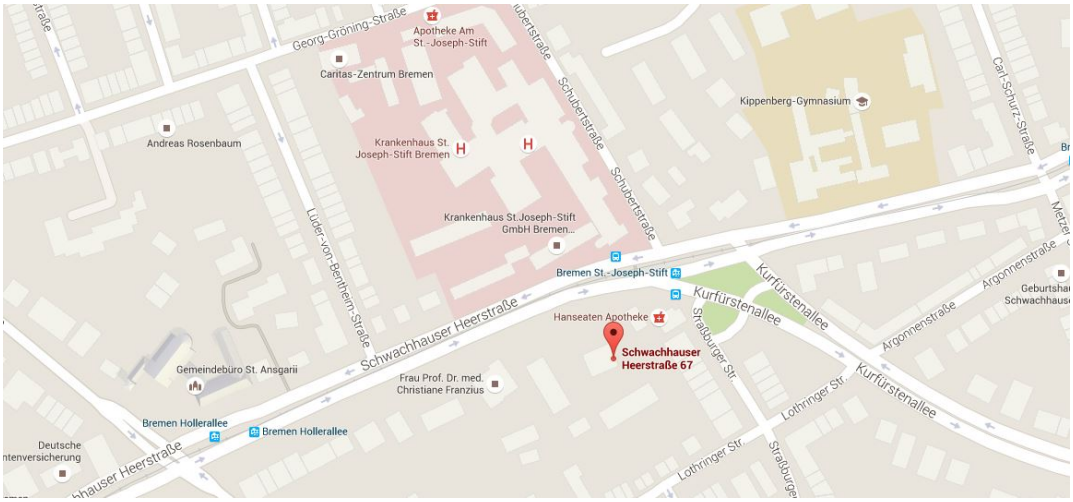
Zur Vermeidung von Wiederholungen hat das Krankenhaus nunmehr unter Beteiligung der Datenschutzaufsicht ein datenschutzrechtlich unbedenkliches Verfahren entwickelt.

Auf der Station wird Informationsmaterial zur Babyfotografie ausgelegt. Die Patientinnen können telefonisch oder per Anmeldekärtchen mit der Fotografin Kontakt aufnehmen und einen Termin vereinbaren. Die Mitarbeiter des Krankenhauses sind nicht mehr beteiligt. Die Eltern geben ihre Kontaktdaten in eigenem Ermessen an die Fotografen weiter.

4. Über die Dienststelle des DDSB / Nord – Bremen

4.1 Infrastruktur

Mit Datum vom 01.01.2016 wurde das Büro der Datenschutzaufsicht von Hannover nach Bremen verlegt.
Es befindet sich im Haus der Göken, Pollak und Partner Treuhand GmbH an der Schwachhauser Heerstr.67 in 28211 Bremen.
Das Büro ist über die Straßenbahnlinien 4 und 1 (5 Stationen (Josef Stift) vom HBF in Richtung Borgfeld/Lilienthal / bzw. Bahnhof Mahndorf) schnell zu erreichen.



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.

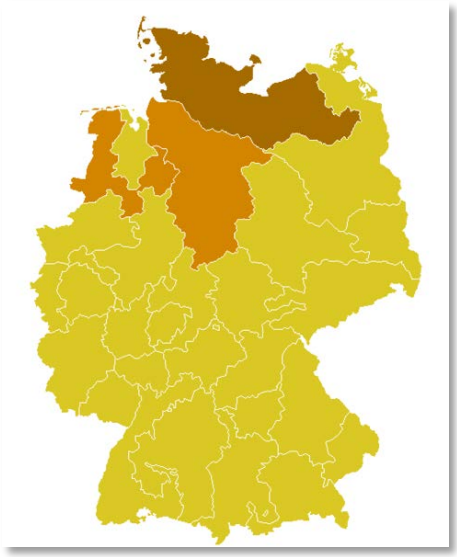
Die Finanz- und Budgethoheit liegt beim Diözesandatenschutzbeauftragten. Die Abwicklung des Haushaltes erfolgt über die Finanzabteilung des bischöflichen Generalvikariates Osnabrück als Belegenheitsbistum für die Stadt Bremen.

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

4.3 Personal

Neben dem Datenschutzbeauftragten (VZ) ist befristet bis Anfang 2018 ein weiterer Mitarbeiter (VZ) im Büro der Datenschutzaufsicht tätig. Das Sekretariat ist mit einer Mitarbeiterin mit einem Stundenumfang von derzeit 15 Stunden besetzt. Bei Fragen der IT – Sachbearbeitung kann temporär auf ein Dienstleistungsangebot einer Bremer IT – Firma zugegriffen werden.

