Der Diözesandatenschutzbeauftragte

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

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Tätigkeitsbericht

des Diözesandatenschutzbeauftragten
der (Erz-)Bistümer Berlin, Hamburg, Hildesheim, Magdeburg, Osnabrück
und des Bischöflich Münsterschen Offizialats in Vechta i.O.

für die Zeit vom 01. Januar 2004 bis 31. Dezember 2009

gemäß § 17 Abs. 3 der Anordnung über den kirchlichen Datenschutz - KDO -
vorgelegt im Januar 2010

Lutz Grammann

Engelbosteler Damm 72 – 30167 Hannover
Telefon: 0511 / 81 93 15 – Telefax: 0511 / 81 21 35
E-Mail: info@datenschutz-kirche.de
Internet: http://www.datenschutz-kirche.de/

Inhalt:

1. Änderungen des Rechts

1.1 Die Rechtsentwicklung im Bereich der Katholischen Kirche Deutschlands

1.1.1 Die Anordnung über den kirchlichen Datenschutz – KDO –

Zu Beginn des Berichtszeitraums ist in allen deutschen Bistümern ist eine neue Anordnung über den kirchlichen Datenschutz in Kraft getreten. Sie ist gültig

- im Erzbistum Berlin seit dem 01. Oktober 2003
- im Erzbistum Hamburg sowie in den Bistümern Hildesheim und Osnabrück seit dem 01. November 2003
- im Oldenburgischen Teil der Diözese Münster seit dem 01. Dezember 2003
- im Bistum Magdeburg seit dem 01. Februar 2005

Mit ihr wurden, in bewährter inhaltlicher Anlehnung an das Bundesdatenschutzgesetz, die Vorgaben der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen und zum freien Datenverkehr vom 24. November 1995 in kirchliches Recht umgesetzt. Seither entspricht das Datenschutzrecht der katholischen deutschen Bistümer dem Standard aller Mitgliedsstaaten der Europäischen Union.

Wegen der unterschiedlichen föderalen Strukturen und der ebenso unterschiedlichen Kirchenverfassungen in den einzelnen Mitgliedsländern, hatte es die Richtlinie den Mitgliedsstaaten selbst überlassen, die Struktur der Datenschutzaufsicht den jeweiligen nationalen Gegebenheiten anzupassen. In der Bundesrepublik hat dies erfreulicherweise dazu geführt, dass das Selbstverwaltungsrecht der Kirche weiterhin dadurch respektiert wird, dass das Bundesdatenschutzgesetz nicht auf sie anwendbar ist. Es bleibt also auch künftig dabei, der Kirche auf diesem Gebiet eine eigene Regelungsgewalt und eigene Aufsichtsinstanzen zuzugestehen.

Ich werde immer wieder gefragt, worin der Sinn der kirchlichen Eigenständigkeit auf dem Gebiet des Datenschutzes liege. Diese Frage ist nicht allein mit dem Hinweis auf de Verfassungslage zu beantworten. Vielmehr scheint mir eine solche Trennung Teil des Datenschutzgedankens selbst zu sein. Eine Anwendung des BDSG auf die Kirchen würde auch eine staatliche Aufsicht über kirchliche Datenverarbeitung bedeuten. Auf Grund der historischen Erfahrungen in Deutschland mit Naziherrschaft und DDR-Diktatur kann sich niemand dies ernsthaft wünschen. Wenn wir das Prinzip der Trennung von Kirche und Staat ernsthaft wollen, müssen beide Seiten, bei aller Bereitschaft zur Zusammenarbeit, auch ihre Grenzen respektieren.

Dem durch Art. 137 Abs. 3 WRV i.V.m. Art. 140 GG garantierten Selbstverwaltungsrecht steht jedoch korrespondierend auch eine Selbstverwaltungspflicht gegenüber. Es kann nicht sein, das kirchliche Einrichtungen selbst darüber entscheiden, ob sie für ihren Bereich diözesanes oder staatliches Recht anwenden und ob der Diözesandatenschutzbeauftragte oder

der jeweilige Bundes- oder Landesbeauftragte für die Datenschutzaufsicht bei ihnen zuständig sein soll. Ein Recht des Bürgers, selbst über die Anwendbarkeit staatlicher Regelungen entscheiden zu dürfen, kennt unsere Rechtsordnung nicht. Da, unter Berücksichtigung des Goch-Beschlusses des Bundesverfassungsgerichts, die Exemtion für alle Dienststellen und Einrichtungen der Kirche gilt, die nach dem Willen der Kirche zur Kirche gehören, halte ich eine Klarstellung für dringend erforderlich. Es muss möglich sein, eine Liste mit den Namen und Anschriften aller Einrichtungen innerhalb eines Bistums zu erstellen, die nach dem Willen der hierzu Berufenen, zur Kirche gehören und daher auch dem kirchlichen Datenschutz unterliegen.

Inhaltlich hat das neue Recht, neben der Änderung und Präzisierung einer Reihe von Begriffen, vor allem eine weitere Stärkung der Rechte der Betroffenen gebracht. So gibt es nach § 14 Abs. 5 KDO nun erstmalig auch die Möglichkeit, einer rechtmäßig durchgeführten Datenverarbeitung zu widersprechen. Neu ist auch die Verpflichtung zur Benachrichtigung des Betroffenen, wenn Daten über ihn ohne seine Kenntnis erhoben werden (§ 13a KDO). Seine schon früher bestehenden Rechte auf Auskunft, Berichtigung, Sperrung und Löschung von Daten, wurden in vollem Umfang beibehalten. Erstmalig wurden nun auch bestimmte Arten personenbezogener Daten, hierzu zählen auch Angaben über religiöse Überzeugungen, als besonders schutzwürdig eingestuft (§ 2 Abs. 10 KDO), deren Erhebung (§ 9 Abs. 5 KDO), Speicherung, Veränderung und Nutzung (§ 10 Abs. 5 KDO) an strenge Voraussetzungen gebunden ist. Erfolgt die Datenerhebung, -verarbeitung oder –nutzung mit Einwilligung des Betroffenen, so muss diese sich ausdrücklich auf die zu verarbeitenden besonderen Daten beziehen (§ 3 Abs. 4 KDO).

Der fortschreitenden technischen Entwicklung wurde durch die neu geschaffene Verpflichtung zur Datenvermeidung und Datensparsamkeit sowie durch die erstmalige Regelung der Beobachtung öffentlich zugänglicher Räume durch optisch-elektronische Einrichtungen (Videoüberwachung, § 5a KDO) und den Einsatz mobiler Speicher- und Verarbeitungsmedien (Chipkaten, § 5b KDO) Rechnung getragen.

Alle Dienststellen und Einrichtungen, die der KDO unterliegen, haben über die von ihnen eingesetzten Verfahren automatisierter Datenverarbeitung ein Verzeichnis zu führen, das von jedermann eingesehen werden kann, der ein berechtigtes Interesse hieran nachweist. Einrichtungen, die keinen betrieblichen Datenschutzbeauftragten bestellt haben, müssen diese Verfahren zudem dem Diözesandatenschutzbeauftragten melden (§ 3a KDO).

Wie bisher auch bleiben alle kirchlichen Einrichtungen verpflichtet, ihrerseits die technisch-organisatorischen Maßnahmen zu treffen, die zum Schutz, der von ihnen verarbeiteten personenbezogenen Daten erforderlich sind (§ 6 KDO). Im Hinblick auf die immer komplexer werdenden Anforderungen in der Informations- und Kommunikationstechnik wird dies künftig immer weniger gelingen können, wenn der Datenschutz nicht als wichtige und zugleich anspruchsvolle Managementaufgabe stärker in den Blick genommen wird. Von den Dienststellen- und Verwaltungsleitern ist das allein kaum noch zu leisten. Als Konsequenz hieraus wurde in den §§ 18a, 18b KDO erstmals die Möglichkeit geschaffen, betriebliche Beauftragte

für den Datenschutz zu bestellen. Der Unterzeichner hat sich mit dafür eingesetzt, dass von der Schaffung einer generellen Verpflichtung zur Bestellung von Betriebsbeauftragten ab einer bestimmten Personenzahl in der Datenverarbeitung abgesehen wurde. Der Grund dafür liegt vor allem darin, dass in den Einrichtungen vielfach keine Mitarbeiter zur Verfügung stehen, die über genügend Kompetenz verfügen und zudem noch bereit sind, diese Aufgabe zu übernehmen. Hier besteht Handlungsbedarf, dem Mangel durch entsprechende Schulungsangebote zu verringern. Dankenswerter Weise hat sich der Verband der Diözesen Deutschlands seit einiger Zeit diesem Thema angenommen und bietet nunmehr Seminare zur Ausbildung von betrieblichen Datenschutzbeauftragten in Kooperation mit der TüV-Akademie Rheinland an. Der Vorteil dieser Zusammenarbeit liegt in einem Mehr an technischer Kompetenz durch die im Bereich der Informatik geschulten Referenten der TüV-Akademie. Der Unterzeichner war als Mitinitiator und Mitglied einer Ad-hoc-Arbeitsgruppe an dieser Entwicklung beteiligt.

Der Betriebsbeauftragte wird künftig ein wichtiges und entscheidendes Instrument für die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung sein.
Zu seinen wichtigsten Aufgaben wird gehören:

- Die Klärung der Rechtsgrundlagen, auf die sich die eigene Datenverarbeitung stützt.
- Die Betrachtung der vorhandenen EDV-Landschaft aus datenschutzrechtlicher Sicht, vor allem in „gewachsenen Strukturen".
- Beratung der Geschäftsleitung und Beteiligung bei der Auswahl möglichst datenschutz-. gerechter neuer Hard- und Software.
- Unterrichtung und Schulung der Mitarbeiter

Als Ansprechpartner für Mitarbeiter und Klienten ist er Teil der Unternehmenskultur.

Das Bundesdatenschutzgesetz wurde inzwischen erneut geändert. Die derzeit gültige Fassung des BDSG hat den Stand vom 14. August 2009. Die wesentlichen Änderungen betreffen

- den Kündigungsschutz für betriebliche Datenschutzbeauftragte (§ 4f Abs. 3 Satz 5 BDSG), die künftig nur noch aus wichtigem Grund entlassen werden können;
- den Arbeitnehmerdatenschutz (§ 32 BDSG);
- die Auftragsdatenverarbeitung (§ 11 Abs. 2 BDSG), hier wurden vor allem die mit dem Auftragnehmer schriftlich zu vereinbarenden Bedingungen der Auftragsvergabe erweitert und präzisiert. Parallel hierzu wurde mit § 80 SGB X eine Vorschrift für die externe Verarbeitung von Sozialdaten geschaffen, die allerdings direkt nur auf staatliche Stellen anwendbar ist. Eine Ausnahme bildet der § 120 Abs. 6 SGB V, der Krankenhäusern die Abrechnung von Notfallleistungen durch andere Stellen gestattet, wenn die Anforderungen aus § 80 SGB X erfüllt sind.
- der Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) bezieht sich künftig nicht mehr nur auf die Auswahl und Gestaltung technischer Systeme, sondern auf die gesamte Datenverarbeitung, also auch auf die Erhebung, Verarbeitung und Nutzung der Daten;

- die Erlaubnis der Verwendung der Daten zu Werbezwecken (§ 28 Abs. 3 BDSG). Ohne Einwilligung der Betroffenen dürfen diese nur noch für die Werbung für eigene Angebote sowie für berufsbezogene Werbung und steuerbegünstigte Spendenwerbung genutzt werden. Damit ist vor allem der Adresshandel wesentlich eingeschränkt worden.

Die genannten Änderungen des Bundesdatenschutzgesetzes werden auch eine erneute Anpassung der Anordnung über den kirchlichen Datenschutz erforderlich machen. Hiermit beschäftigt sich im Augenblick die Ständige Arbeitsgruppe Datenschutz-/Meldewesen-/IT-Recht der Rechtskommission des Verbandes der Diözesen Deutschlands.

Nach Einschätzung des Unterzeichners wird auch die Kirche, trotz des grundsätzlich bestehenden „dritten Weges" am Arbeitnehmerdatenschutz nicht vorbei kommen. Die KDO gestattet zu Zeit eine Erhebung von Mitarbeiterdaten, soweit ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist (§ 9 Abs. 1 KDO). Ob diese allgemeine Vorschrift dem verfassungsrechtlichen Bestimmtheitsgrundsatz entspricht, muss angesichts der Rechtsprechung des Bundesverfassungsgerichts in anderen Fällen bezweifelt werden. Immerhin muss der Arbeitnehmer eine große Fülle von Daten über seine persönlichen Verhältnisse preisgeben, die für eine Vielzahl von Zwecken, wie Lohn- und Gehaltsabrechnung, Lohnsteuervorwegabzug, Zahlung von Beiträgen an Sozialversicherungsträger, Beihilfeabrechnungen, berufliche Aus- und Weiterbildung, etc. benötigt werden. Hier wäre eine bereichsspezifische und normenklare Regelung durch ein Arbeitnehmerdatenschutzgesetz erforderlich, wie es im Bund auch geplant ist. Der § 32 BDSG schafft hier zunächst einmal vorab eine spezialgesetzliche Rechtsgrundlage, die zudem einen dringenden Punkt regelt, der in den vergangenen Jahren immer wieder zu Schwierigkeiten geführt hat, die Aufdeckung von Straftaten im Betrieb. Die Frage, welche Daten konkret für welche Zwecke erhoben werden dürfen und wie eine Trennung des Datenbestandes nach Aufgabenbereichen vorgenommen werden kann ohne den Grundsatz der Einheit der Personalakte aufzugeben, beantwortet § 28 BDSG allerdings nicht. Hier bleibt eine einzelgesetzliche Regelung abzuwarten.

Im Gegensatz zur Ständigen Arbeitsgruppe beim VDD ist der Unterzeichner auch der Meinung, dass die Erweiterungen des § 11 Abs. 2 BDSG zur Auftragsdatenverarbeitung in die KDO übernommen werden sollten. Die Datenverarbeitung durch Dritte schafft zusätzliche Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen. Strenge Anforderungen in diesem Bereich sind somit die Voraussetzung dafür, dass eine solche Zusammenarbeit überhaupt gestattet werden kann. In der Praxis wird dies leider nicht immer ernst genommen. Manch verantwortliche Stelle hält es für ausreichend, wenn ihr eine einseitige „Datenschutzerklärung" des Auftragnehmers mit wohlwollend formulierten allgemeinen Absichtserklärungen vorgelegt wird. Demgegenüber enthält das BDSG klar definierte Anforderungen, die vor Beginn der Zusammenarbeit durch eine beidseitige schriftliche Vereinbarung geregelt werden müssen. Darüber hinaus ist die Kirche in vielfältiger Weise gerade auch in sozialen Bereichen tätig. Es macht daher Sinn, eine dem § 80 SGB X entsprechende Vorschrift in der KDO zu haben.

Die Nutzung der Daten des Gemeindemitgliederverzeichnisses für eigene Werbezwecke sollte hingegen durch eine Fundraisingordnung oder zumindest durch eine Ausführungsvorschrift zu § 5 Abs. 6 KMAO geregelt werden. Eine Aufnahme in die KDO sehe ich nicht als erforderlich an.

Die Übernahme der Änderungen des § 3a BDSG (Datenvermeidung und Datensparsamkeit) dürfte hingegen kaum Vorteile bringen, zumal das Verhältnis dieser Norm zum Grundsatz der Erforderlichkeit (§§ 9 Abs. 1, 10 Abs. 1, 11 Abs.1 Zi. 1 und 12 Abs. 1 Zi. 1 KDO) aus meiner Sicht nicht geklärt ist.

Die Übernahme des Kündigungsschutzes für betriebliche Datenschutzbeauftragte ist sinnvoll, um die Bereitschaft zur Übernahme dieser Aufgabe zu verbessern.

1.1.2 Die Anordnung über das kirchliche Meldewesen (KMAO)

Ein weiterer Meilenstein im kirchlichen Datenschutzrecht war die Reform, der seit 1978 bestehenden Anordnung über das kirchliche Meldewesen (KMAO). Die neue KMAO ist in den norddeutschen Diözesen am 1. November 2005 (Erzbistum Berlin, Bistum Osnabrück), am 1. Dezember 2005 (Offizialat Vechta), am 1. Januar 2006 (Erzbistum Hamburg, Bistum Hildesheim) und am 1. Juli 2006 (Bistum Magdeburg) in Kraft getreten.

Die wichtigste Änderung ist dabei die neue Regelung zum Gemeindemitgliederverzeichnis. Bisher wurde es ausschließlich für die seelsorgerischen Aufgaben der Pfarreien geführt. Dementsprechend wurden auch die Kirchengemeinden allein als „Herr der Daten" angesehen. Die Meldestellen der Bistümer nahmen zwar die von den kommunalen Meldebehörden übermittelten Daten entgegen und ließen sie in Rechenzentren weiterverarbeiten, dies geschah jedoch ausschließlich im Auftrag der Gemeinden. Die Grenzen dieses Systems waren vor allem im Fundraising sichtbar. Für eine Auswertung und Nutzung des Gesamtdatenbestandes gab es keine Rechtsgrundlage. Jede Übermittlung von Gemeindemitgliederdaten an kirchliche Einrichtungen zum Zwecke des Versendens von Spendenaufrufen war an die Zustimmung der jeweiligen Gemeindeleiter vor Ort gebunden. Die neue KMAO ermöglicht hier eine größere Flexibilität und Praxisbezogenheit. Den Pfarreien steht auch in Zukunft ein Verzeichnis der Kirchenmitglieder und ihrer Angehörigen für ihren jeweiligen Sprengel zur Verfügung. Darüber hinaus hat nunmehr auch das Bistum die Möglichkeit die Daten aller Kirchenmitglieder der Diözese zu erheben, zu verarbeiten und zu nutzen (§ 5 Abs. 1, 6 KMAO). Beide Seiten sind, jeweils für ihren Bereich, Herr der Daten und verantwortliche Stelle im Sinne von § 2 Abs. 8 KDO. Durch Schaffung einer Ausführungsvorschrift nach § 5 Abs. 6 Satz 3 KMAO besteht zudem die Möglichkeit, die Zugriffsberechtigung für das Gemeindemitgliederverzeichnis des Bistums im Sinne kirchlicher Aufgabenerfüllung zu regeln.

