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 2010 bis 28. Februar 2014

Vorgelegt im Juli 2014

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/

Tätigkeitsbericht 2010 - 2014

des Datenschutzbeauftragten der norddeutschen Diözesen

Inhalt:

Vorwort

Die Vollversammlung des Verbandes der Diözesen Deutschlands hat auf ihrer Herbsttagung am 28.11.2013 den Bistümern die Inkraftsetzung einer neuen „Anordnung über den kirchlichen Datenschutz (KDO)“ empfohlen. Die Änderung wurde als notwendig erachtet, um die Bestimmungen des kirchlichen Datenschutzrechts an die Anforderungen aus dem Urteil des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzbeauftragten[1] anzugleichen. Dabei wurde sowohl die Bestellung des Diözesandatenschutzbeauftragten (§ 16 KDO), seine Rechtsstellung (§ 17 KDO), seine Aufgaben (§ 18 KDO) und durch ihn vorzunehmende Beanstandungen (§ 19 KDO) in erheblichem Umfang neu geregelt. Die wesentlichen Unterschiede zum bisherigen Recht sind in der folgenden Liste im Überblick dargestellt:

1. *Der Diözesandatenschutzbeauftragte muss die Befähigung zum Richteramt nach § 5 DRiG besitzen (§ 16 II KDO).*
2. *Er ist oberste Dienstbehörde im Sinne des § 96 StPO und oberste Aufsichtsbehörde im Sinne des § 99 VwGO (§ 17 V KDO).*
3. *Er hat für den Fall seiner Verhinderung einen Vertreter zu bestellen (§ 17 VI KDO).*
4. *Er verfügt über einen eigenen jährlichen Haushalt, der gesondert auszuweisen und zu veröffentlichen ist (§ 17 III KDO).*
5. *Er wählt das notwendige Personal aus, das von einer kirchlichen Stelle angestellt wird. Die Mitarbeiter unterstehen seiner Dienst- und Fachaufsicht und können nur mit seinem Einverständnis gekündigt werden (§ 17 IV KDO).*
6. *Der Diözesandatenschutzbeauftragte kann Datenschutzverstöße gegenüber der betroffenen kirchlichen Dienststelle beanstanden (§ 19 I KDO) und Maßnahmen zur Beseitigung dieser Mängel anordnen (§19 VI KDO).*
7. *Er erstellt jährlich einen Tätigkeitsbericht (§ 18 III KDO).*

Der Datenschutz in den Bistümern der katholischen Kirche in Deutschland wird hierdurch organisatorisch auf eine völlig neue Ebene gestellt. In den Diözesen von Berlin, Hildesheim und Osnabrück ist die KDO-2014 jeweils zum 1. März in Kraft gesetzt worden, in Hamburg sowie im Offizialat Vechta zum 1. April und in Magdeburg zum 1. Mai 2014. Trotz dieser leicht unterschiedlichen Verkündungstermine wird davon auszugehen sein, dass die Tätigkeit des Unterzeichners ab dem 01.03.2014 auf der neu geschaffenen Grundlage erfolgt. Dies hat dazu geführt, dass dieser Tätigkeitsbericht sich auf den Zeitraum bis zum 28.02.2014 bezieht und somit zeitlich mit der Geltungsdauer der KDO-2003 abschließt. Für die Zukunft ist dann ein jährlicher Tätigkeitsbericht zu erstellen, der sich dann jeweils auf den Zeitraum vom 01.03. bis 28.02 des Folgejahres beziehen wird.

Der vorliegende Bericht ist seit einiger Zeit überfällig. Grund hierfür war eine schwerwiegende Erkrankung des Unterzeichners im Jahre 2011, durch deren Behandlung und

[1] Gerichtshof der Europäischen Union, Urteil vom 09.03.2010, Az.: C-518/07

Rehabilitation er für fast vier Monate nicht arbeitsfähig war. Nach Mitteilung der Ärzte gehört der Unterzeichner zu den 30% der Erkrankten, die nach einer solchen Erkrankung anschließend wieder als voll berufsfähig eingestuft werden können. Ich bin den norddeutschen Bistümern deshalb dankbar dafür, dass sie mir die Gelegenheit gegeben haben, mein Amt weiter fortzuführen. Die Zeit nach dem Wiedereinstieg war mit einer neuen Einarbeitung in die bestehenden Aufgaben und der Bewältigung einer Fülle von, zwischenzeitlich aufgelaufenen, neuen Themen ausgefüllt, die eine zeitlich angemessene Erstellung des Berichts verhindert haben. Ich bitte daher darum, diesen Bericht auch zum jetzigen Zeitpunkt als Erfüllung meiner festgelegten Aufgabe entgegenzunehmen.