Angesichts des oben beschriebenen Aufgabenprofils, das sich aus Art. 57 ff. EU-DSGVO ergibt, ist es aber erforderlich noch einmal ganz eigenständige Überlegungen zur personellen Ausstattung der Datenschutzaufsicht zu treffen. Schon allein die Durchführung von Prüfungen vor Ort, die auch zu den datenschutzrechtlichen Pflichtaufgaben (§ 18 Abs. 2 Nr. 2 KDO, 58 Abs. 1 lit. b EU-DSGVO) gehören wird angesichts des territorialen Zuständigkeitsbereichs der Dienststelle der Datenschutzaufsicht Nord deutlich, dass



Quelle: Wikipedia

eine adäquate und mit der europäischen Vorgabe kompatible Aufgabenerfüllung nur mit einem deutlich vergrößertem Personaltableau zu leisten ist.

Bei der Neukonzeption der kirchlichen Datenschutzaufsicht gingen die beteiligten Kirchenleitungen grundsätzlich davon aus, pro Datenschutzaufsichtsstelle zwischen drei und vier Mitarbeiter (VZ) zu schaffen. Im evangelischen Bereich ist die Neustrukturierung schon weit vorangeschritten. Laut Tätigkeitbericht des BfD

EKD arbeiten neben den vier Mitarbeitern in der Zentrale in Hannover jeweils drei Mitarbeiter in einer der vier Außenstellen.

Für den Bereich der Datenschutzaufsicht Nord wird es erforderlich sein, im Laufe des ersten Halbjahres verbindliche Entscheidungen über den Einsatz von zwei weiteren MitarbeiterInnen zu treffen. Der Bereich der IT – Sachbearbeitung wird wegen der weiter steigenden Anforderungen an die IT – Sicherheit ebenfalls ausgebaut werden müssen.

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 (bis November 2016)
- 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
- Ökumenischer Datenschutztag (Köln 2016)

4.5 Vernetzung

Im Berichtszeitraum sind Kontakte aufgebaut und Gespräche mit den Landesbeauftragten für den Datenschutz und Informationsfreiheit in Bremen, Niedersachsen und Hamburg 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

Für den Internetauftritt wurde bisher ein Content-Management-System (CMS), Drupal, in der Version 6.38 verwendet. Das System wird in der benannten Version nicht mehr unterstützt, bzw. es hat nicht unerhebliche Sicherheitslücken im Hinblick auf die Homepage gegeben. Im Zuge eines deshalb notwendigen Softwareupgrade von Drupal 6.38 auf Drupal 8.1.7 wurde die Webseite aktualisiert und neu gestaltet.

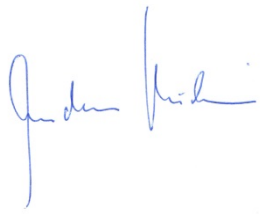
Der Internetauftritt der Datenschutzaufsicht Nord wird offensichtlich bundesweit genutzt und lässt nach den Rückäußerungen der Nutzer den Schluss zu sehr geschätzt sein. Es wird auch deshalb zukünftig das Ziel sein müssen, die Internetseite wie bisher zu pflegen und sie jeweils dem neuesten Stand des kirchlichen, und gegebenenfalls auch weltlichen, Datenschutzrechts anzupassen.

Die vorgehaltenen Informationen, Arbeitshilfen 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 erlebt rasante Zeiten. Nicht nur die Entwicklung eines europäischen Standards, sondern auch die daraus folgenden Anpassungen auf der Bundesebene und die rechtliche Notwendigkeit der Anpassung der kirchlichen Datenschutznormen und Datenschutzorganisation an die weltlichen Vorgaben unter Beibehalt der eigenen kirchlichen Datenschutzhoheit hat den Berichtszeitraum wesentlich mitgeprägt. Zudem ist der kirchliche Datenschutz für unsere Einrichtungen und Verbände ein zunehmendes Qualitätsmerkmal, bis hin zum Nachweis eines Datenschutzkonzeptes bei der Beteiligung an Ausschreibungsverfahren. Die Nachfrage nach Fortbildung und Hilfe bei der Umsetzung des Datenschutzes war im Verlauf des Berichtsjahres deutlich zunehmend. Das Problembewusstsein im Hinblick auf das Recht zur informationellen Selbstbestimmung für sich selbst, aber auch für andere, nimmt trotz Whats App und sozial Media zu. Diesen Tendenzen wird sich auch die Datenschutzaufsicht für die norddeutschen (Erz)Diözesen stellen müssen.

Bremen , im Januar 2017



Andreas Mündelein

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