Weitere Verbesserungen aus der Sicht des Datenschutzes sind die Regelungen zum Umfang der Datenerhebung (§ 5 Abs. 3 KMAO) und die ausdrückliche Verpflichtung zur Beachtung von Auskunfts- und Übermittlungssperren (§ 5 Abs. 5 KMAO). Die früher geltende KMAO hatte die Festlegung des Datenkataloges einer Ausführungsvorschrift überlassen, die inso-

weit jedoch nie erlassen wurde. Durch das neue Recht wird klargestellt, dass sich die Gemeindemitgliederverzeichnisse aus dem kommunalen Datenbestand, soweit er den Kirchen nach den Meldegesetzen zu übermitteln ist und den kircheneigenen Matrikeldaten zusammensetzt.

Zur Bereinigung des Datenbestandes in Umzugsfällen kann eine Einsichtnahme in das Mitgliederverzeichnis einer anderen Diözese notwendig sein. Auch eine schnelle Klärung kirchenrechtlicher Fragen, wie sie z.B. in Zusammenhang mit Eheschließungen auftreten können, ist nicht immer ohne Einsicht in das Register eines anderen Bistums möglich. Die KMAO-1979 enthielt hierzu in § 7 die Bestimmung: „Die Bistümer werden untereinander den für die Erfüllung kirchlicher Aufgaben erforderlichen Datenaustausch durchführen." Diese Vorschrift findet sich in der neuen KMAO nicht mehr, wobei dieser Umstand wohl eher auf ein Redaktionsversehen, als auf eine bewusste Entscheidung zurückzuführen ist. Die Notwendigkeit einer solchen Regelung besteht jedoch uneingeschränkt weiter. Der Unterzeichner unterstützt daher die Bemühungen des VDD, eine erneute Änderung der KMAO durch Einfügung eines neuen § 5a vorzunehmen:

> § 5a Datenübermittlung
> (1) Im Einzelfall werden die Bistümer die für die Erfüllung kirchlicher Aufgaben erforderliche Datenübermittlung durchführen. § 11 Abs. 4 KDO findet Anwendung.
> (2) Werden die Daten für andere als Meldezwecke übermittelt (§ 10 Abs. 2 KDO), ist die Übermittlung auch in geeigneter Weise zu dokumentieren.
> (3) Das übermittelnde Bistum kann im Einzelfall der Übermittlung widersprechen.

Die neue KMAO hat die Grundlage für eine zeitgemäße und effektive Datenverarbeitung im Bereich der Bistümer geschaffen. In einem weiteren Schritt sollte überlegt werden, für welche Nutzungen und Nutzer das Gemeindemitgliederverzeichnis künftig zur Verfügung stehen soll und dies in einer Ausführungsvorschrift festgelegt werden.

1.1.3 Die Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft

Auf Initiative des früheren Diözesandatenschutzbeauftragten der bayerischen Diözesen, Herrn Fischer, hat die Vollversammlung des Verbandes der Diözesen Deutschlands am 25.11.2003 beschlossen, allen Bistümern die Einführung einer „Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft" zu empfehlen. In den norddeutschen Diözesen sind das Erzbistum Hamburg (28.02.2005), das Bistum Hildesheim (01.08.2004), das Bistum Osnabrück (12.10.2004) und das Offizialat Vechta (21.05.2004) der Empfehlung gefolgt

Die Vorschriften des I., VIII. und X. Buches des Sozialgesetzbuchs gelten unmittelbar nur für die staatlichen Leistungsträger. Soweit Aufgaben der Kinder- und Jugendhilfe auf kirchliche Einrichtungen übertragen werden, bedurfte es bisher einer Vereinbarung, die sicherstellte, dass die Datenschutzvorschriften des SGB, insbesondere das Sozialgeheimnis auch

von den Leistungserbringern eingehalten werden. Durch die Anordnung über den Sozialdatenschutz werden diese Vorschriften nunmehr als auch für kirchliche Einrichtungen unmittelbar geltendes Recht übernommen. Das erleichtert die Zusammenarbeit mit den staatlichen Stellen. Ein weiterer Vorteil besteht in der Schaffung von Rechtsgrundlagen für die Datenverarbeitung kirchlicher Dienststellen in diesem Bereich. So ist es zum Schutz der Kinder zweifelsfrei wünschenswert, dass Mitarbeiter in Kindergärten auf etwaige Auffälligkeiten hinsichtlich bestimmter Straftaten, wie Kindesmissbrauch, überprüft werden. § 72a SGB VIII gibt nunmehr auch kirchlichen Kindergärten die Möglichkeit hierzu, schafft aber gleichzeitig die Verpflichtung, sich den staatlicherseits gesetzten Qualitätsstandards anzupassen.

Die Anordnung über den Sozialdatenschutz stellt einen Fortschritt in der Zusammenarbeit mit den staatlichen Leistungsträgern dar und schafft Rechtssicherheit für die kirchlichen Leistungserbringer. Sie sollte von den Bistümern, die der Empfehlung bisher nicht gefolgt sind, in Kraft gesetzt werden.

1.2 Die Rechtsentwicklung im Bereich der norddeutschen Bistümer

Auch nach Erlass der neuen Anordnung über den kirchlichen Datenschutz – KDO – gelten die bisher schon in den norddeutschen Bistümern erlassenen bereichsspezifischen Vorschriften, wie die zur Datenverarbeitung in Schulen, Krankenhäusern und Friedhöfen weiter fort. Das Bistum Hildesheim hat dies durch Veröffentlichung im Kirchlichen Amtsblatt vom 18.12.2003 sogar ausdrücklich klargestellt.

Neu geschaffen wurde die Regelung zur Datenübermittlung in Zusammenhang mit den Fusionen der Kirchengemeinden im Erzbistum Berlin und die Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim. Die im Erzbistum Hamburg und in den Bistümern Hildesheim, Osnabrück sowie im Offizialatsbezirk Vechta bestehende Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft wurde um zwei Vorschriften erweitert.

1.2.1 Datenübermittlung im Zusammenhang mit den Fusionen der Kirchengemeinden (Erzbistum Berlin)

In praktisch allen deutschen Bistümern kommt es derzeit zur Zusammenlegung mehrerer Pfarrgemeinden jeweils zu einer neuen, größeren Gemeinde. Das nach einer solchen Fusion auch die Datenbestände aus den Gemeindemitgliederverzeichnissen zusammengeführt werden, ist selbstverständlich und durch § 11 Abs. 1 KDO auch rechtlich abgedeckt. Die Übermittlung der Daten der aufzulösenden Kirchengemeinden ist insoweit zur Erfüllung der pastoralen Aufgaben erforderlich und erfolgt für den gleichen Zweck, für den sie erhoben worden sind. Zur Vorbereitung der Fusion können diese Daten nunmehr schon drei Monate vorher übermittelt werden, wenn der seelsorgerische Leiter der Gemeinde diese anfordert. Aus Sicht des Datenschutzes erfreulich ist dabei vor allem die klare zeitliche Begrenzung.

1.2.2 Die Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim (FundrO)

Angesichts knapper werdender Ressourcen wird die Suche nach neuen Einnahmequellen immer wichtiger. In vielen Bistümern hat sich schnell herumgesprochen, dass persönlich gehaltene Spendenbriefe meist einen guten Erfolg versprechen. Dies umso mehr, wenn Personengruppen erreicht werden, die statistisch gesehen als besonders spendenfreudig gelten (z.B. kirchlich gebundene, allein stehende Damen über 60 Jahre). Daher liegt es nahe, die Gemeindemitgliederverzeichnisse entsprechend auszuwerten und mit den gefundenen Adressdatensätzen, die betreffenden Personen direkt anzuschreiben (sog. „Direct Mailing"). Unter dem alten Melderecht gab es hierfür allerdings keine Rechtsgrundlage. In Zusammenarbeit zwischen Fundraisingbüro, Rechtsamt, Meldestelle und Datenschutz wurde daher eine Fundraisingordnung geschaffen, die innerhalb der katholischen Kirche vorbildlich ist. Durch sie wird die Nutzung personenbezogener Daten gerade für diesen Zweck gestattet (§ 1 Abs. 1 FundrO) und eine kontrollierte und koordinierte Verarbeitung (§ 1 Abs. 2, 3 FundrO) gewährleistet. Die Forderungen des Datenschutzes wurden dabei in vollem Umfange erfüllt. Hierbei fällt vor allem ins Gewicht, dass

- die Ziele und Zwecke der Datenverarbeitung genau bestimmt sind;
- der Umfang der personenbezogenen Daten, die zur Verarbeitung zur Verfügung stehen, präzise festgelegt wurde (§§ 2, 4 Abs. 1 FundrO);
- eine Weitergabe, der bei Durchführung der Maßnahme gewonnenen Daten an andere Stellen, ausgeschlossen ist (§ 4 Abs. 3 FundrO);
- Übermittlungssperren (§ 4 Abs. 4 FundrO) und Robinson-Listen (§ 4 Abs. 5 FundrO) beachtet werden und
- eine Frist zur Löschung der Daten nach Ende der Maßnahme festgelegt wurde.

Darüber hinaus besteht natürlich auch in diesem Bereich die Verpflichtung, die Daten durch technisch-organisatorische Maßnahmen zu schützen (§ 2 Abs. 3 FundrO). Die Schaffung einer zentralen Fundraisingstelle ist dabei sicherlich eine Besonderheit, die nicht für alle Diözesen in Frage kommt, jedoch die Möglichkeit gibt, verschiedene Maßnahmen zeitlich aufeinander abzustimmen. Das dürfte nicht nur deren Wirksamkeit erhöhen, sondern gleichzeitig auch zu einer besseren „Verträglichkeit" auf Seiten der Betroffenen führen. Darüber hinaus erfahren auch die Einrichtungen, die mit dem Thema Fundraising bisher noch wenig vertraut sind, professionelle Unterstützung.

Seit Erlass der neuen Meldewesenanordnung (KMAO) besteht für die Bistümer die Möglichkeit der Führung und Nutzung eines eigenen Gemeindemitgliederverzeichnisses. Hierdurch wurde die Rechtsgrundlage für eine einheitliche Auswertung und Nutzung des Gesamtdatenbestandes in der Diözese geschaffen. Die Fundraisingordnung ist wegen der vorbezeichneten präzisen Festlegungen und der von ihr geschaffenen organisatorischen Regelungen allerdings trotzdem nicht entbehrlich geworden und wurde auch nach Schaffung der neuen KMAO erneut verkündet und in Kraft gesetzt.

Fundraisingmaßnahmen werden in Zukunft immer wichtiger. Zum Schutz der hierbei verwendeten personenbezogenen Daten, sollten konkrete Regelungen darüber erfolgen, wer, wann, unter welchen Umständen, welche Daten erhalten und nutzen darf. Hierzu bieten sich Ausführungsvorschriften im Sinne von § 5 Abs. 6 Satz 3 KMAO an. Die im Bistum Hildesheim erlassene Ordnung kann hier in gewisser Weise Vorbildfunktion entfalten.

Allerdings wurden schon im Jahre 2008 von dem neuen Leiter des Fundraisingbüros, Herrn Heil Änderungswünsche an dieser Vorschrift angemeldet. Im Kern geht es dabei darum, die Effektivität des Spendensammelns durch den Aufbau einer eigenen Spenderdatenbank zu verbessern. Hierdurch soll den Werbern das notwendige „Hintergrundwissen" zur Verfügung gestellt werden, um Spender gezielt für bestimmte Projekte ansprechen zu können. Zum Aufbau einer solchen Datenbank wäre ein regelmäßiger Abgleich mit dem Gemeindemitgliederregister des Bistums erforderlich, der zudem nicht vom Fundraisingbüro selbst, sondern von einem externen Drittanbieter durchgeführt werden soll. Die Fundraisingordnung in ihrer derzeitigen Fassung gestattet eine solche Verfahrensweise nicht.

Nach einem umfangreichen Gespräch mit dem Leiter des Fundraisingbüros, der Justiziarin, dem Leiter der Meldestelle und dem Unterzeichner im Fundraisingbüro in Hildesheim wurde zunächst vereinbart, dass Herr Heil seine Änderungswünsche einmal schriftlich klar definiert, damit geprüft werden kann, in wie weit sich diese datenschutzgerecht umsetzen lassen. Bisher sind solche Vorschläge jedoch nicht unterbreitet worden. Eine zuletzt im Juni 2009 erhobene Nachfrage von Seiten der Rechtsabteilung beim Fundraisingbüro blieb bisher ohne konkrete Antwort. Sollte der Wunsch nach einer Verbesserung des Fundraisings weiter bestehen, wird es hier in Zukunft noch erheblicher Anstrengungen bedürfen, um die notwendigen rechtlichen Grundlagen zu schaffen.

1.2.3 Änderung der Schuldatenschutzanordnung

Die im Erzbistum Hamburg sowie in den Bistümern Hildesheim und Osnabrück sowie im Offizialatsbezirk Vechta geltende „Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft" wurde in zwei wichtigen Punkten geändert.

Zi. 6.8 der Richtlinie zum Einsatz von Arbeitsplatzcomputern in den Diözesen Hildesheim, Osnabrück und im oldenburgischen Teil des Bistums Münster gestattet die Verarbeitung dienstlicher Daten auf privaten Rechnern nur, wenn dies zur Erfüllung der dienstlichen Aufgaben unabweislich oder zwingend geboten ist. Die seit dem Zeitpunkt des Erlasses der Richtlinie im Jahre 1994 fortschreitende Entwicklung hat jedoch vor allem im Schulbereich dazu geführt, dass immer mehr Lehrkräfte die Daten ihrer Schüler auf eigenen Rechnern zu Hause bearbeiten. Mit Erlass vom 11.11.2004 hat das Niedersächsische Kultusministerium diesem Umstand Rechnung getragen und die private Datenverarbeitung für diesen Bereich allgemein, unter bestimmten Voraussetzungen zugelassen. Aus kirchlicher Sicht stellte sich daher die Frage, ob dieser Erlass inhaltsgleich auch für katholische Schulen übernommen werden sollte. In Abstimmung mit den Rechtsämtern, den Schulabteilungen der beteiligten Generalvikariate und dem Diözesandatenschutzbeauftragten konnte geklärt werden, dass

der Erlass unter Einfügung einer Bestimmung über die Bestellung eines betrieblichen Datenschutzbeauftragten wortgleich übernommen werden kann. Aufgrund der Einwendungen des Bistums Osnabrück gegen die Installation eines betrieblichen Datenschutzbeauftragten in Schulen, wurde diese Bestimmung, parallel zur KDO als Kann-Bestimmung geschaffen. Hierzu wurden die §§ 2a und 7 neu in die Schuldatenschutzanordnung eingefügt:

> § 2a Betrieblicher Beauftragter für den Datenschutz
> (1) Für die Schulen kann ein betrieblicher Beauftragter für den Datenschutz bestellt werden. Mehrere Schulen können gemeinsam einen betrieblichen Datenschutzbeauftragten bestellen. Die Bestellung muss schriftlich erfolgen.
> (2) Zum betrieblichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der Schule beauftragt werden.
> (3) Der betriebliche Datenschutzbeauftragte für die Schulen ist dem Leiter der jeweiligen Schule zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.
> (4) Die Schulen haben den betrieblichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgabe zu unterstützen. Betroffene können sich jederzeit an den betrieblichen Datenschutzbeauftragten wenden.
> (5) Im Übrigen findet § 16 KDO entsprechende Anwendung.
> (6) Der betriebliche Datenschutzbeauftragte ist auch berechtigt, die Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungsgeräten von Lehrkräften im Sinne von § 7 zu kontrollieren.
> (7) Der betriebliche Datenschutzbeauftragte ist darüber hinaus verpflichtet, die Schulen in allen datenschutzrechtlichen Fragen zu beraten.
>
> § 7 Verarbeitung personenbezogener Daten auf privaten Datenverarbeitungsgeräten von Lehrkräften
> (1) Lehrkräften der Schule kann mit schriftlicher Genehmigung der Schulleitung gestattet werden, personenbezogene Daten der von ihnen unterrichteten Schüler auf ihren eigenen privaten Datenverarbeitungsanlagen zu verarbeiten.
> (2) Das Nähere regelt eine Ausführungsvorschrift zu dieser Anordnung.

Die in § 7 Abs. 2 SchulDO bezeichnete Ausführungsvorschrift wurde zeitgleich erlassen. Die genannten Änderungen wurden im Bistum Osnabrück zum 01.06.2008, im Erzbistum Hamburg zum 01.02.2009 und im Bistum Hildesheim zum 01.04.2009 in Kraft gesetzt. Im Offizialatsbezirk Vechta sind sie bisher nicht erlassen worden. Nach Mitteilung des Rechtsamtes hat dies allerdings nur redaktionelle Gründe. Der Erlass soll in Kürze gemeinsam mit dem Bischöflichen Schulgesetz erfolgen.

1.2.4 Geplant: Bischöfliches Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen

Zum Schutz von Kindern und Jugendlichen vor sexuellem Missbrauch und körperlicher Misshandlung sieht § 72a SGB VIII vor, dass die Träger der öffentlichen Jugendhilfe sicherzustellen haben, dass sie keine Personen beschäftigen, die wegen eine dieser Taten vorbestraft sind. Hierzu haben sie sich von den Bewerbern vor Beginn ihrer Tätigkeit und von den bereits Beschäftigten in regelmäßigen Abständen alle 5 Jahre ein Führungszeugnis nach dem Bundeszentralregistergesetz vorlegen zu lassen. Diese allgemein für sinnvoll erachtete Vorschrift wurde leider nicht in die „Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft" übernommen, so dass sie nicht unmittelbar auf die kirchlichen Leistungserbringer anwendbar ist. Damit fehlt zunächst die Rechtsgrundlage, um bei kirchlichen Einrichtungen in gleicher Weise verfahren zu können. Um dies zu erreichen bedarf es daher jeweils einer Vereinbarung mit den Kostenträgern, um den Schutzauftrag nach § 8a SGB VIII sicherzustellen.