Hannover, den 30.06.2014

Lutz Grammann
Diözesandatenschutzbeauftragter

1. Rechtsänderungen

1.1 Regelungen innerhalb der Europäischen Union

Die Rechtskommission der Europäischen Union hat am 25. Januar 2012 einen Vorschlag für eine "Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" vorgelegt[2]. Dieser soll die seit 1995 geltende Datenschutzrichtlinie 95/46/EG ablösen. Nach schwierigen Verhandlungen über den Entwurf wurde im Innenausschuss des Europäischen Parlaments (LIBE) ein Kompromissvorschlag verabschiedet, den das Europäische Parlament in erster Lesung verabschiedet hat[3]. Im nächsten Schritt wird nun der EU-Rat zu dem Verordnungsvorschlag Stellung nehmen. Es wird größtenteils nicht erwartet, dass dies noch in der laufenden Legislaturperiode bis Ende Mai 2014 erfolgen wird. Sollte es zu einer Reform des Datenschutzrechts innerhalb der Europäischen Union kommen, werden sich hieraus eine Reihe von wichtigen organisatorischen und inhaltlichen Änderungen gegenüber dem bisherigen Recht ergeben.

Geplant ist eine **Verordnung** an Stelle der bisherigen **Richtlinie**. Eine Verordnung wäre als unmittelbar geltendes Recht in den Mitgliedstaaten anzuwenden, ohne dass es hierbei, wie bei einer Richtlinie, einer Umsetzung in nationales Recht bedarf. Demgemäß hätten die beteiligten Staaten auch keine Möglichkeit mehr, Änderungen an den getroffenen Bestimmungen vorzunehmen. Eine Umsetzung, die noch über die Festlegungen der Verordnung hinaus geht und ein "Mehr an Datenschutz" verwirklicht, wäre in diesem Fall nicht mehr möglich. Die Europäische Union würde auf diese Weise praktisch zum alleinigen Gesetzgeber des Datenschutzes in Europa. Der "Flickenteppich" Datenschutz, mit unterschiedlichen Regelungen in den Mitgliedsländern würde somit beseitigt. Die EU beruft sich insoweit darauf, dass hiermit einheitliche Bedingungen für den gemeinsamen Wirtschaftsraum geschaffen werden. Zugleich wird hiermit die Geltung des Grundrechts aus Art. 8 EUV der "Charta der Grundrechte der Europäischen Union" (GrCh) allgemein festgelegt. Dieser gewährt allen EU-Bürgern ein Recht auf Schutz ihrer personenbezogenen Daten.

> ***Art. 8 Schutz personenbezogener Daten***
> *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
> *(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*
> *(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.*

[2] Dokument KOM(2012) 11/4
[3] Dokument COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)

Einschränkungen dieses Grundrechts sind nur unter den Voraussetzungen des Art. 52 GrCh möglich. Hier wird bestimmt, dass jede Einschränkung der Rechte und Freiheiten **gesetzlich** vorgesehen sein und den Wesensgehalt dieser Rechte achten muss. Der Grundrechtsschutz kann aber innerhalb Europas keinen unterschiedlichen Normen unterliegen. Der Fall "Facebook" macht dies deutlich, da hier deutsche Datenschutzaufsichtsbehörden mit den Entscheidungen ihrer irischen Kollegen in vielen Fällen nicht einverstanden sind. Hier kann nur ein einheitliches Recht mit einer einheitlichen Prüfungspraxis weiterhelfen.

Als problematisch wird allerdings die Tatsache angesehen, dass die künftige Verordnung nicht mehr zwischen dem öffentlichen Bereich und privater Datenverarbeitung unterscheidet. Es wird befürchtet, dass somit eine "Super-Aufsichtsbehörde" geschaffen wird, die selbst einem Ministerium bestimmte Datenverarbeitungen untersagen kann, obwohl dieses auf Grund nationalen Verfassungsrechts nur dem Parlament gegenüber verantwortlich ist. Man mag sich nur einmal vorstellen, ein Datenschutzbeauftragter würde dem Finanzministerium Nordrhein-Westfalen die Verwendung einer in der Schweiz unrechtmäßig erstellten CD über deutsche Geldanleger für den Erlass von Festsetzungsbescheiden und der Einleitung von Steuerstrafverfahren im Hinblick auf Art. 53 Abs. 1 Nr. g) EU-DSGV endgültig verbieten und gegen die Behörde ein Bußgeld in Höhe von 1 Mio. EUR nach Art. 79 Abs. 6 Zi. l) EU-DSGV festsetzen. Er müsste dies tun, gegen den Willen des Ministers und des Landtages, die dieses Verfahren genehmigt haben.