In den (Erz-)Bistümern Hamburg, Hildesheim, Osnabrück sowie im Offizialatsbezirk Vechta entstand daher der Wunsch, hier eine eigenständige Regelung zu schaffen und diese auf den gesamten Bereich kirchlicher Kinder- und Jugendarbeit auszudehnen. Sie sollte auch die Bereiche außerhalb des SGB VIII, vor allem in den Pfarrgemeinden, Schulen sowie den Ehe-, Familien-, Lebens- und Erziehungsberatungsstellen erfassen. Eine von den Diözesanjuristen gebildete „Arbeitsgruppe Schutzauftrag § 72a SGB VIII", mit Vertretern aus den genannten Diözesen und dem Unterzeichner hat in mehreren Sitzungen einen Entwurf für ein „Bischöfliches Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen" entworfen. Der aktuelle Entwurf (Stand: 11. Juni 2008) ist diesem Bericht im Anhang beigefügt.

Kritik an diesem Entwurf besteht vor allem bei der Einbeziehung ehrenamtlicher Mitarbeiter. Insoweit wird befürchtet, dass hierdurch die Bereitschaft zur Mitarbeit abnehmen könnte. Allerdings sieht der Entwurf die Vorlage eines Führungszeugnisses für diesen Personenkreis nur dann vor, wenn sie Jugendfreizeiten hauptverantwortlich, also ohne Begleitung durch einen der hauptamtlich Tätigen (Pfarrer, Pastoral- oder Gemeindereferenten) durchführen. Gerade hier besteht aber die Gefahr, dass es ohne die notwendige Kontrolle zu Übergriffen kommen könnte.

Bisher ist das Gesetz noch nicht verkündet worden. Nach den Informationen, die der Unterzeichner zuletzt erhalten hat, soll dies aber nunmehr in Kürze nachgeholt werden.

2. Informations- und Kommunikationstechnik

2.1 Nutzerverfolgung (Tracking) im Internet mit Hilfe von Google Analytics

Die Firma Google Inc. mit Sitz in den USA stellt ihre Dienstleistungen im Internet allen Endkunden kostenlos zur Verfügung. Kostenlose E-Mail-Adressen (Google-Mail), Webalben (Picasa), das Hochladen und Speichern von Videos (You Tube), Adress- und Terminverwaltung, das Anlegen eigener Blogs, die Nutzung eines Navigationsprogramms und vieles mehr ist möglich. Zwischenzeitlich wurde sogar ein eigenes Betriebssystem (Android) geschaffen, damit diese so scheinbar segensreichen Möglichkeiten nicht nur vom heimischen PC, sondern auch mobil vom eigenen Handy oder Smartphone aus erreichbar sind. Finanziert wird dies alles über Werbeeinnahmen. Der Kunde, der dies alles nutzt, gibt dabei eine Vielzahl personenbezogener Daten von sich preis. Zwar hat Google umfangreiche Datenschutzbestimmungen (Privacy Policy) hierzu im Internet veröffentlicht, eine öffentliche Datenschutzaufsicht, die deren Einhaltung kontrollieren könnte, existiert in den Vereinigten Staaten jedoch nicht.

Seit einiger Zeit bietet Google Inc. nun auch Webseitenbetreibern einen kostenlosen Dienst an, der es ermöglicht, die Zahl der Zugriffe auf die Homepage und eine Reihe weiterer Daten zur Nutzung der einzelnen Angebote der Webseite zu erfassen und statistisch auszuwerten (Google Analytics). Hierzu muss ein entsprechender Link auf eine Seite von Google in den eigenen Source-Code implementiert werden. Sodann wird nicht nur die IP-Adresse des Besuchers ermittelt, sondern mit Hilfe sogenannter First-Party-Cookies auch noch weitere personenbezogene Daten der Internetnutzer erhoben und an Google Inc. übermittelt. Der Betroffene wird dabei nicht ausreichend über den Umfang und die Verwendung seiner Daten aufgeklärt. Über die IP-Adresse ist es auch leicht möglich, diese Daten mit den bei Google ohnehin gespeicherten Daten der angemeldeten Nutzer der Google-Dienste zusammenzuführen und somit umfangreiche Nutzerprofile zu erstellen.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat hierzu bereits im Januar 2009 eine gutachterliche Stellungnahme veröffentlicht, die zu der Feststellung kommt, dass der Einsatz von Google-Analytics wegen Verstoßes gegen § 15 des Telemediengesetzes (TMG) rechtswidrig sei. Zudem soll es sich nach Auskunft der Firma Google Deutschland GmbH um eine Auftragsdatenverarbeitung handeln. In diesem Falle würde noch ein weiterer Verstoß gegen § 8 KDO hinzukommen, da insoweit die gesetzlichen Anforderungen nicht erfüllt sind.

Im Bereich der Nordbistümer hatten zunächst das Erzbistum Hamburg, später auch die Bistümer Hildesheim und Osnabrück diesen Dienst auf ihren Internetangeboten eingesetzt. In allen drei Fällen wurden die verantwortlichen Webadministratoren angeschrieben und vom Unterzeichner aufgefordert, das Tool von der jeweiligen Webseite zu entfernen. In einem Falle bedurfte es eines förmlichen Beanstandungsverfahrens nach § 18 Abs. 1 KDO um dieses Ziel zu erreichen, in den beiden anderen Fällen haben die Betreiber schon nach kurzer Zeit selbst Google-Analytics von ihrer Seite entfernt.

2.2 Veröffentlichung von Fotos im Internet

Immer wieder kommt es zu Anfragen, unter welchen Voraussetzungen die Veröffentlichung von Fotos auf denen Personen klar erkennbar sind im Internet zulässig sei. Allgemein gilt auch hier das Recht am eigenen Bild, dass durch § 22 Kunsturhebergesetz geschützt wird. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Ausnahmen von diesem Grundsatz bestehen, für

- Bildnisse, für die der Abgebildete hierfür eine Entlohnung erhalten hat, § 22 Satz 2 KunstUrhG,
- Bildnisse aus dem Bereich der Zeitgeschichte, § 23 Abs. 1 Zi. 1 KunstUrhG
- Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen; § 23 Abs. 1 Zi. 2 KunstUrhG
- Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben; § 23 Abs. 1 Zi. 3 KunstUrhG
- Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient, § 23 Abs. 1 Zi. 2 KunstUrhG.

Aber auch in diesen Ausnahmefällen darf eine Veröffentlichung nach § 23 Abs. 2 KunstUrhG nur dann erfolgen, wenn hierdurch kein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird. Eine Publikation im World Wide Web verletzt jedoch immer das berechtigte Interesse des Betroffenen. Grund dafür sind die spezifischen Gefahren einer im Wortsinn grenzenlosen Verbreitung, der jederzeitigen Möglichkeit der Weiterverwendung zu anderen Zwecken und der vielfältigen Veränderungs- und Bearbeitungsmöglichkeiten solcher Bilder. Die genannten Risiken sind mit denen einer Veröffentlichung in Printmedien, für die das Gesetz ursprünglich geschaffen wurde, auch nicht annähernd vergleichbar.

Aus diesem Grunde bedarf die Veröffentlichung von personenbezogenen Bildern im Internet immer der Einwilligung der Betroffenen. Die Einwilligung muss dabei im Einzelfall erteilt werden. Eine formularmäßige Erklärung, etwa im Kindergartenaufnahmevertrag ist unwirksam. Kinder sind hier, im Hinblick auf die Verbreitung von Kinderpornographie besonders gefährdet. Eventuelle Täter sehen die Bilder von Kindergartenkindern wie einen Katalog, aus dem man sich die geeigneten „Lustobjekte" aussuchen kann und zudem noch erfährt, wo man ihnen auflauern und sie ansprechen kann. Aus diesem Grunde hat die Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands gemeinsam mit der Konferenz der Datenschutzbeauftragten der evangelischen Landeskirchen eine Erklärung zu der Frage, ob Fotos von Kindergartenkindern im Internet veröffentlicht werden dürfen, verfasst. Der Wortlaut der gemeinsamen Erklärung ist im Anhang abgedruckt.

2.3 Datenschutzrechtliche Anforderungen an die Gestaltung von Webseiten durch das neue Telemediengesetz

Im Berichtszeitraum hat der Bundesgesetzgeber das Telemediengesetz (TMG) erlassen. Hierdurch wurde eine notwendige Anpassung an das europäische Recht, wie auch gleichzeitig eine Zusammenfassung, der bisher auf das TDG, das TDDSG und den Mediendienstestaatsvertrag (MDStV) verteilten Rechtsmaterie erreicht. Dieses Gesetz gilt in vollem Umfang auch für kirchliche Einrichtungen. Von Bedeutung sind vor allem

- die Impressumspflicht, § 5 TMG und
- die Datenschutzerklärung (Privacy Policy), § 13 TMG.
- Bestandsdaten (§ 14 TMG) und Nutzungsdaten (§ 15 TMG) dürfen nur in dem für die Inanspruchnahme der Telemedien erforderlichen Umfang erhoben und verwendet werden. Für Bestandsdaten gilt eine Ausnahme für Zwecke der Strafverfolgung und zur Gefahrenabwehr (§ 14 Abs. 2 TMG).

Zur Information der kirchlichen Webseitenbetreiber hat der Unterzeichner eine Handreichung verfasst, die auf der Internetseite „www.datenschutz-kirche.de" als PDF-Datei abrufbar ist.

3. Datenschutz in kirchlichen Einrichtungen

3.1 Meldewesen

3.1.1 Hauswerbung Kirchenzeitung im Bistum Hildesheim

Die Weitergabe von Namen und Anschriften katholischer Haushaltsvorstände an den Bernward Verlag zum Zwecke der Haustürwerbung für die Kirchenzeitung (KiZ) führt immer wieder zu Beschwerden von Seiten der Betroffenen. Verlag und Redaktion der KiZ, deren Herausgeber der Bischof ist, sind kirchliche Stellen im Sinne von § 1 Abs. 2 KDO, die die Anordnung über den kirchlichen Datenschutz anzuwenden haben. Sie haben auch Anteil am seelsorgerischen Auftrag der Kirche, indem sie nicht nur Nachrichten verbreiten, sondern zugleich auch zur Mission und zur Förderung einer inneren Einheit der Kirche beitragen. Eine Datenübermittlung muss insoweit die Anforderungen nach § 11 Abs. 1 KDO erfüllen. Um ihrem Auftrag gerecht werden zu können, muss die KiZ auch bemüht sein, neue Leser zu gewinnen. Hierzu hat der Unterzeichner schon von Anbeginn die Auffassung vertreten, die Werbung gehöre zur rechtmäßigen Aufgabenerfüllung der Datenempfängerin, so dass ihr im notwendigen Umfang Adressmaterial zur Verfügung gestellt werden könne. Eine schon seit 1994 bestehende Richtlinie des Bistums Hildesheim regelt den Umgang und die Nutzung dieser Daten. Beschwerden wurden daher, unter Hinweis auf die Rechtslage abgewiesen.

Andererseits darf nicht verkannt werden, dass gerade die Hauswerbung von Betroffenen immer weniger akzeptiert wird. Der Vergleich mit „Drückerkolonnen" früherer Tage drängt sich hier leider schnell auf, auch wenn die Beteiligten zweifelsohne bemüht sind, diesen Ein-

druck zu vermeiden. Andere Formen der Werbung scheinen, von Ausnahmen abgesehen, weniger belastend zu sein.

3.1.2 Unverlangtes Probeabonnement der Kirchenzeitung im Bistum Hildesheim

Als Alternative zur Haustürwerbung bieten sich in bestimmten Fällen Probeabonnements an. So fragte die Kirchenzeitung beim Diözesandatenschutzbeauftragten nach, ob Mitarbeitern der Caritas die Zeitschrift probeweise mit einem Anschreiben des Bischofs übersandt werden dürfe. Mit einer ähnlichen Aktion waren früher bereits einmal ehrenamtliche Mitarbeiter in den Pfarrgemeinden (Kirchenvorstände, Pfarrgemeinderäte) beworben worden. Problematisch ist dies einerseits wegen der Durchbrechung der Zweckbindung der Daten, die für die Durchführung des Dienstverhältnisses erhoben wurden, andererseits weil es naheliegt, hier eine direkte Verbindung zum Dienstverhältnis zu erkennen.

Eine Ausnahme vom Grundsatz der Zweckbindung besteht nach § 10 Abs. 2 Zi. 3 KDO in dem Fall, dass anzunehmen ist, dass die Weitergabe der Daten im Interesse der Betroffenen liegt, die hier die Möglichkeit erhalten sollten, die Zeitschrift zunächst einmal kostenlos und unverbindlich kennen zu lernen. Diese Voraussetzung ist aber nur dann gegeben, wenn jeder „Datenabgleich" und jede Information des Dienstgebers über den Bezug der KiZ durch seine Mitarbeiter organisatorisch strikt ausgeschlossen wird, die Betroffenen also ohne moralischen Druck frei und unbeeinflusst über den Bezug entscheiden können. Im konkreten Fall ließen sich diese Bedingungen erfüllen. Zwar gab es danach eine Beschwerde von Seiten der Mitarbeitervertretung des Ortsverbandes Hildesheim, die aber nach Aufklärung über die organisatorischen Rahmenbedingungen nicht weiter verfolgt wurde.

3.1.3 Telefonaquisition

Ohne vorherige Rücksprache hat die Kirchenzeitung Empfänger von Probeabonnements angerufen, um telefonisch nachzufragen, wie die Zeitschrift gefalle und ob Interesse an einem weiteren Bezug bestehe. Prompt gingen beim Diözesandatenschutzbeauftragten hierzu eine Reihe von Beschwerden Betroffener ein. Der Unterzeichner war daher gezwungen, die Verantwortlichen auf die verschärften Vorschriften des Gesetzes gegen den unlauteren Wettbewerb aufmerksam zu machen, die genau dieses Verhalten als unzumutbare Belästigung des Verbrauchers mit einem Bußgeld bedrohen. Eine telefonische Kontaktaufnahme ist seither nur noch mit ausdrücklicher, vorheriger Zustimmung der Betroffenen erlaubt. Die Kirchenzeitung hat zugesagt, solche Aktionen künftig zu unterlassen.

3.1.4 Datenschutzrechtliche Beurteilung von „e-mip"

Die Pfarrgemeinden in den Bistümern, die die Verarbeitung der Meldedaten dem Kirchlichen Rechenzentrum in Mainz übertragen haben, arbeiten mit der Software „e-mip". Dort wurde nunmehr die Möglichkeit geschaffen, die Gemeindemitgliederdatei nicht mehr auf dem eigenen Rechner vorhalten zu müssen, sondern diese online auf dem Rechner des Rechenzentrums einsehen und dort auch entsprechende Auswertungen erstellen zu können. Die Ver-

bindung wird durch das Programm „e-mip" hergestellt. Die Übertragung erfolgt verschlüsselt. Der Unterzeichner hat sich vom Bistum Hildesheim einen Zugangscode geben lassen, um sich selbst von der datenschutzgerechten Arbeitsweise dieses Verfahrens überzeugen zu können. Hierüber wurde ein Bericht erstellt, der zu dem Ergebnis kommt, dass das Verfahren in seiner derzeitigen Form nicht zu beanstanden ist.

3.2 Seelsorge

3.2.1 Veröffentlichung personenbezogener Daten im Pfarrbrief

Im Gegensatz zu früheren Jahren, bereitet die Veröffentlichung personenbezogener Daten im Pfarrbrief immer seltener Schwierigkeiten. Hier gibt es kaum noch Beschwerden. Der Unterzeichner führt dies darauf zurück, dass die nunmehr seit Jahren praktizierte „Widerspruchslösung" mittlerweile allgemein bekannt ist und wohl auch Akzeptanz gefunden hat.

Lediglich eine Beschwerdeführerin aus Bad Nenndorf sah das anders. Sie hatte wohl über Jahre hinweg, ihr wahres Alter den Freunden und Bekannten verschwiegen und fühlte sich nunmehr „geoutet". Den Pfarrbrief erhielt sie regelmäßig, in dem auch der Hinweis auf das Widerspruchsrecht veröffentlicht worden war. Von dieser Möglichkeit hatte sie dennoch keinen Gebrauch gemacht. Trotzdem gab der Fall Veranlassung darüber nachzudenken, ob die Widerspruchslösung wirklich ausreichend ist. Immerhin geht es hier um eine Güterabwägung zwischen dem seelsorgerischen Anliegen der Pfarrgemeinde und dem Geheimhaltungsinteresse des Einzelnen. Ich hatte daher den Priesterrat des Bistums Hildesheim gebeten, die Sache zu erörtern und eine gemeinsame Haltung zur Frage nach der Bedeutung des seelsorgerischen Anliegens in diesen Fällen zu finden. Dieser hat sich ausführlich mit der Sache befasst und mir das Ergebnis seiner Erörterungen schriftlich zur Verfügung gestellt. Hierin sind ausreichende Gründe für die Aufrechterhaltung dieser seit Jahren geübten seelsorgerischen Praxis benannt worden. Dementsprechend wird der Unterzeichner auch in Zukunft Beschwerden zurückweisen, wenn zuvor auf die geplante Veröffentlichung im Pfarrbrief hingewiesen wurde.

Anders sieht es mit der Veröffentlichung personenbezogener Daten im Internet, als auf der Homepage der Kirchengemeinde aus. Dabei liegt das Augenmerk vor allem auf der Verbreitung von Fotos von Gemeindefesten, Fronleichnamsprozessionen, etc. Die besonderen Gefahren des Internets führen in diesen Fällen dazu, dass die schriftliche Einwilligung der Betroffenen eingeholt werden muss. Näheres hierzu wurde schon unter Zi. 2.2 in diesem Bericht erläutert.

3.2.2 Veröffentlichung personenbezogener Daten durch E-Mail

Aus Magdeburg erreichte mich eine Beschwerde, weil ein Rundmail mit einer Einladung an Kommunion- und Diakonatshelfer die Empfänger unter „CC" (Carbon Copy) auswies, so dass jeder der Angeschriebenen über die Mailadressen der übrigen Empfänger unterricht wurde. Für eine solche ungewollte oder gewollte Datenübermittlung besteht weder eine

Rechtsgrundlage noch lag das Einverständnis der Betroffenen hierfür vor. Zudem war sie auch nicht erforderlich, weil ein Eintrag der Adressen unter „BC" (Blind Copy) ohne Schwierigkeiten zu einer Vermeidung dieses Ergebnisses geführt hätte. Für die Betroffenen führt eine solche Verfahrensweise meist zu einer erheblichen Zunahme von Spam-Mails. Hier ist für die Zukunft mehr Achtsamkeit erforderlich.

3.2.3 Seelsorge im Krankenhaus

Art. 140 GG in Verbindung mit Art. 141 der Weimarer Reichsverfassung garantiert den öffentlich-rechtlichen Religionsgesellschaften das Recht zur Vornahme seelsorgerischer Handlungen in Krankenanstalten, wobei jeder Zwang fernzuhalten ist. Schon lange wurde daher gemeinsam mit den Landesbeauftragten für den Datenschutz in den norddeutschen Bundesländern geklärt, dass ein Krankenhaus bei der Aufnahme eines Patienten nach dessen Religionszugehörigkeit fragen darf, wobei darauf hinzuweisen ist, dass diese Angabe freiwillig ist. Weiterhin ist der Patient zu befragen, ob er mit einer Weitergabe dieses Datums sowie seines Namens und der aufnehmenden Station/Zimmernummer an den zuständigen Krankenhausseelsorger einverstanden ist. Trotz dieser eindeutigen Lösung bestehen noch immer Unsicherheiten bei ihrer Umsetzung.

So wurde der Unterzeichner gelegentlich gebeten, bei der Abfassung entsprechender Formulierungen in Aufnahmeverträgen behilflich zu sein.

Nach wie vor kommen auch Anfragen, wie bei Patienten zu verfahren ist, die nicht ansprechbar sind. Hier ist über die engsten Angehörigen oder eine etwa getroffene Vorausverfügung der mutmaßliche Wille des Betroffenen zu ermitteln. Eine Sakramentsspendung (Krankensalbung) ohne solche Ermittlungen kann nur in unaufschiebbaren Notfällen in Betracht gezogen werden.

Der Unterzeichner wurde auch gefragt, ob die Auslage eines Gedenkbuches mit den Namen Verstorbener in der Krankenhauskapelle ausgelegt werden könne. Auch wenn sich der Schutz des Persönlichkeitsrechts auf lebende Personen bezieht, so erlischt dieses Recht auch nach dem Tode nicht vollständig und kann von den engen Angehörigen wahrgenommen werden. Seit der „Mephisto"-Entscheidung des Bundesverfassungsgerichts ist dies allgemein anerkannt. Die Eintragung eines Verstorbenen in ein Totengedenkbuch bedarf daher der Einwilligung der Angehörigen

Die Krankenhausseelsorge ist ein Angebot an die Patienten außerhalb des normalen Klinikbetriebs und steht somit auch außerhalb des heute im Gesundheitswesen erforderlichen Zeit- und Kostenmanagements. Eine Vergütung hierfür erfolgt weder durch den Patienten selbst, noch durch Krankenkassen oder –versicherungen. Gerade hieraus ergibt sich ihr wohltuender Effekt. Hier nimmt sich ein Mensch Zeit für die Hoffnungen, Sorgen und Nöte anderer Menschen, die sich in einer besonders schwierigen Situation befinden. Das Ansinnen einer neurologischen Klinik, auch seelsorgerische Gespräche einer EDV-mäßigen Erfassung als geleistete therapeutische Leistungen (KTL) am einzelnen Patienten mit Angabe von Häu-

figkeit und Dauer zuzuführen, war daher aus datenschutzrechtlicher Sicht unakzeptabel. Der zuständige Klinikseelsorger wurde entsprechend informiert und gebeten, die geforderten Angaben zu verweigern.

3.2.3 Videoüberwachung in der Kirche

An die Tatsache, dass viele öffentliche Plätze, U-Bahn-Stationen, Einkaufszentren und andere Orte videoüberwacht werden, haben sich viele Menschen längst gewöhnt. Aber Videoüberwachung auch in der Kirche? Der gute katholische Brauch, Kirchen auch tagsüber für Menschen zum Beten und zur Besinnung geöffnet zu halten, wird heutzutage durch Vandalismus und Diebstähle immer mehr in Frage gestellt. Und viele Kirchengemeinden sehen inzwischen nur dann noch die Möglichkeit, diesen Brauch fortzusetzen, wenn das Gebäude ausreichend geschützt werden kann. So fragen Kirchenvorstände immer wieder nach, ob eine Videoüberwachung zulässig ist. Dabei ist eine dauerhafte Beobachtung auf Grund der Personalsituation kaum möglich. Bleibt also nur die Aufzeichnung, um im Schadensfall die Täter wenigstens ausfindig machen zu können.

Die Rechtslage ist nach § 5a KDO zu beurteilen. Auch der Innenraum der Kirche ist ein öffentlich zugänglicher Raum, der von jedermann betreten werden kann. Die Videoüberwachung soll ja gerade dies ermöglichen und wird vielfach als wesentliche Voraussetzung für die Herstellung von Öffentlichkeit angesehen. Die Verhinderung von Diebstahl und Vandalismus gehört sicher auch zur Wahrnehmung berechtigter Interessen, wie § 5a Abs. 1 Zi. 2 KDO sie als Anlass fordert. Dennoch ist hier besondere Sensibilität gefragt. Zudem ergibt sich ein effektiver Schutz nur dann, wenn auch die Rahmenbedingungen entsprechend gestaltet werden können. In der Regel wird das dazu führen müssen, dass tagsüber nur ein Eingang zum Gotteshaus geöffnet bleibt. Dabei sind Seiteneingänge meist besser zu schützen, als der Haupteingang. Dort können Besucher erfasst werden, ohne sie beim Beten zu stören. Der Hauptraum kann mit einer Weitwinkelkamera ausgestattet werden, der die Personen (noch) nicht identifizierbar macht. Wird dort eine Straftat begangen, so lässt sich an Hand der Kamera im Eingangsbereich feststellen, welche Person unmittelbar danach die Kirche verlassen hat. Voraussetzung ist, dass Datum und Uhrzeit, wie üblich, mit aufgezeichnet werden. Auf diese Weise bleibt die Intimität des Betens erhalten. Selbstverständlich ist auch in diesen Fällen auf den Umstand der Überwachung hinzuweisen. Die Aufzeichnungen haben sich, spätestens nach 72 Stunden selbst zu überschreiben und der Zugriff auf die Aufzeichnungsgeräte ist klar zu regeln und für Dritte unzugänglich sein. Bei Beachtung dieser Grundsätze werden wir uns wohl auch an die Videoüberwachung in Kirchen gewöhnen müssen.

3.3 Kindertagesstätten

3.3.1 Weitergabe von Lerndokumentationen an Grundschulen

Kein Problem sah der Unterzeichner bei der Weitergabe von Lerndokumentationen der Kindertagesstätten an Grundschulen. Einerseits ist die Zusammenarbeit zwischen Kindergärten

und Grundschulen nunmehr in § 6 NSchG rechtlich verankert andererseits stellt auch der Runderlass des Kultusministeriums vom 2.5.2006 klar, dass vor der Datenübermittlung die Zustimmung der Erziehungsberechtigten eingeholt werden soll. Über Inhalte und Formen des Austausches von Informationen sollen sich die Eltern, die Fachkräfte des Kindergartens und die Lehrkräfte der Grundschule einvernehmlich verständigen. Diese Sichtweise entspricht der bisher schon in diesen Fällen vertretenen Auffassung.

3.3.2 Zusammenarbeit zwischen Kindergärten und Grundschulen

Mit der Neufassung des Niedersächsischen Schulgesetzes im Jahre 2003 ist auch die Zusammenarbeit zwischen den Grundschulen und Kindergärten gesetzlich verankert worden. Mit Runderlass vom 2.5.2006 hat das Niedersächsische Kultusministerium klargestellt, dass der Austausch über Beobachtungen und Erkenntnisse, die im Kindergarten zur Entwicklung und zum Lernverhalten von Kindern gewonnen worden sind, nur mit Zustimmung der Erziehungsberechtigten weitergegeben werden sollen. Ohne deren Einverständnis ist eine Weitergabe daher nur in schwerwiegenden Fällen möglich, in denen eine Verständigung mit den Eltern nicht zustande gekommen ist und das Kindeswohl dies erfordert.

3.4 Schulen

3.4.1 Weitergabe von Daten katholischer Religionslehrer

Das Niedersächsische Kultusministerium hatte sich, unter Berufung auf eine Stellungnahme des Niedersächsischen Landesbeauftragten für den Datenschutz geweigert, die Namen der tatsächlich an den Schulen des Landes eingesetzten katholischen Religionslehrer mitzuteilen. Begründet wurde dies damit, dass die Übermittlung dieser Daten nicht erforderlich sei, da ohnehin nur Lehrkräfte mit einer von den Bistümern erteilten Lehrerlaubnis (Missio Canonica) eingesetzt würden, deren Person dem entsendenden Bistum also ohnehin bekannt sei. Ich habe dem Landesbeauftragten für den Datenschutz daher mitgeteilt, dass die Approbation der Religionslehrer gemäß can. 805 CIC ein Recht des Ortsbischofs sei und jeweils nur für sein Bistum gelte. Bei einer Versetzung von Lehrkräften an eine Schule in den Bereich eines anderen Bistums werde jedoch häufig übersehen, dass die vorliegende Missio hierfür nicht mehr gültig sei. Die Beurteilung, ob die tatsächlich eingesetzten Lehrkräfte die Erlaubnis des zuständigen Bischofs besitzen, sei aber nur durch die erbetene Datenübermittlung möglich. Der Landesbeauftragte hat daraufhin seine Bedenken gegen die Weitergabe der gewünschten Daten nicht mehr aufrechterhalten.

3.4.2 Schulabgangsbefragung durch die Stadt Osnabrück

Im Rahmen einer Schulabgangsbefragung wurden auch Schulabgänger der Thomas-Morus-Schule in Osnabrück, zu ihrem schulischen und beruflichen Werdegang befragt. Wochen später wurde die Schule dann aufgefordert, Name, Anschriften, Geburtsort und Nationalität der Schulabgänger mitzuteilen, ohne dass klar war, für welchen Zweck diese Daten benötigt wurden. In Abstimmung mit dem Landesbeauftragten für den Datenschutz Niedersachsen

konnte festgestellt werden, dass eine Genehmigung der Schulaufsichtsbehörde für diese Befragung nicht vorgelegen hat und die Erhebung somit nur auf freiwilliger Basis möglich war. In den verteilten Fragebögen wurden die Angaben zur Person und ethnischen Herkunft unmittelbar abgefragt, so dass insoweit eine Datenübermittlung von Seiten der Schule nicht erforderlich war. Eine Übermittlung der Namen der Schüler, die nicht teilgenommen hatten, war in Zusammenhang mit der Freiwilligkeit bei der Teilnahme unstatthaft.

3.4.3 Weitergabe von Schülerdaten an katholische Kirchengemeinden

Um neu eingeschulte Kinder katholischen Bekenntnisses zu einer gemeinsamen Eucharistiefeier einladen zu können, bat das Katholische Pfarramt St. Bonifatius in Wunstorf die Leiter der Grundschulen um Bekanntgabe der Namen und Anschriften der Erstklässler. Eine Schule verweigerte die Auskunft. In Rücksprache mit der zuständigen Sachbearbeiterin beim Landesbeauftragten für den Datenschutz Niedersachsen konnte schnell geklärt werden, dass nur § 31 NSchG als Rechtsgrundlage für die gewünschte Datenübermittlung in Bertacht kam. Dort wird jedoch nur allgemein festgestellt, dass eine Verarbeitung der Schülerdaten zulässig sei, „soweit dies zur Erfüllung des Bildungsauftrags der Schule oder der Fürsorgeaufgaben, zur Erziehung oder Förderung der Schülerinnen und Schüler … erforderlich ist". Ich habe argumentiert, diese Formulierung decke durchaus auch eine Zusammenarbeit mit anderen Erziehungsträgern ab. Im Falle der Kirchengemeinde sei eine ergänzende religiöse Erziehung und die damit verbundenen Erlebnismöglichkeiten innerhalb einer Gruppe durchaus geeignet, die geistige Entwicklung und Heranbildung eines eigenen Wertesystems der Kinder zu fördern. Leider fand dieses Argument keine Zustimmung, obwohl der Werteverfall in unserer Gesellschaft immer wieder beklagt wird und die Schulen auf sich allein gestellt kaum die Möglichkeit haben werden, dies entscheidend zu ändern. Für die Kirche bleibt nur der Weg, über Gespräche mit dem Kultusministerium eine Änderung der Haltung in dieser Frage, gegebenenfalls auf dem Erlasswege, herbeizuführen.

3.4.4 Schulbezogene Gewaltprävention durch das Projekt „Balu und Du"

Der Caritasverband Hannover plante eine Beteiligung an dem Projekt „Balu und Du". Zur Verhinderung von Gewalt an Schulen sollten bestimmte auffällige Kinder von den Lehrkräften an eine Vermittlungsstelle, die Caritas gemeldet werden. Von dort aus sollten Paten gefunden werden, die diese Kinder während der Freizeit und bei der Erledigung der Hausaufgaben begleiten. Um Risiken des Kindesmissbrauchs auszuschließen sollte zuvor eine Überprüfung dieser Personen durch das LKA Niedersachsen stattfinden. Schließlich sollten die Paten Tagebücher/Verlaufsberichte führen, die von geschulten Experten ausgewertet werden sollten. Dabei stellten sich eine Reihe datenschutzrechtlicher Fragen bezüglich der Zusammenarbeit und des Datenaustausch verschiedener Stellen, die zum Teil den kirchlichen, in anderen Fällen aber den staatlichen Rechtsvorschriften unterlagen. Eine Klärung war daher nur in Abstimmung mit dem Landesbeauftragten für den Datenschutz Niedersachsen möglich. Nach intensiver Erörterung mit der zuständigen Sachgebietsleiterin beim LfD Niedersachsen ergab sich folgende Lösung:

- Die Teilnahme der Kinder an dem Projekt erfolgt freiwillig und nach umfassender Aufklärung und Belehrung der Sorgeberechtigten über das Verfahren und ihrer Einwilligung in die geplanten Datenweitergabe.
- Auch die Teilnahme der Paten an dem Projekt ist freiwillig. Eine polizeiliche Überprüfung darf nur aufgrund ihrer zuvor gegebenen Einwilligung erfolgen.
- Soweit eine Information des Jugendamtes erforderlich sein sollte, ist die Rechtmäßigkeit jeweils im Einzelfall noch einmal zu prüfen.

Unter Berücksichtigung dieser Punkte ergaben sich Seitens des LfD Niedersachsen und des Diözesandatenschutzbeauftragten keine datenschutzrechtlichen Bedenken gegen die Durchführung des Projekts.

3.5 Krankenhäuser

Staatliche und kirchliche Rechtsvorschriften sehen einheitlich vor, dass Krankenhäuser einen betrieblichen Datenschutzbeauftragten bestellen müssen. Für die Nordbistümer ist dies durch § 8 Abs. 2 der Krankenhausdatenschutzordnung vorgeschrieben. Gerade hier ist im Berichtszeitraum viel unternommen worden, um ein mehr an Kompetenz und Bereitschaft zur Übernahme dieser Aufgabe zu schaffen. An dieser Stelle darf hierzu auf die Ausführungen unter Ziffer 4.3 dieses Berichts verwiesen werden. Natürlich ist dies keine einmalige Sache. Die Betriebsbeauftragten wenden sich häufig mit den Fragen, die an sie herangetragen werden, an den Diözesandatenschutzbeauftragten, um sich rechtlich abzusichern. Insoweit besteht ein sehr intensiver Kontakt und eine sehr gute Zusammenarbeit. Die Folge ist, dass dem Unterzeichner nur selten Patientenbeschwerden zugehen.

Andererseits sind Krankenhäuser in dem sehr sensiblen Bereich des Gesundheitswesens tätig und erzeugen die Daten, die nach Auffassung der Europäischen Datenschutzrichtlinie, wie sie in § 9 Abs. 5 und § 10 Abs. 5 KDO ihren Niederschlag gefunden hat, besonders schützenswert sind. Daher wird gerade an dieser Stelle die Eigenständigkeit des kirchlichen Datenschutzes von den Kollegen in Bund und Ländern kritisch gesehen. Die Kirche muss gerade hier nachweisen, dass sie mit dem staatlichen Datenschutzniveau mithalten kann. Die noch laufenden Gespräche mit dem Berliner Datenschutzbeauftragten sind hierfür der beste Beleg. Insoweit darf auf die Darstellung unter Ziffer 5.4 dieses Berichts Bezug genommen werden.