Hiermit nicht einverstanden ist allerdings der deutsche Bundesrat, der gegen den Erlass der Verordnung an Stelle einer Richtlinie eine Subsidiaritätsrüge[4] eingelegt hat. Hierbei hat er sich auf Art. 5 Abs. 3 EUV berufen. Große Aussichten werden dieser Rüge im Hinblick auf Art. 16 AEUV[5] allerdings kaum beizumessen sein. Dieser nimmt in Absatz 1 textlich die Grundrechtsformulierung aus Art. 8 Abs. 1 GrCH auf und bestimmt, in Einklang mit Art. 52 Abs. 1 GrCh, eine Einschränkung dieses Rechts durch ein parlamentarisches Gesetz.

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Das Europäische Parlament und der Rat erlassen **gemäß dem ordentlichen Gesetzgebungsverfahren**[6] Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen und über den freien Datenverkehr. **Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht**.
> Die auf der Grundlage dieses Artikels erlassenen Vorschriften lassen die spezifischen Bestimmungen des Art. 39 des Vertrages über die Europäische Union unberührt.

[4] Pressemeldung des Bundesrates vom 30.03.2012, Nr. 51/12, veröffentlicht unter: http://www.bundesrat.de/nn_8396/DE/presse/pm/2012/051-2012.html
[5] Konsolidierte Fassung des Vertrags über die Europäische Union, veröffentlicht im Abl. C 83/13
[6] Der Fettdruck wurde durch den Verfasser eingefügt.

1.2 Auswirkungen auf das kirchliche Recht

Wo steht bei dieser Sachlage künftig der kirchliche Datenschutz, in Form der unter Berufung auf das verfassungsrechtliche Selbstverwaltungsrecht der öffentlichen Religionsgesellschaften vorgenommenen eigenständigen Datenschutzregelungen und Datenschutzaufsichten? Die Europäische Union hat durch den Lissaboner Vertrag die den Kirchen nach nationalem Recht zustehenden Rechte anerkannt. So hat sie in Art. 17 Abs. 1 AEUV festgelegt:

> *"Die Union achtet den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht."*

Zur Achtung des Selbstverwaltungsrechts der Kirchen in Deutschland ist die Europäische Union somit vertraglich verpflichtet.

Dieser Verpflichtung ist sie durch Schaffung von Art. 85 EU-DSGV nachgekommen. Im Erwägungsgrund 128 hat die Kommission unter wörtlicher Bezugnahme auf Art. 17 AEUV ausgeführt, dass in Kirchen, die zum Zeitpunkt des Inkrafttretens der Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anwenden, diese weiter gelten, wenn sie mit der Verordnung **in Einklang gebracht** werden. Darüber hinaus sollen die Kirchen verpflichtet werden, eine **völlig unabhängige Datenschutzaufsicht i.S.v. Kapitel VI** einzurichten. In einer zwischenzeitlich vorliegenden „Legislativen Entschließung des Europäischen Parlaments vom 12.03.2014[7]“ wurde hierzu eine Abänderung vorgeschlagen[8]. Hierbei wurde der Ausdruck „umfassende Regeln“ durch „angemessene Regeln“ ersetzt. In Absatz 2 ist die Verpflichtung zur Schaffung einer eigenen, unabhängigen Datenschutzaufsicht nach Kapitel VI fallen gelassen worden. Verlangt wird jetzt nur noch, dass eine Bescheinigung die Vereinbarkeit mit der Datenschutzgrundverordnung nach Art. 38 anerkennt[9].

Vielfach wird befürchtet, dass hierdurch die eigenständige kirchliche Datenschutzaufsicht in Frage gestellt wird. Das würde inhaltlich jedoch wenig Sinn machen.