3.5.1 Externe Archivierung von Patientenakten

Immer wieder wird danach gefragt, ob Patientenakten, Röntgenbilder und andere wichtige Unterlagen außerhalb der Einrichtung mit Hilfe hierauf spezialisierter gewerblicher Anbieter archiviert werden können. In all diesen Fällen handelt es sich um eine Auftragsdatenverarbeitung im Sinne von § 8 KDO, mit den entsprechend hohen Anforderungen an die Auswahl des Auftragnehmers und die technisch-organisatorischen Absicherungen zum Schutz der Daten. Im Gesundheitsbereich kommt jedoch hinzu, dass diese Daten strafrechtlich in besonderer Weise geschützt sind. So unterliegen Patientenakten, solange sie sich im Gewahr-

sam des Arztes oder der Krankenanstalt befinden nach § 97 Abs. 1 Nr. 3, Abs. 2 StPO im Strafverfahren einem Beschlagnahmeverbot. Die Auslagerung ganzer Akten oder Teilen hiervon führt daher notwendiger Weise zu einer wesentlichen Verschlechterung der Rechte des Patienten. Daher ist ein solches Verfahren an die schriftliche Einwilligung der Patienten gebunden, die zugleich über das beauftragte Unternehmen und die zum Schutz der Daten getroffenen Maßnahmen zu unterrichten sind. Will man diesen aufwändigen Weg nicht gehen, so bleibt nur die Verschlüsselung der Daten. Diese muss zwingend so vorgenommen werden, dass weder das Fremdunternehmen, noch die Staatsanwaltschaft sondern allein der zur Verweigerung des Zeugnisses berechtigte Auftraggeber die Möglichkeit der Entschlüsselung besitzt. Hierfür stehen inzwischen technische Verfahren zur Verfügung, die vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, der bisher einzigen Zertifizierungsstelle in Deutschland, mit einem Gütesiegel versehen worden sind. Die anfragenden Einrichtungen wurden über diese Zusammenhänge informiert und aufgefordert, zertifizierte Verfahren einzusetzen.

3.5.2 Externe Abrechnung von Notfallscheinen

Die neue Regelung in § 120 Abs. 6 SGB V gestattet, die Abrechnung von im Notfall erbrachten ambulanten ärztlichen Leistungen mit den Kassenärztlichen Vereinigungen auf andere Stellen zu übertragen. Auftraggeber und Auftragnehmer unterliegen dabei ausdrücklich der Aufsicht, der nach § 38 BDSG zuständigen Stelle. Für kirchliche Kliniken ist dies der Diözesandatenschutzbeauftragte.

Bei der Auftragserteilung sind dabei vor allem die strengen Anforderungen des § 80 SGB X zu beachten. So sind in dem schriftlich zu erteilenden Auftrag die Datenerhebung, -verarbeitung und –nutzung, die technisch-organisatorischen Maßnahmen zu ihrem Schutz und etwaige Unterauftragsverhältnisse festzulegen. Dem Auftragnehmer sind dabei umfassende Kontrollrechte einzuräumen. Zwei Berliner Krankenhäuser haben in diesem Bereich einen gewerblichen Drittanbieter beauftragt. Eine Durchsicht der Verträge ergab, dass diese nicht den Anforderungen des § 80 SGB X genügten. Der Unterzeichner hat die Häuser daher aufgefordert, die Verträge im Sinne der gesetzlichen Vorschriften nachzubessern. Darüber hinaus hat der Unterzeichner den Vorschlag gemacht, gemeinsam mit den Betriebsbeauftragten die Datenverarbeitungseinrichtungen des Auftragnehmers vor Ort in Augenschein zu nehmen und sich von der Einhaltung der Vereinbarungen zu überzeugen. Die betroffenen Einrichtungen haben entsprechende Zusagen gegeben.

3.5.3 Outsourcing des Patiententransportdienstes

Aus betriebswirtschaftlichen Gründen werden immer mehr nichtärztliche Leistungen im Krankenhaus auf Drittanbieter übertragen. So hat im Hamburger Marienkrankenhaus ein Fremdunternehmen das Management des Patiententransportdienstes übernommen. Daher stellte sich die Frage, ob die Auftragnehmerin auch Zugriff auf das Dienstplanprogramm der Einrichtung, das seinerseits mit den Personalstammdaten und dem Personalabrechnungs-

system verknüpft ist, erhalten solle. Es konnte geklärt werden, dass eine Einsichtnahme dieses Umfanges nicht erforderlich ist und somit zu unterbleiben hat.

3.5.4 WLAN im Krankenhaus

Ein Hamburger Krankenhaus fragte an, unter welchen Umständen die Einrichtung eines WLAN zulässig sei, mit dem man Patienten die Möglichkeit geben wolle, unter Benutzung eigener Endgeräte Internetdienste in Anspruch nehmen zu können. Von den Patienten soll hierfür ein Entgelt erhoben werden. Der Diözesandatenschutzbeauftragte gab zunächst folgende Hinweise:

- Wer einen solchen „Hotspot" einrichtet betreibt geschäftsmäßig einen Telekommunikationsdienst im Sinne des Telekommunikationsgesetzes, so dass die Datenschutzvorschriften der §§ 91 – 107 TKG einzuhalten sind.
- Das WLAN muss eine nach heutigem technischen Stand eine sichere Verschlüsselung bieten (WPA 2)
- Es muss sichergestellt sein, dass kein Anwender die Möglichkeit hat, auf den Rechner eines anderen Anwenders zu gelangen (sog. „User Isolierung")
- Die Anmeldung zum Netz muss auf einer sicheren Seite (Secure Socket Layer) erfolgen.
- Der Nutzer muss über den Umfang der gespeicherten Daten und die getroffenen Schutzmaßnahmen vor Inanspruchnahme der Dienste unterrichtet werden.

Da sich die Überlegungen hierzu noch im Planungsstadium befinden, hat der Datenschutzbeauftragte der Klinik zunächst die WLAN-Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik zur Verfügung gestellt und auf die dortigen Spezifikationen hingewiesen.

3.5.5 Befragung Berliner Krankenhäuser

Zum Ende des Berichtszeitraums hat der Diözesandatenschutzbeauftragte den kirchlichen Krankenhäusern im Erzbistum Berlin einen Fragebogen übersandt, mit dem er sich Aufklärung über die eingesetzten Klinikinformationssysteme, den Umfang der Auslagerung bestimmter Tätigkeiten (Outsourcing) und den Einsatz von Videoüberwachung verschaffen will. Nach Auswertung der Informationen sollen zunächst die Auftragsdatenverarbeitungen an Hand der abgeschlossenen Verträge überprüft werden. Weitere Maßnahmen sollen dann, je nach dem festgestellten Bedarf erfolgen.

3.6 Soziale Einrichtungen

3.6.1 Heimaufsicht

Nach wie vor bestehen Unsicherheiten auf Seiten der Leistungserbringer, wenn es um die Rechte der Heimaufsicht geht, obwohl durch die Neufassung des Heimgesetzes insoweit

klare rechtliche Vorgaben geschaffen worden sind. So enthält § 15 Abs. 1 Satz 5 HeimG nunmehr die Bestimmung, dass die erforderlichen Auskünfte mündlich oder schriftlich eingeholt werden können. Die weitere Regelung, dass der Träger des Heimes die Unterlagen am Ort der Prüfung vorzuhalten habe, ist nur eine Ergänzung, die Prüfungen vor Ort erleichtern soll, ohne die Aufsichtsbehörde auf diese Verfahrensweise zu beschränken. Entsprechend wurde die anfragende Caritasstiftung Oldenburg gebeten, die Anfrage der Stadt Oldenburg im verlangten Umfang zu beantworten.

3.6.2 Zentrale Datenverarbeitung für zehn Beratungsstellen

Die Mitarbeitervertretung Psychologische Beratungsstellen im Bistum Osnabrück fragte an, ob die Einrichtung eines zentralen Terminalservers für die Datenverarbeitung in 10 Einrichtungen zulässig sei. Soweit hierdurch Kosteneinsparungen erzielt werden können, will der Datenschutz dies keineswegs verhindern. Es muss jedoch gewährleistet sein, dass die Mitarbeiter weiterhin nur auf die Daten zugreifen können, die für ihre Arbeit erforderlich sind. Dies setzt eine eingehende Rechteverwaltung und ein klar geregeltes Vergabeverfahren voraus. Selbstverständlich müssen auch die Übertragungswege zwischen dem Server und den Arbeitsplatzrechnern (Clients) gesichert sein. Hier bietet sich die Verschlüsselungstechnik an. Hier konnten die Hinweise des Bremischen Datenschutzbeauftragten zur technischen Umsetzung genutzt werden.

3.6.3 Videoüberwachung im Seniorenwohnheim

Die Videoüberwachung hält auch in sozialen Einrichtungen Einzug. Zwei Häuser in Hamburg hatten Probleme mit Diebstählen und Vandalismus. In einem Fall war ein nahegelegenes Seemannsheim der Grund für häufige Straftaten zu Lasten des Eigentums der Bewohner. Mit einer Überwachung des Eingansbereichs bei gleichzeitiger Beobachtung und Aufzeichnung sollte eine Verbesserung der Situation erreicht werden. Der Unterzeichner hat sich die räumlichen Gegebenheiten vor Ort angesehen und gemeinsam mit der Verwaltungsleitung nach einer datenschutzgerechten Lösung gesucht. Die Kamera ließ sich so justieren, dass ausschließlich das Betreten und Verlassen des Hauses erfasst wurde. Durch Beobachtung konnte schnell auf unerwünschte Besucher zugegangen werden. Die Aufzeichnungen standen für eine trotzdem notwendige Strafverfolgung zur Verfügung. In Absprache mit den Mitarbeitern konnte sichergestellt werden, dass eine Überprüfung des Arbeitsverhaltens ausgeschlossen ist. Unter diesen Umständen hatte der Datenschutzbeauftragte keine Bedenken. Die Situation hat sich seither auch wesentlich gebessert.

3.6.4 Altenhilfeeinrichtung als verlängerter Arm der GEZ

Die Gebühreneinzugszentrale wollte von einem Heimbetreiber die Namen der Bewohner, die nicht über die Heimleitung als Rundfunkteilnehmer angemeldet worden waren, um deren Anmeldepflicht überprüfen zu können. Eine solche Datenübermittlung, so hilfreich sie auch sein mag, ist allerdings unzulässig. Einerseits widerspricht sie der Zweckgebundenheit, da sie nur für die Verwaltung des Heimes erhoben wurden, andererseits ist sie auch nicht er-

forderlich, da sich die GEZ über die ihr zur Verfügung gestellten Meldedaten ausreichend informieren kann.

3.6.5 Prüfung der Stiftung St. Pius Stift in Cloppenburg

Das St. Pius Stift betreibt ein Altenheim, eine Tagespflegeeinrichtung und eine Altenpflegeschule in Cloppenburg. Anfang 2006 wurde dort eine umfassende Prüfung der Datenverarbeitung vor Ort vorgenommen. Sämtliche eingesetzten Verfahren zur Verarbeitung der Personal- und Bewohnerdaten sowie die Videoüberwachung des Eingangsbereichs wurden einer getrennten Betrachtung unterzogen und auf mögliche Schwachstellen untersucht. Beanstandet wurde die nicht ordnungsgemäße Dokumentation der Auftragsdatenverarbeitungen mit der ITEBO und dem Caritasverband Vechta wie auch die fehlenden Verfahrensdokumentationen nach § 3a KDO. Darüber hinaus lagen für ein Teil der Mitarbeiter keine Verpflichtungserklärung nach § 4 KDO vor. Die Beanstandungen wurden inzwischen beseitigt.

Der technische Ablauf der Verarbeitungsverfahren war erfreulicherweise nicht zu beanstanden. Der Einrichtung wurde trotzdem empfohlen, eine komplette Grundschutzprüfung nach dem Handbuch des BSI durch ein Auftragsunternehmen durchführen zu lassen, um eventuell verdeckte Schwachstellen ausfindig zu machen.

3.7 Personalangelegenheiten

3.7.1 Mitwirkung beim Abschluss von Dienstvereinbarungen

Eine Reihe von Angelegenheiten des Arbeitslebens können im Wege einer Dienstvereinbarung zwischen dem jeweiligen Dienstgeber und der Mitarbeitervertretung geregelt werden. Die Vorteile einer solchen Regelung liegen klar auf der Hand: Eine einvernehmliche Regelung bezieht die fachliche Kompetenz der Mitarbeiter mit ein, stärkt das Vertrauen in die Zusammenarbeit und fördert das Bewusstsein, als Dienstgemeinschaft zusammen zu wirken. Soweit dabei auch die Verarbeitung personenbezogener Daten geregelt wird, stellt die Dienstvereinbarung auch eine Rechtsgrundlage im Sinne von § 3 Abs. 1 Nr. 2 KDO dar. In den Fällen, in denen weder spezielle Rechtsvorschriften noch die KDO selbst die geplante Datenverarbeitung gestatten, ist sie sogar der einzige Weg, der Schaffung der notwendigen Rechtsvorschrift (Beispiel: Personalinformationssysteme). Andererseits dürfen Dienstvereinbarungen bestehenden Rechtsnormen nicht widersprechen (§ 38 Abs. 3 MAVO). Die Grundlagen des Datenschutzes und das Recht auf informationelle Selbstbestimmung der Mitarbeiter, sind beim Aushandeln der jeweiligen Arbeitsbedingungen ebenso zu berücksichtigen, wie bestehende Arbeitsvertragsordnungen. Aus datenschutzrechtlicher Sicht ist vor allem die Regelung jener Angelegenheiten im Sinne von § 38 Abs. 1 der Rahmenordnung für eine Mitarbeitervertretungsordnung (MAVO) von Bedeutung, in denen es um den Inhalt von Personalfragebögen (§ 38 Abs. 1 Nr. 5 MAVO) sowie die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Mitarbeiterinnen und Mitarbeiter zu überwachen (§ 38 Abs. 1 Nr. 9 MAVO) geht. In der Praxis kommt es daher häufig zum Abschluss von Betriebsvereinbarungen über die Einführung von

Arbeitszeiterfassungssystemen und die Einrichtung von Arbeitsplätzen mit Nutzung von Internet, E-Mail und Intranet. Zu den Aufgaben des Diözesandatenschutzbeauftragten gehört es zu prüfen, ob die geplanten Regelungen mit dem Recht der Mitarbeiter auf informationelle Selbstbestimmung konform gehen.

Sehr häufig wird der Unterzeichner um Mitwirkung bei Dienstvereinbarungen über die Nutung von Internet und E-Mail am Arbeitsplatz gebeten. Wird die Privatnutzung dieser Systeme vollständig ausgeschlossen, sind größere datenschutz- oder steuerrechtliche Probleme nicht zu erwarten. Hier kann durchaus auf Musterdienstvereinbarungen zurückgegriffen werden. Aber auch die Vereinbarung einer Privatnutzung in geringem Umfang, die steuerrechtlich noch nicht als geldwerter Vorteil anzusehen ist, ist möglich. Die Folge einer solchen Vereinbarung ist, dass der Dienstgeber zum Diensteanbieter im Sinne von § 11 Abs. 1 Telemediengesetz (TMG) wird und daher auch die Datenschutzvorschriften dieser Norm zu beachten hat. Damit unterliegen die Bestands- und Nutzungsdaten der Mitarbeiter dem Schutz der §§ 14, 15 TMG und dürfen nur zum Zwecke der Vertragsanbahnung und –gestaltung sowie zur Ermöglichung der Inanspruchnahme der Telemedien genutzt werden. In diesem Falle gilt es also, dienstliche und private Nutzung streng voneinander zu trennen. Zudem gilt das Fernmeldegeheimnis auch in diesem Bereich. Im Bistum Osnabrück hatte man damit Probleme.

Im Falle der Dienstvereinbarung über die Nutzung von Internet, Intranet und E-Mail zwischen dem Bistum Osnabrück und der Mitarbeitervertretung der Laienmitarbeiterinnen und Laienmitarbeiter im Bistum Osnabrück sollten alle ein- und ausgehenden E-Mails als dienstlich angesehen und vom Dienstgeber geöffnet werden dürfen, obwohl eine private Nutzung in geringem Umfange erlaubt werden sollte. Der Unterzeichner hat darauf hingewiesen, dass ein genereller Verzicht auf die Wahrung des Fernmeldegeheimnisses nicht statthaft und strafrechtlich auch ohne Belang ist. Eindeutig als privat erkennbare Post darf demnach nicht geöffnet und gelesen werden.

Eine Privatnutzung dienstlicher Internetzugänge ist heute nicht mehr erforderlich und sollte daher nach Möglichkeit vermieden werden. Fast jedes Handy kann heute auch als E-Mail-Client zum Empfang und Versand von Mails verwendet werden. Das Angebot der Mobilfunkbetreiber an preiswerten Flatrates wächst ständig. So kann bei Telefonica Deutschland o2 ein Datenvolumen von 30 MB für € 5,- monatlich hinzugebucht werden. Damit lassen sich bereits mehrere hundert Mails im Monat übertragen. Eine unbegrenzte Internetnutzung über UMTS gibt es für € 10 /Mt., die sich per UMTS-Stick auch auf Netbooks oder Notebooks nutzen lässt. Andere Anbieter haben ähnliche Tarife. Angesichts der Tatsache, dass es in Deutschland mehr registrierte Handys als Einwohner gibt, dürfte mit hoher Wahrscheinlichkeit jeder Mitarbeiter auch privat über ein entsprechendes Gerät verfügen.

3.7.2 Ehrenamtsbefragung durch das Institut für Demoskopie in Allensbach

Im Auftrag des Deutschen Caritasverbandes sollte das Institut für Demoskopie in Allensbach eine Studie über ehrenamtliche Tätigkeit im Bereich der Caritas durchführen und hat hierzu

940 Personen befragt. Zur Absicherung der dabei erzielten Ergebnisse sollten nun auch die hauptamtlichen Mitarbeiter zu ihren Erfahrungen in der Zusammenarbeit mit Ehrenamtlichen befragt werden. Eine Reihe von Krankenhäusern wurde daher angeschrieben und gebeten eine vollständige Liste aller hauptamtlichen Mitarbeiter zur Verfügung zu stellen, damit hieraus 300 Personen nach dem Zufallsprinzip ausgewählt werden können. Mehrere Häuser fragten daher an, ob eine solche Datenübermittlung überhaupt zulässig sei. Ihnen wurde mitgeteilt, dass es für diese Verfahrensweise keine Rechtsgrundlage gebe und die Weitergabe von Personaldaten daher nur mit ausdrücklicher Zustimmung der Betroffenen statthaft sei.

3.7.3 Aufbewahrung von Protokollen von Mitarbeiterjahresgesprächen

Zum Zwecke der Personalentwicklung und Personalführung hat sich, neben anderen Instrumenten, das Mitarbeiter-Vorgesetzten-Gespräch (MAVG) etabliert. Hierdurch ergibt sich die Möglichkeit, Stärken der Mitarbeiter zu erkennen und zu fördern, Fragen der Zusammenarbeit zu klären, die Zielorientierung zu erhöhen, notwendigen Entwicklungsbedarf konstruktiv anzusprechen und ein Feedback zum Führungsverhalten des Vorgesetzten zu bekommen. Über diese Gespräche wird in der Regel ein Protokoll angefertigt, dass sowohl dem Vorgesetzten, wie auch seinem Mitarbeiter ausgehändigt wird, damit sie jeweils nachvollziehen können, worüber gesprochen wurde. Wurde eine Vereinbarung getroffen, so ist diese in jedem Fall schriftlich festzuhalten und von beiden Seiten zu unterschreiben.

Die Mitarbeitervertretung im Erzbischöflichen Generalvikariat Hamburg wollte nun wissen, ob diese Protokolle nicht in die Personalakte gehören, weil sie nur dort ausreichend geschützt seien. Da in der Hamburger Verwaltung schon länger Erfahrungen mit dem MAVG bestehen, hat der Unterzeichner in diesem Falle Kontakt mit der zuständigen Sachgebietsleiterin beim Hamburgischen Datenschutzbeauftragten aufgenommen, um zu erfahren, welche Handhabung dort besteht. Das Ergebnis dieses Gesprächs war, dass der Inhalt des Protokolls, bzw. einer getroffenen Vereinbarung zwischen den Gesprächspartnern vertraulich behandelt werden muss. Deshalb müssen diese Unterlagen in jedem Fall für Dritte unzugänglich aufbewahrt werden. Eine Weitergabe einzelner Informationen darf nur erfolgen, wenn dies zum Vollzug einer getroffenen Vereinbarung erforderlich ist und zuvor mit dem Mitarbeiter abgesprochen wurde. Auf keinen Fall gehören solche Vereinbarungen und Protokolle in die Personalakte! Beim nächsten Gespräch sollten die Vereinbarungen gemeinsam überprüft und die Protokolle anschließend vernichtet (geshreddert) werden. Das EGV wurde von dieser Rechtslage unterrichtet.

3.7.4 Weitergabe von Arztunterlagen bei Wechsel des Betriebsarztes

Ein Alten- und Pflegeheim wechselte den Betriebsarzt. Dabei sollten die ärztlichen Unterlagen an den neuen Arzt weitergegeben werden. Allen Beteiligten war klar, dass dies nur mit Einwilligung der betroffenen Mitarbeiter geschehen durfte, so dass auch entsprechende Einwilligungserklärungen eingeholt werden sollten. Die vorbereiteten Erklärungen enthielten jedoch den Passus, dass die Weitergabe über die Heimleitung erfolgen sollte. Der Unter-

zeichner wies in diesem Fall daraufhin, dass die Möglichkeit einer Einsichtnahme in die Akten durch die Heimleitung strikt ausgeschlossen werden müsse. Das sei in der Regel nur bei einer direkten Weitergabe von Arzt zu Arzt gewährleistet.

3.7.5 Weitergabe von Vergütungslisten an die MAV

Aus dem Bistum Osnabrück kam eine Anfrage der Mitarbeitervertretung, ob der Dienstgeber berechtigt sei, ihr Bruttolohn- und Gehaltslisten der Mitarbeiter zur Verfügung zu stellen. Der MAV kam es darauf an, zuverlässiges Material in die Hand zu bekommen, um abschätzen zu können, welche Auswirkungen und Einsparpotentiale die Anwendung der Öffnungsklausel für den einzelnen Mitarbeiter hat. Zur effektiven Wahrnehmung ihrer Aufgaben ist ein Aushändigen dieser Listen nicht erforderlich und auch nicht von § 26 Abs. 2 MAVO gedeckt. Zulässig ist jedoch eine Einsichtnahme in Anwesenheit des Dienstgebers oder eines von ihm bestimmten Vertreters, um die Richtigkeit des verwendeten Zahlenmaterials überprüfen zu können.

4. Öffentlichkeitsarbeit / Unterrichtung der Dienststellen

4.1 Internetauftritt

Angesichts des immer komplizierter werdenden Rechts und der gewachsenen technischen Risiken, wird die Schulung und Unterrichtung der Mitarbeiter in kirchlichen Dienststellen und Einrichtungen immer wichtiger. Durch Vorträge und Gespräche vor Ort kann das Bewusstsein für den Datenschutz verbessert werden. Ein langfristiger Erfolg ist jedoch nur dann zu erwarten, wenn sich die Unterrichtung auch im Arbeitsalltag fortsetzt. Mitarbeiter müssen die Möglichkeit haben, sich jederzeit schnell und gezielt über die geltenden Datenschutzregeln zu informieren. In dieser Hinsicht bietet eine Informationsseite im Internet ein Höchstmass an Aktualität, direkter Erreichbarkeit und Schnelligkeit („Information at your fingertips"). Die vom Datenschutzbeauftragten der norddeutschen Bistümer verantwortete Website ist die zurzeit immer noch einzige Datenschutzhomepage im Bereich der katholischen Kirche in Deutschland.

Es macht daher Sinn, dieser Seite besondere Beachtung zu schenken. Gegenüber den früheren Versuchen des Unterzeichners, die Homepage selbst zu entwickeln und zu pflegen, wird diese nunmehr seit Frühjahr 2004 von der Bernward Medien Gesellschaft und in ihrem Auftrag von Herrn Mehring betreut. Hierdurch ist klar erkennbar ein „mehr" an professioneller Gestaltung und Aufbereitung der Informationen hinzugekommen. Die inhaltliche Verantwortlichkeit und das halte ich für unabdingbar, liegt nach wie vor beim Unterzeichner. Zuletzt ist die Seite im Oktober 2006 einem gründlichen Relaunch unterzogen worden. Hierdurch ist eine Reihe von Verbesserungen erfolgt:

- alle Informationen, einschließlich der pdf-Dateien sind nunmehr barrierefrei und somit auch Menschen mit starker Sehbehinderung und Blinden, die auf spezielle Browser zum Vorlesen des Quellcodes angewiesen sind, ungehindert zugänglich;

- die Schriftgröße kann den Sehgewohnheiten individuell angepasst werden;
- es gibt zu jeder Seite eine Druckansicht, die dem Nutzer eine weitere Verwendung der Informationen in seinem beruflichen Umfeld erleichtert;
- durch Neustrukturierung der Websites sind die Informationen besser und schneller auffindbar;
- der Wunsch der Bistümer, die Gesetzestexte nach regionalen Gesichtspunkten zu ordnen, damit die Mitarbeiter, die für ihre Diözese geltenden Vorschriften schneller zur Hand haben, wurde umgesetzt.

Eine weitere wesentliche Neuerung und Verbesserung ist das Angebot von Online-Formularen zur Abgabe der Verfahrensmeldung nach § 3a KDO, des Verfahrensverzeichnisses und der Verpflichtungserklärungen nach § 4 KDO. Hierbei wurde Wert darauf gelegt, dass die Formulare nicht zuerst ausgedruckt und dann von Hand ausgefüllt werden müssen, sondern bereits am Bildschirm elektronisch bearbeitet werden können. Das so erstellte Verfahrensverzeichnis lässt sich anschließend mit einem einfachem Mausklick als Email an den Diözesandatenschutzbeauftragten versenden und als Beleg für die eigene Akte vollständig ausdrucken. Auch die anderen Formulare lassen sich online bearbeiten und anschließend drucken. Ein Versand ist hier nicht erforderlich. Neben der Einsparung von Druckkosten dürfte diese Verfahrensweise auch eine erhebliche Erleichterung für Dienststellen und Einrichtungen darstellen.

Die Qualität der Homepage ist auch die Voraussetzung für eine Mitarbeit des Datenschutzbeauftragten der norddeutschen Bistümer als Projektpartner im Virtuellen Datenschutzbüro (www.datenschutz.de). Hierzu werde ich unter Zi.5.5 berichten.

Die Homepage „Datenschutz in der Katholischen Kirche" hat sich in den zurückliegenden Jahren zu einem wichtigen Instrument der Unterrichtung kirchlicher Dienststellen in Fragen des Datenschutzes entwickelt. Sie ist gleichzeitig ein Instrument, das das Vorhandensein und die Qualität kirchlichen Datenschutzes stärker in das Bewusstsein der Öffentlichkeit rückt. Es wird auch in Zukunft zu den wichtigen Aufgaben gehören, diese Seite auszubauen und zu pflegen.

4.2 Broschüren, Handreichungen

Gegenüber dem Internetauftritt hat die Informationsverbreitung durch Printmedien wesentlich an Bedeutung verloren. Der gelbe Loseblattordner „Kirchlicher Datenschutz" wird daher schon seit einiger Zeit nicht mehr fortgeführt. Zu groß ist der Aufwand an Zeit und Geld, um solche Veröffentlichungen durch Erstellung und Verteilung von Nachlieferungen stets aktuell zu halten. Zudem haben heute fast alle kirchlichen Einrichtungen Zugang zum Internet, so dass die jeweils gültigen Texte dort eingesehen, herunter geladen und im Bedarfsfall ausgedruckt werden können.

Sinn machen Broschüren dort, wo ehrenamtliche Mitarbeiter mit den Vorschriften bekannt gemacht werden müssen. Das Bistum Hildesheim hat hierfür einen Ringordner „Handbuch für Kirchengemeinden – Rechtsvorschriften" herausgegeben, der unter anderem auch ein Heft mit den Vorschriften zum Datenschutz enthält. Dieser Ordner wird insbesondere an Kirchenvorstände und Pfarrgemeinderäte verteilt. Auch andere Diözesen haben ihre Vorschriften in gedruckter Form publiziert.

Die Deutsche Bischofskonferenz hat die gemeinsamen Vorschriften, KDO, KMAO und die Anordnung zum Sozialdatenschutz mit den Entwurfstexten und jeweils sehr eingehenden Ausführungen von Herrn Dr. Hammer (KDO) und Herrn Fischer (KMAO) als Arbeitshilfe Nr. 206 unter dem Titel „Datenschutz und Melderecht der katholischen Kirche 2006" veröffentlicht. Auch hierauf kann jederzeit zurückgegriffen werden.

Weitere wichtige Arbeitshilfen aus der gleichen Schriftenreihe sind die Broschüren „Zeugenaussage, Zeugnisverweigerungsrecht und Schweigepflicht - Ein juristischer Leitfaden für Seelsorger zum Schutz des Beicht- und Seelsorgegeheimnisses" (AH Nr. 222 vom 1. Januar 2008) und „Internetpräsenz" (AH Nr. 234 vom 22. Juni 2009).

Mit den genannten Broschüren dürfte der Bedarf an schriftlich vorliegenden Versionen der Gesetzestexte abgedeckt sein. Der Unterzeichner sieht zurzeit keine Veranlassung, über seine Vortragsmanuskripte hinaus, Informationen in gedruckter Form herauszugeben.

4.3 Schulungen und Vorträge

Neben der Unterrichtung der Dienstellen und Einrichtungen über das Internet und durch Printmedien, bleibt das persönliche Gespräch mit den Mitarbeitern im Rahmen von Schulungen und Vorträgen eine wichtige und wesentliche Aufgabe. Die Ziele und Aufgaben des Datenschutzes lassen sich so am besten und direktesten vermitteln. Das Datenschutzbewusstsein wird auf diese Weise gefördert und die Teilnehmer wirken in Einrichtungen oftmals als Multiplikatoren, die das erworbene Wissen und das tiefere Verständnis für die Zusammenhänge in die tägliche Arbeit hineintragen. Der zwangsläufig mit diesen Veranstaltungen verbundene Arbeits- und Kostenaufwand erscheint daher mehr als sinnvoll.

Seit der Schaffung der neuen KDO steht vor allem die Ausbildung betrieblicher Datenschutzbeauftragter im Vordergrund. Diesen müssen aber nicht nur juristische, sondern auch technische Grundkenntnisse vermittelt werden. Da den Diözesandatenschutzbeauftragten keine Mitarbeiter mit informationstechnischer Ausbildung zur Verfügung stehen, muss eine Kooperation mit anderen öffentlichen Stellen erfolgen. So hat sich der Verband der Diözesen Deutschlands auf Anregung des Unterzeichners entschlossen, gemeinsam mit der TüV-Akademie Rheinland Seminare anzubieten. Hierüber wurde bereits unter Zi. 1.2.1 berichtet.

Ein weiteres Beispiel für eine erfolgreiche Kooperation ist das vom Unterzeichner gemeinsam mit dem Datenschutzinstitut Niedersachsen (DIN) am 02./03. Mrz. 2005 durchgeführte Inhouse-Seminar für Betriebsbeauftragte in Krankenhäusern der Kongregation der Barm-

herzigen Schwestern vom Hl. Vinzenz von Paul. Den Seminaren des VDD vergleichbar, wurden die Teilnehmer hier an zwei Tagen fit gemacht. Den ersten Tag hatte der Unterzeichner übernommen, um über die wesentlichen Rechtsgrundlagen der Datenverarbeitung im Krankenhaus zu sprechen, am zweiten Tag informierte dann Herr Grabow (DIN) die Teilnehmer über die technisch-organisatorischen Fragen, während der Unterzeichner weiterhin für Fragen aus dem Bereich des kirchlichen Rechts zur Verfügung stand. Eine Reihe von Themen war bereits im Vorfeld mit dem Veranstalter abgestimmt worden, um möglichst praxisnahe Informationen vermitteln zu können. Diese Verfahrensweise hat sich als sehr effizient herausgestellt.

Selbstverständlich werden auch weiterhin Mitarbeiter geschult, die nicht als Betriebsbeauftragte tätig sind. Das Spektrum der angebotenen Vorträge reicht hier von der Schulung

- für Pfarrsekretärinnen (Erzbistum Berlin, Bistum Magdeburg),
- von Pastoral- und Gemeindereferenten (Erzbistum Hamburg)
- von Mitarbeitern in der stationären, bzw. ambulanten Pflege (Offizialat Vechta),
- von Krankenhausmitarbeitern (Bistum Hildesheim, Bistum Osnabrück),
- von Mitarbeitern in der Suchthilfe (alle Bist.),
- von Mitarbeitern in Werkstätten für psychisch Kranke (Offizialat Vechta)
- von Mitarbeitern der Caritasstiftung (Offizialat Vechta),
- von Lehrern an Schulen in kirchlicher Trägerschaft (Offizialat Vechta, Bistum Magdeburg)
- von Mitarbeitern in der Katholischen Erwachsenenbildung (für den gesamten niedersächsischen Bereich)
- von Mitarbeitervertretern an katholischen Schulen (Erzbistum Hamburg) und
- von Mitgliedern der Diözesanen Arbeitsgemeinschaft für Mitarbeitervertreter (Erzbistum Hamburg, Bistum Osnabrück).

Für das kommende Jahr sind weitere Veranstaltungen geplant.

Für den Bereich der Kirche stehen zwei weitere Fortbildungsangebote zur Verfügung, die nicht vom Diözesandatenschutzbeauftragten verantwortet werden. Da es sich hier um spezialisierte Angebote handelt, soll an dieser Stelle dennoch auf sie hingewiesen werden:

- Die Fortbildungsakademie des Deutschen Caritasverbandes bietet Seminare zu den Themen „Datenschutz in sozialen Einrichtungen“ und „Rechtliche Fragen bei der Erstellung von Publikationen und Internet-Auftritten“ an.
- Joachim Wenzel, der das Sicherheitskonzept für die Telefonseelsorge entwickelt hat, bietet auf Wunsch Veranstaltungen zum Thema „Den Gefahren des Internets aktiv begegnen – Grundlagen des Datenschutzes und der Internetsicherheit in Beratung und Seelsorge“ an.

Wegen der besonderen Sachkompetenz der Veranstalter ist diesen Fortbildungsangeboten ein hohes Maß an Aufmerksamkeit auf Seiten unserer Einrichtungen zu wünschen. Aus die-

sem Grund finden sich Hinweise zu diesen Veranstaltungen auch auf der Internetseite des Diözesandatenschutzbeauftragten.

Die Qualifizierung von Mitarbeitern ist im modernen Arbeitsleben zu einem wichtigen Anliegen geworden. Der Datenschutz darf hier nicht zurückstehen. Auch für den kirchlichen Bereich besteht mittlerweile ein ausreichendes Angebot an Fortbildungsmöglichkeiten bei gleichzeitig niedrigen Kosten. Für die Zukunft ist zu hoffen, dass diese Seminare noch häufiger in Anspruch genommen werden. Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer lässt sich hier auch gerne fordern.

5. Zusammenarbeit

5.1 Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands

Kirchliche Datenschutzvorschriften sind diözesanes Recht, wenn auch die wichtigsten Regelungen, die KDO und die KMAO auf einer Empfehlung der Deutschen Bischofskonferenz beruhen und somit gleichlautend in allen Bistümern erlassen wurden. Die Umsetzung dieser Vorschriften allerdings kann voneinander abweichen, zumal auch die Rechtsauffassungen der jeweiligen Diözesandatenschutzbeauftragten nicht immer einheitlich sein müssen. Darüber hinaus ist gerade auch bei schwierigen Fragen der Kontakt mit den Kollegen wichtig, um andere Sichtweisen in die eigenen Überlegungen mit einbeziehen zu können. Schließlich fungiert die Konferenz auch als Ansprechpartner für den Verband der Diözesen Deutschlands, wenn es um die Weiterentwicklung kirchlichen Rechts geht. Die Bedeutung der gemeinsamen Arbeit kann daher nicht hoch genug eingeschätzt werden. Leider hat dies bisher nicht dazu geführt, die Konferenz der Datenschutzbeauftragten der Diözesen in die Liste der überdiözesanen Arbeitstagungen beim VDD aufzunehmen.

Die Konferenz tagt regelmäßig zweimal im Jahr, wobei sich aus Sicht des Unterzeichners vor allem die zweitägigen Sitzungen bewährt haben, weil hier einfach mehr Zeit zur Verfügung steht, die Themen ausführlich zu behandeln. Die Fülle der behandelten Tagungsordnungspunkte kann hier nicht dargestellt werden. Stattdessen sollen einige, besonders wichtige Arbeitsergebnisse dargestellt werden.

- Die Konferenz hat alle im Bereich der Gesamtkirche anstehenden Rechtsänderungen durch eigene Entwürfe und Stellungnahmen zu den Entwürfen der Kommission Meldewesen und Datenschutz begleitet.
- Die Konferenz hat die Schaffung von Schulungsmöglichkeiten für betriebliche Datenschutzbeauftragte angeregt und mitgetragen.
- Zu wichtigen Themen wurden gemeinsame Entschließungen mit den Datenschutzbeauftragten im Bereich der Evangelischen Kirche in Deutschland verfasst (siehe Anhang).

Der Leiter der Konferenz der Datenschutzbeauftragten im Bereich der Evangelischen Kirche in Deutschland wurde ebenso regelmäßig zu den Treffen eingeladen, wie die für den jeweiligen Sitzungsort zuständigen Landesbeauftragten für den Datenschutz.

5.2 Zusammenarbeit mit den Datenschutzreferenten

Dem Diözesandatenschutzbeauftragten stehen weiterhin die Datenschutzreferenten in den Bistümern zur Verfügung. Von Seiten des Bistums Hildesheim nimmt auch die betriebliche Datenschutzbeauftragte des Generalvikariats an den gemeinsamen Sitzungen teil. Die treffen finden jeweils nach Bedarf und vorheriger Absprache im Niels-Stensen-Haus in Hannover statt. Thematische Schwerpunkte der letzten Jahre waren:

- Die Diskussion über die im Bereich der Gesamtkirche geplanten Rechtsänderungen, mit dem Ziel die Wünsche der Bistümer hier frühzeitig mit einzubringen. So wurde beispielsweise ein eigener Entwurf zur Änderung der Anordnung über das kirchliche Meldewesen erstellt und der Kommission beim VDD vorgelegt.
- Eigene Rechtsänderungen im Bereich der Nordbistümer, insbesondere die Schuldatenschutzanordnung und das Bischöfliche Gesetz zur Vermeidung von Kindeswohlgefährdungen.
- Die Umsetzung der Vorschriften, zum Beispiel durch Entwicklung elektronischer Formulare für die Meldungen nach § 3a KDO

5.3 Zusammenarbeit mit den Datenschutzbeauftragten und -referenten im Bereich der Evangelischen Kirche Deutschlands

Der Unterzeichner ist regelmäßiger Gast der Tagung der Beauftragten für den Datenschutz in den Gliedkirchen der Evangelischen Kirche in Deutschland, die einmal jährlich in Berlin stattfindet.

Ebenso wird der Diözesandatenschutzbeauftragte regelmäßig zu den Sitzungen der Referentenkonferenz für Datenschutz, Meldewesen und Kirchenmitgliedschaftsrecht im Landeskirchenamt in Hannover eingeladen. Als besonderer Erfolg dieser Zusammenarbeit darf die an den Unterzeichner gerichtete Bitte der Konferenz verstanden werden, einer Arbeitsgruppe beizutreten, die einen Entwurf für eine Fundraisingordnung für die Gliedkirchen der EKD erarbeiten sollte. Grund dafür war, dass das Bistum Hildesheim zuvor bereits eine solche Rechtsvorschrift geschaffen hatte und somit bereits Erfahrungen auf diesem Gebiet bestanden. Der Unterzeichner ist dieser Bitte gerne nachgekommen und hat das Vorhaben durch aktive Teilnahme an den Sitzungen begleitet. Die Arbeiten am Entwurf sind inzwischen abgeschlossen.

5.4 Zusammenarbeit mit den Datenschutzbeauftragten der Länder

Die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz gehört nach § 18 Abs. 5 KDO zum Aufgabenbereich des Diözesandatenschutzbeauftragten. Die Landesdatenschutzgesetze sehen hingegen eine solche Zusammenarbeit nicht ausdrücklich vor. Es ist daher jeweils vom guten Willen der Landesbeauftragten abhängig, ob regelmäßige Kontaktgespräche mit den kirchlichen Vertretern geführt werden. Zum Zeitpunkt dieses Berichts war das nur noch in Hamburg der Fall. Vor wenigen Tagen erst hat der neu gewählte Hamburgische Datenschutzbeauftragte, Herr Prof. Dr. Caspar die Kirchenvertreter zu einem gemeinsamen Gespräch in seine Dienststelle eingeladen und deutlich gemacht, dass er die, nun schon zur Tradition gewordenen Treffen am Buß- und Bettag gerne fortführen möchte.

Das mangelnde Interesse der übrigen Landesbeauftragten führe ich jedoch nicht auf eine kirchenfeindliche Haltung zurück, sondern eher auf den Umstand, dass die Arbeitsbelastung in den Behörden durch Einsparungen in den letzten Jahren zunehmend größer geworden ist und somit keine Zeit bleibt für die Wahrnehmung von Aufgaben, die gesetzlich nicht vorgeschrieben sind. Ein persönlicher Kontakt ergibt sich in diesen Fällen nur noch, wenn die Landesbeauftragten die Einladung zu den Tagungen der kirchlichen Datenschützer annehmen. So sind Herr Dr. Dix als Berliner Datenschutzbeauftragter und Frau Hartge als Brandenburgische Datenschutzbeauftragte regelmäßig Gast der Konferenz im Hause der EKD. Der Niedersächsische Landesbeauftragte, Herr Wahlbrink war Gast unserer Konferenz in Hannover.

Dort, wo konkrete Fallgestaltungen gemeinsam zu lösen sind, etwa dann, wenn kirchliche und staatliche Stellen gemeinsam an einem Datenaustausch beteiligt sind, klappt die Zusammenarbeit reibungslos. Hierzu trägt vor allem auch der Umstand bei, dass keine gravierenden Unterschiede zwischen dem kirchlichen und dem staatlichen Recht bestehen. Beide Seiten sind in diesen Fällen bemüht, schnell zu einer gemeinsamen Lösung zu kommen.

Von Seiten des Unterzeichners besteht großes Interesse daran, die Zusammenarbeit in der Zukunft weiter zu intensivieren. Die Überlegungen hierzu stehen jedoch noch ganz am Anfang. Vorstellbar wäre beispielsweise eine aktive Beteiligung an klar umgrenzten Projekten der Landesbeauftragten. So bereitet die Hansestadt Hamburg zurzeit eine Aktion in Schulen vor, die Schüler über die Risiken des Internets aufklären soll. Eine Ausdehnung auf die katholischen Schulen wäre hier gut vorstellbar. Leider sind wir im Moment noch nicht soweit, dass beide Seiten sich hier gegenseitig in den Blick nehmen und von Anfang an mit einbeziehen. Auch die Durchführung gemeinsam getragener Veranstaltungen, Konferenzen, Symposien wäre eine lohnende Sache.

Vom Berliner Landesbeauftragten wurde der Vorschlag gemacht, die Prüfung von Krankenhäusern gemeinsam vorzunehmen. Angesichts, der gerade in diesem Bereich immer komplexer werdenden „EDV-Landschaften" mit umfangreichen Klinikinformationssystemen wäre hier eine Unterstützung sicher hilfreich. Dies umso mehr, als der Diözesandatenschutzbeauftragte nicht auf die Unterstützung ausgebildeter Informatiker und Computertechniker zurückgreifen kann, wie dies bei den staatlichen Behörden der Fall ist.

Die Korrespondenz in dieser Sache hat bisher jedoch zu keinem Ergebnis geführt. Dabei war für den Unterzeichner nicht immer erkennbar, dass der kirchliche Datenschutz in seiner Eigenständigkeit respektiert und ernst genommen wird. So war plötzlich in einem E-Mail auch von der Prüfung anderer Einrichtungen, wie Kindergärten die Rede, obwohl in dem zuvor geführten telefonischen Gespräch mit Herrn Dr. Dix hierüber überhaupt nicht gesprochen worden war. Es wurde vorgeschlagen, kirchliche Datenschutzbeauftragte sollten an den Prüfungen teilnehmen, wenn sie es wünschen, so als sei ihre Teilnahme nicht erforderlich. Zeitweise konnte sogar der Eindruck entstehen, als solle der kirchliche Datenschutz auf „kaltem Wege" abgeschafft werden. Trotz dieser Schwierigkeiten kann sich der Unterzeichner eine Zusammenarbeit weiterhin vorstellen, wenn dabei Einigkeit über folgende Punkte besteht:

- Prüfungen kirchlicher Einrichtungen können immer nur vom zuständigen Diözesandatenschutzbeauftragten angeordnet und durchgeführt werden. Es handelt sich insoweit um eine Amtshandlung, die nur von der zuständigen Stelle wahrgenommen werden darf.
- Aus diesem Grund kann auch nur der Diözesandatenschutzbeauftragte Art und Umfang der Prüfungshandlungen festlegen. Eine Abstimmung hierüber, mit dem Ziel gleiche Datenschutzstandards für alle Häuser in Berlin zu erreichen, ist dabei durchaus erstrebenswert.
- Die jeweilige Einrichtung hat Anspruch darauf, von der zuständigen Stelle geprüft zu werden. Daher ist die Anwesenheit des Diözesandatenschutzbeauftragten Pflicht. Kann er, zum Beispiel aus gesundheitlichen Gründen den Termin nicht wahrnehmen, muss er verschoben werden.
- Der Diözesandatenschutzbeauftragte ist offiziell Prüfungsleiter.

Ob diese Voraussetzungen von der anderen Seite akzeptiert werden können, ist unklar. Insoweit wird ein persönliches Gespräch mit Herrn Dr. Dix, dem Vertreter der Evangelischen Kirche, Herrn Rückert, der Justiziarin des Erzbistums, Frau Ballhause und mir angestrebt, das Anfang Januar in Berlin stattfinden könnte. Sollte sich hierbei allerdings der Eindruck aus der Korrespondenz bestätigen, wird es besser sein, auf eine Zusammenarbeit zu verzichten.

5.5 Projektpartnerschaft im Virtuellen Datenschutzbüro

Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer betreibt die zurzeit einzige Homepage im Internet, die über den Datenschutz der katholischen Kirche informiert. Da er mit zu den öffentlichen Aufsichtsinstanzen in Deutschland gehört, besteht die Möglichkeit, sich als Projektpartner am Virtuellen Datenschutzbüro (http://www.datenschutz.de/) zu beteiligen. Die Idee, auf diese Weise ein gemeinsames Portal zu schaffen, das jeden, der am Datenschutz interessiert ist, schnell zu den gewünschten Informationen führt, wurde von ihm von Anfang an unterstützt. Die Beteiligung an diesem Projekt hat wesentliche Vorteile:

- Die Inhalte der eigenen Werbseite sind auch für diejenigen, die die Seite bisher

nicht kannten, auffindbar.
- Die Eigenständigkeit des kirchlichen Datenschutzes wird der Allgemeinheit in größerem Umfang bekannt.
- Die Präsenz an dieser Stelle stärkt das Vertrauen der Öffentlichkeit in das kirchliche Bemühen um den Datenschutz.
- Die Gleichwertigkeit mit dem staatlichen Datenschutz wird betont.

Diese Vorteile rechtfertigen auch den finanziellen Beitrag, den die Mitgliedschaft erfordert. Die Fortführung dieser Zusammenarbeit bleibt daher auch für die nächsten Jahre ein wichtiges Anliegen.

6. Entwicklung der Dienststelle

Seit Beginn des Jahres 2001 hat der Diözesandatenschutzbeauftragte sein Büro im Niels-Stensen-Haus am Engelbosteler Damm 72 in Hannover. Bis Ende 2002 wurde er unterstützt durch eine Sekretärin, die vormittags anwesend war und während dieser Zeit alle organisatorischen Aufgaben erledigte. Im Zuge des immer stärker werdenden Zwangs zur Kosteneinsparung wurde sie nach ihrem Eintritt in den Ruhestand nicht durch eine neue Fachkraft ersetzt. Dies führt dazu, dass der Unterzeichner alle bürotechnischen Aufgaben, von der Behandlung der Post über die Anlage und Führung der Akten, bis hin zur Terminverwaltung alles selbst erledigen muss. Dass hierdurch weniger Zeit für die eigentlichen Sachaufgaben bleibt, versteht sich von selbst. Nach nunmehr fast 18 Jahren der Tätigkeit in diesem Amt, hat sich auch naturgemäß eine Fülle von Vorgängen angesammelt, die in dem kleinen Büro kaum noch übersichtlich unterzubringen sind. Hier ist eine organisatorische Neuorientierung dringend erforderlich. Im Moment scheint ein Übergang zur elektronischen Aktenführung der einzige Weg zu sein, die Situation zu verbessern. Der Unterzeichner verspricht sich hiervon eine schnellere Auffindbarkeit der Akten mit Hilfe einer qualifizierten Stichwortsuche, eine verbesserte thematische Strukturierung, eine verbesserte E-Mail-Verwaltung und die zentrale Speicherung immer wieder benötigter Dokumente. Insoweit sind im Gespräch mit dem Bistum Hildesheim schon konkrete Überlegungen erfolgt.

Das der Technikeinsatz nicht immer zuverlässig und reibungslos funktioniert, wurde im Jahr 2008 in besonderer Weise deutlich. Zu diesem Zeitpunkt führte das Versagen fast der gesamten Bürotechnik zu einer enormen Arbeits- und Nervenbelastung auf Seiten des Unterzeichners. Im Einzelnen:
- Das Faxgerät war nicht einsatzfähig, weil es sich trotz mehrfacher stundenlanger Anwesenheit und Bemühungen eines Technikers der Deutschen Telekom immer wieder von selbst auf Empfang schaltete und somit ständig „besetzt" zu sein schien, obwohl aktuell kein Empfang erfolgte.
- Auch die Kopierfunktion dieses Gerätes war nicht mehr zu gebrauchen.
- Der E-Mail-Empfang war mit mehreren hundert Spam-Mails pro Tag überflutet.
- Der Arbeitsplatzrechner und das Notebook waren, wie sich später herausstellte, trotz Einsatz der Norton Internet Security derart mit Viren, Trojanern und anderen

Schadprogrammen verseucht, dass deren Vernichtung und eine Wiederherstellung der Systeme aussichtslos war. Davon waren auch eine Reihe von Systemdateien betroffen.

- Der Arbeitsplatzrechner war wegen häufiger Systemabstürze sowie dem plötzlichen Abbruch von Anwenderprogrammen, wie Winword kaum noch vernünftig zu benutzen.

Mit Hilfe eines Fachunternehmens wurde daraufhin ein Server angeschafft, der seither die Funktion einer Hardware-Firewall übernimmt. Die Festplatten der Rechner wurden komplett neu formatiert und deren Betriebssysteme neu installiert. Das Multifunktionsgerät der Deutschen Telekom wurde durch ein Gerät von OKI ersetzt.

Gleichzeitig traten weitere Schwierigkeiten auf. Bei der Neueinrichtung des E-Mail-Clients traten immer wieder Fehler auf, so dass ein reibungsloser Empfang der Mails unter der standardmäßig verwendeten Adresse „info@datenschutz-kirche.de" nicht möglich war. Nach langem Suchen stellte sich heraus, dass der Host-Provider, ohne den Unterzeichner zu informieren, die Zugangskennungen verändert hatte. Begründet wurde dies mit Umstellungen am eigenen System. Aber schon nach kurzer Zeit kamen wieder keine Mails auf dem Rechner des Unterzeichners mehr an. Mit der jetzt zutreffenden Zugangskennung war allerdings noch ein Lesen der Mails unmittelbar auf der Webseite des Providers möglich. Den automatischen Abruf hatte die Firma aus nicht nachvollziehbaren Gründen und wieder ohne Vorwarnung gesperrt. Schließlich blieb keine andere Wahl, als ein Wechsel des Host-Providers. Seither läuft alles wieder reibungslos.

Technische Schwierigkeiten führten 2008 zeitweise zu einem „Stillstand" der Rechtspflege", die nur mit erheblichem Aufwand an Zeit und Kosten wieder beseitigt werden konnten. Der neu geschaffene Zustand bietet wieder die Basis, um vernünftig arbeiten zu können.

Für die Zukunft bleibt noch die Neuorganisation der Akten- und Schriftgutveraltung als wesentliche Verbesserung der Arbeitsmöglichkeiten.

Schlussbemerkung:

Die vorstehenden Ausführungen geben nur einen kleinen Teil der Arbeit des Diözesandatenschutzbeauftragten wieder. Die Aufnahme sämtlicher Anfragen, Beschwerden sowie die Mitteilung der gesamten Beratungsarbeit in den Einrichtungen vor Ort würden den Rahmen eines solchen Berichts bei weitem sprengen. Es kam dem Unterzeichner darauf an, wesentliche Schwerpunkte herauszuarbeiten und Hinweise für die Zukunft zu geben.

Hannover, den 31.12.2009

Diözesandatenschutzbeauftragter

Statistik

Würde man die Zuverlässigkeit des kirchlichen Datenschutzes allein an der Zahl der Beschwerden von Betroffenen messen, müsste Niemandem bange sein. Mehr als durchschnittlich 5 bis 6 Eingaben pro Jahr gehen beim Unterzeichner nicht ein. Man könnte dies nun darauf zurückführen, dass der Diözesandatenschutzbeauftragte als Aufsichtsinstanz für kirchliche Einrichtungen noch zu wenig bekannt ist. Allerdings kommt es auch meist nur einmal im Jahr vor, dass Beschwerden von den Landesbeauftragten zuständigkeitshalber an den Unterzeichner weitergeleitet werden. Den Gesprächen mit den Kollegen entnehme ich, dass auch dort die Zahl der Bürgereingaben eher gering ist. Die Kontrolle durch die Betroffenen scheint eher eine stumpfe Waffe im Kampf um mehr Datenschutz zu sein. Ein Drittel der Beschwerden beziehen sich dabei allein auf die Veröffentlichung von Jubiläumsdaten im Pfarrbrief und die Werbung der Kirchenzeitung.

Bei der Zahl, der von den Dienstellen und Einrichtungen ausgehenden Anfragen und konkret gewünschten Vor-Ort-Beratungen sind die „kleinen" Anfragen, die sich meist sehr schnell schon telefonisch klären lassen nicht mit erfasst. Ebenso wenig wurden hier die Vorträge berücksichtigt, die für Teilnehmer aus einer größeren Zahl von Einrichtungen gehalten wurden. Sie können der Übersicht unter Zi. 4.3 entnommen werden.

Gerade der Bereich „Krankenhäuser" hat sich dabei zunehmend zum Schwerpunkt entwickelt. Das wird nicht jedem gefallen, der sich wünscht, der Diözesandatenschutzbeauftragte möge sich mehr mit den Strukturen der verfassten Kirche beschäftigen. Aber gerade dort, wo Kirche sehr stark in das öffentliche Leben hineinwirkt und zudem mit staatlichen und privaten Einrichtungen konkurriert, wird die Aufrechterhaltung des Selbstverwaltungsrechts auf dem Gebiet des Datenschutzes für die Zukunft nur gelingen, wenn ein ernsthaftes Bemühen um gleichwertige Qualitätsstandards erkennbar wird. Meine Ausführungen hierzu unter Zi. 5.4 mögen dafür als Beleg gelten.

Die Sicherheit der Daten im Meldewesen wird durch professionelle Rechenzentren gesichert. Hier ist Datenschutz nur durch die Entwicklung sicherer Verfahren unter Beteiligung des Diözesandatenschutzbeauftragten, wie im Beispiel mit „e-mip" (Zi. 3.1.4) und eine entsprechende Schulung der Mitarbeiterinnen und Mitarbeiter zu gewährleisten.

Bisher haben lediglich 17 Einrichtungen ihre Verfahrensverzeichnisse gemäß § 3a KDO dem Diözesandatenschutzbeauftragten gemeldet. Vollständig erfasst ist dabei lediglich der Bereich der Katholischen Erwachsenenbildung im Land Niedersachsen. Der Unterzeichner ist organisatorisch nicht imstande, alle kirchlichen Einrichtungen im gesamten Bereich der Nordbistümer anzuschreiben und zur Abgabe der vorgeschriebenen Meldungen aufzufordern. Die bei den Bistümern insoweit angefragte Unterstützung, etwa durch Hinweise in den Amtsblättern, blieb bisher aus. Hier besteht für die Zukunft dringender Handlungsbedarf!

Die nachfolgende Tabelle gibt einen Überblick. Dabei wurde im ersten Abschnitt nach den anfragenden Stellen, im zweiten Abschnitt nach den betroffenen Rechtsgebieten struktu-riert.

	2004	2005	2006	2007	2008	2009	Gesamt
Anfragen / Beratungen							
- Kath. Büro	1	0	0	0	0	0	1
- Bistümer	10	13	4	11	17	8	63
- Pfarreien	1	3	3	7	3	5	22
- Caritas und soziale Einrichtungen,	5	8	8	8	12	10	51
- Mitarbeitervertretungen	1	3	4	1	2	3	14
- Krankenhäuser	11	18	4	12	15	32	92
- Schulen	0	0	1	4	1	2	8
Gesamtzahl	**29**	**45**	**24**	**43**	**50**	**60**	**251**
Beschwerden							
- Spendenaufrufe	1	0	0	0	0	0	1
- Jubiläumsdaten	0	1	2	1	0	0	4
- Werbung Kirchenzeitung	1	1	1	2	0	2	7
- sonst. Werbung	1	0	0	0	0	1	2
- Ahnenforschung	0	0	0	0	1	0	1
- Arbeitsverhältnis	1	1	1	3	0	1	7
- Krankenhausbehandlung	0	0	1	1	1	1	4
- Soziale Einrichtungen	0	0	0	0	3	1	4
- Meldewesen	0	0	0	0	1	0	1
- Internet / E-Mail	0	0	0	0	2	0	2
Gesamtzahl	**4**	**3**	**5**	**7**	**8**	**6**	**33**

Das geltende Datenschutzrecht in den norddeutschen Diözesen

A. Erzbistum Berlin

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Datenübermittlung im Zusammenhang mit den Fusionen der Kirchengemeinden
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien

B. Erzbistum Hamburg

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnabrück
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Sozialdatenschutz in der freien Jugendhilfe in der katholischen Kirche
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte

C. Bistum Hildesheim

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Veröffentlichung von persönlichen Daten (z.B. Altersjubiläum) in Pfarrbriefen und ähnlichen Publikationen

- Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim - FundrO
- Ordnung zur Regelung der Betreuungsverhältnisse in katholischen Tageseinrichtungen für Kinder im Bistum Hildesheim
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Hildesheim
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Hildesheim
- Besonderer Schutz von Computerprogrammen nach dem Urheberrechtsgesetz
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte

D. Bistum Magdeburg

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien

E. Bistum Osnabrück

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Pfarrbrief und Datenschutz
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnabrück
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Sozialdatenschutz in der freien Jugendhilfe in der katholischen Kirche

- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte

F. Offizialat Vechta

- Anordnung über den kirchlichen Datenschutz – KDO –
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO)
- Anordnung über das kirchliche Meldewesen – KMAO
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Offizialatsbezirk Oldenburg
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern im Offizialatsbezirk Oldenburg
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien
- Richtlinien zum Einsatz von Arbeitsplatzcomputern im oldenburgischen Teil des Bistums Münster

Bischöfliches Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen im Bistum .....[1]

(Stand: 11. Juni 2008)

Präambel

Aus Sorge um das körperliche und geistige Wohl junger Menschen, zur **Gewährleistung** der Qualität kirchlicher Arbeit mit Kindern und Jugendlichen und zur Wahrung des christlichen Erziehungsauftrags muss sichergestellt werden, dass nur **von ihrer Persönlichkeit her geeignete Personen** mit der Betreuung von Kindern und Jugendlichen beauftragt werden. Um dieses Ziel zu erreichen wird das nachfolgende Gesetz erlassen:

§ 1 Persönliche Eignung

Kirchliche Rechtsträger haben hinsichtlich der persönlichen Eignung **insbesondere** sicherzustellen, dass keine Personen, die in kirchlichen Einrichtungen mit Kindern und Jugendlichen arbeiten oder diese betreuen, *eingesetzt* werden, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 181a, 182 bis 184e oder 225 des Strafgesetzbuches verurteilt worden sind.

§ 2 Führungszeugnis

(1) Zur Erfüllung ihrer Verpflichtung aus § 1 haben kirchliche Rechtsträger sich bei der Einstellung oder Beauftragung und in regelmäßigem Abstand von fünf Jahren von den beschäftigten/beauftragten Personen ein **Privat**führungszeugnis nach § 30 Abs. 1 des Bundeszentralregistergesetzes vorlegen zu lassen. Von bereits Beschäftigten hat sich der Dienstgeber das Führungszeugnis erstmalig unverzüglich nach In-Kraft-Treten dieses Gesetzes vorlegen zu lassen.

(2) Die Verpflichtung nach **Abs. 1** gilt insbesondere für **die Beschäftigung und Beauftragung folgender Personengruppen:**

1. Geistliche
2. Pastoral- und Gemeindereferenten
3. Mitarbeiter in Kindertagesstätten in kirchlicher Trägerschaft
4. **Ehe-, Familien-, Lebens- und Erziehungsberater**
5. Lehrkräfte an Schulen in kirchlicher Trägerschaft
6. Ehrenamtliche als hauptverantwortliche Leiter insbesondere von Jugendfreizeiten
7. N.N. (von Caritas zu benennen)
8. *sonstige im Sinne von § 1 eingesetzte Personen*

§ 3 Verfahren

(1) Das Führungszeugnis nach § 2 ist **unmittelbar nach Zugang von dem jeweiligen Personalverantwortlichen zu prüfen und danach** in einem verschlossenen Umschlag

[1] Soweit in diesem Gesetz auf natürliche Personen Bezug genommen wird, gilt dieses für weibliche und männliche Personen – ausgenommen Geistliche – in gleicher Weise. Dienst- und Funktionsbezeichnungen werden von Frauen in der weiblichen Form geführt.

zur Personalakte, *im Falle von nach § **2 Abs. 2 Ziffer 6** betroffenen Ehrenamtlichen zu den Generalakten des kirchlichen Rechtsträgers* zu nehmen.

(2) Dem Betroffenen sind die durch die Beantragung und Vorlage des Führungszeugnisses entstanden Kosten zu erstatten. Dies gilt nicht, wenn das Zeugnis im Rahmen einer Einstellungsbewerbung erstmalig vorgelegt wird. Die Höhe der Kosten ist in geeigneter Form zu belegen.

§ 4 In-Kraft-Treten

Dieses Gesetz tritt am ……. in Kraft.

……., den …….

Gemeinsame Erklärung

Zu der Frage, ob Fotos von Kindergartenkindern im Internet veröffentlich werden dürfen, auf denen Kindergartenkinder zu erkennen sind:

1. Geplante Veröffentlichung als Datenübermittlung:
   Das Veröffentlichen von Bildern in Internet ist eine Datenübermittlung an einen unbekannten Personenkreis. Der Datenschutz ist hiervon betroffen, wenn

   I. Die abgebildeten Personen klar erkennbar sind und/oder
   II. Die Namen der abgebildeten Personen mitgeteilt wird.

2. Kunsturhebergesetz keine Rechtsgrundlage
   § 23 Abs. 1 Kunsturhebergesetz ist keine ausreichende Rechtsgrundlage für eine solche Veröffentlichung im Internet. Selbst dann, wenn einer der Ausnahmetatbestände (z. B. Teilnahme an öffentlichen Veranstaltungen) zutrifft, verletzt gerade die Publikation im Word Wide Web die berechtigten Interessen des Betroffenen im Sinne von § 23 II Kunsturhebergesetz. Hierbei ist zu berücksichtigen, dass

   I. Fotos beliebig auf die eigene Festplatte heruntergeladen werden können,
   II. Digitale Bilder mit Bildbearbeitungsprogrammen nachbearbeitet, verändert und in einen völlig anderen Kontext gestellt werden können,
   III. Die Veröffentlichung von Kinderbildern dem Jugendschutz zuwider läuft.

3. Einwilligung erforderlich.
   Die kirchliche Datenschutzanordnung und das Datenschutzgesetz der EKD kennen keine Norm, (Rechtsgrundlage), die die Bildveröffentlichung im Internet zulassen würde. Es ist daher vor der Einstellung von Fotos in die Website der Pfarrgemeinde oder des Kindergartens in jeden Fall die Zustimmung der Sorgeberechtigten erforderlich. Liegt sie nicht vor, ist die Veröffentlichung rechtswidrig. Ein Verstoß hiergegen kann nach dem Kunsturhebergesetz mit Freiheitsstrafe bis zu einem Jahr bestraft werden.

4. Schriftlichkeit der Einwilligung
   Die Einwilligung aller abgebildeten Personen muss schriftlich vorliegen und auf den konkreten Einzelfall bezogen sein. Die Sorgeberechtigten müssen die Möglichkeit haben, die Bilder vor Abgabe der Einwilligungserklärung zu sehen. Formularmäßig erklärte Einwilligungen, etwa im Aufnahmevertrag, reichen nicht aus.

18.3.2008 5. 2. 2008
Konferenz der Datenschutzbeauftragten im ..... Konferenz der Datenschutzbeauftragten
Bereich der Katholischen Kirche Deutschlands ..... der evangelischen Landeskirchen

Entschließung der Datenschutzbeauftragten der katholischen Kirche Deutschlands und der Datenschutzbeauftragten in den Gliedkirchen der EKD

Berlin, den 12. Mai 2004

Einsichtnahme der Kranken- und Pflegekassen in Patientenakten und Pflegedokumentationen

Aufgrund des Zwanges zur Einsparung von Kosten im Gesundheitswesen sehen zahlreiche Kranken- und Pflegekassen (Kostenträger) die Notwendigkeit, in größerem Umfang als bisher die von Krankenhäusern und Pflegediensten (Leistungserbringer) erstellten Kostenrechnungen zu überprüfen.

Die Übernahme der in Rechnung gestellten Kosten wird in letzter Zeit von den Kostenträgern immer häufiger von der Einsichtnahme bzw. der Übersendung der gesamten Krankenunterlagen und/oder Patientendokumentation abhängig gemacht.

Ein Recht auf Einsichtnahme oder gar Übersendung der gesamten Krankenunterlagen und/oder Patientendokumentation steht den Kostenträgern jedoch nicht zu. Sie haben vielmehr das Recht auf Auskunft. Der Umfang der Daten, die an die Kostenträger übermittelt werden dürfen, ist durch § 301 Abs.1 SGB V abschließend regelt worden. Weitergehende Rechte dürfen den Kostenträgern nicht eingeräumt werden.

Es ist daher nicht hinzunehmen, dass die in Rechnung gestellten Kosten von den Kostenträgern nicht fristgerecht bezahlt werden, weil ihnen das Anliegen auf Einsichtnahme nicht zugestanden worden ist.

Der Bundesbeauftragte für den Datenschutz hat in seinem 18. Tätigkeitsbericht (Nr. 21.3) uns in seinem 19. Tätigkeitsbericht (24.1.4. und 24.2.2.) ausführlich zu der von den Kostenträgern geforderten Einsichtnahme in Patientenunterlagen Stellung genommen.

Er hat dazu ausgeführt, dass die §§ 73 Abs. 2 Nr. 9, § 301 Abs. 1 S. 1 Nr.3 SGB V und § 100 SGB X keine rechtliche Verpflichtung der Leistungserbringer enthalten, den Kostenträgern Entlassungsberichte, Arztbriefe, Befundberichte, ärztliche Gutachten, Röntgenaufnahmen usw. zur Verfügung zu stellen. Die Überprüfung medizinischer Sachverhalte sei durch § 275 SGB V allein dem Medizinischen Dienst der Krankenversicherung (MDK) vorbehalten. Auch die Einholung einer Einwilligungserklärung des Versicherten könne eine Befugnis zur Einsichtnahme in Patientenunterlagen nicht begründen, da sie wegen der damit verbundenen Umgehung der gesetzlichen Regelung unwirksam sei.

Das Bundessozialgericht hat diese Rechtsauffassung durch Urteil v. 23.07.2002, Az.: B 3 KR 64/01 R, GSGE 90, S.1 ff) bestätigt. Dabei wird ausdrücklich festgestellt:

„Zur Überprüfung einer Krankenhausabrechnung daraufhin, ob die Leistungen den einschlägigen Fallpauschalen und Sonderentgelte nicht richtig zugeordnet sind, hat die Krankenkasse kein eigenständiges Recht auf Einsichtnahme in die Behandlungsunterlagen."(LS 1)

In einem weiteren Urteil des Bundessozialgerichts vom 28.05.2003, Az: B 3 KR 10/02R, heißt es:

„Die Krankenkasse ist nicht berechtigt, die Herausgabe de Krankenunterlagen an sich selbst zu verlangen und nach Erfüllung dieses Begehrens bis zum Abschluss des Prüfungsverfahrens die Bezahlung der geltend gemachten Kosten zu verweigern."

Die Datenschutzbeauftragten der katholischen Kirche Deutschlands und die Datenschutzbeauftragten in den Gliedkirchen der EKD teilen die Rechtsauffassung des Bundesbeauftragten für den Datenschutz und des Bundessozialgerichts.

Die Datenschutzbeauftragten weisen alle Leistungserbringer in kirchlicher Trägerschaft darauf hin, dass diese Rechtslage von ihnen zu beachten ist.

Damit ist folgendes zu beachten:
Leistungserbringer (Krankenhäuser und Pflegedienste) sind nicht berechtigt, über § 301 SGB V hinaus den Kostenträgern (Kranken- und Pflegekassen) Behandlungsunterlagen der Patienten – auch nicht zum Zwecke der Überprüfung der Leistungsabrechnung – zu überlassen. Dies gilt selbst bei Vorlage einer Einwilligungserklärung des Betroffenen.

> *(Hinweis: Möglich ist allenfalls eine Einsichtnahme in die Unterlagen durch den Medizinischen Dienst der Krankenkassen (MDK); hiervon kann die Krankenkasse unterrichtet werden.)*
>
> *Festzuhalten ist: „Ärztliche Unterlagen dürfen nur vom MDK geöffnet werden."*
>
> *Jede unbefugte Offenbarung von Patientendaten ist durch § 203 Strafgesetzbuch (StGB) mit Strafe bedroht ist.*
> *(Hierzu: Gebauer, Grenzen der Übermittlung von Patientendaten zwischen Krankenhaus und Krankenkasse; NJW 2003, Seite 777 ff.)*
>
> *Die Weigerung eines Kostenträgers zur Zahlung der Krankenhaus- bzw. Pflegedienstabrechnung ist nach höchstrichterlicher Rechtsprechung unzulässig, wenn diese auf die Weigerung zur Überlassung von Patientenunterlagen gestützt wird.*