1. Wenn weiter kirchliches Recht gelten soll, dann müssten die staatlichen Aufsichtsbehörden bei einem Teil ihrer Tätigkeit nach EU-Recht und im anderen Teil nach Kirchenrecht verfahren, obwohl beide Regelungen vergleichbar (angemessen) sind.
2. Es liegt nicht im Zuständigkeitsbereich der Union, die Regelung der Aufsicht in den Mitgliedstaaten vorzugeben. Ob diese dezentral verteilt ist, wie in Deutschland oder

[7] Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Ordentliches Gesetzgebungsverfahren: 1. Lesung

[8] Abänderung 197: Vorschlag für eine Verordnung Artikel 85

[9] Vorgeschlagene Änderung der Erwägung 128 der Datenschutz-Grundverordnung

zentral nur von einer Stelle wahrgenommen wird, wie in Frankreich, kann die EU nicht bestimmen. Für die Organisation des Datenschutzes sind auch kircheneigene Rechtsvorschriften zu beachten, insbesondere der CIC. Der Kompromissvorschlag überlässt es daher den Kirchen, ihre Datenschutzaufsicht in Übereinstimmung mit diesem Recht zu regeln und selbst darüber zu entscheiden, ob gegen den Bischof ein Bußgeld verhängt werden kann! Gefordert wird nur eine vergleichbare Anwendung der Verhaltensregeln nach § 38 EU-DSGV.

Für die Auffassung der Evangelischen Kirche in einem Vermerk der Dienststelle Brüssel des Bevollmächtigten vom 28.10.2013 „Danach könnte zwar das kircheneigene Datenschutzrecht beibehalten werden, die diesbezügliche Aufsicht müsste jedoch von staatlichen Stellen geführt werden." besteht nach dem Wortlaut des Kompromissvorschlags keine Veranlassung.

Für die Kirche besteht daher besonderer Handlungsbedarf, wenn sie ihre Eigenständigkeit auf dem Gebiet des Datenschutzes erhalten will. Dabei muss sie vor allem dafür sorgen, dass datenschutzrechtliche Regeln im Sinne der Richtlinie im innerkirchlichen Bereich auch durchsetzbar sind und entsprechende Aufsichtsbehörden schaffen.

- Die Kirche in ihrer verfassten Form erhält kommunale Meldedaten ihrer Mitglieder und deren Angehörigen, die nur bei Bestehen eines angemessenen Datenschutzrechts übermittelt werden dürfen.
- Kirche ist der größte Arbeitgeber in Deutschland. Die Dienstnehmer haben Anspruch auf datenschutzgerechten Umgang mit ihren Personaldaten.
- Darüber hinaus unterhalten kirchliche Rechtsträger eine Vielzahl von wirtschaftlichen Einrichtungen, die nach außen wirken und mit vergleichbaren Institutionen der Länder, der Kommunen oder privaten Trägern konkurrieren. Beispiele sind Krankenhäuser, Schulen, Kindergärten, Heime, soziale Beratungsstellen und viele andere mehr.
- Der Datenschutz muss hierbei ebenso geregelt sein, wie in der Europäischen Datenschutz-Grundverordnung.

Das setzt eine weitgehende Änderung der KDO in sachlicher und formeller Hinsicht voraus.

In einem ersten Schritt sind durch den Erlass der neuen Anordnung über den Kirchlichen Datenschutz (KDO) in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 18.11.2013 (KDO-2013) schon Änderungen zur Unabhängigkeit des Diözesandatenschutzbeauftragten durchgeführt worden. Hierdurch wird bereits jetzt die Unabhängigkeit der Aufsicht, wie sie vom Gerichtshof

der Europäischen Union im Urteil vom 09. März 2010 festgelegt wurde[10], verwirklicht[11].

1.3 Die Rechtsentwicklung im Bereich der katholischen Kirche Deutschlands

1.3.1 Die Anordnung über den kirchlichen Datenschutz – KDO –

Änderung des § 18a KDO

Die Vollversammlung des Verbandes der Diözesen Deutschlands hat in ihre Sitzung am 21.06.2010 die Änderung der Bestimmung über die betrieblichen Datenschutzbeauftragten in § 18a KDO beschlossen. Hiermit wurde parallel zur Regelung im Bundesdatenschutzgesetz in der Fassung von 2009 ein Kündigungsschutz für Betriebsbeauftragte eingeführt, die nur noch aus wichtigem Grund entlassen werden können. Durch diese Regelung werden die Betriebsbeauftragten in ihrer Tätigkeit wesentlich gestärkt. Die Änderung wurde inzwischen von allen Bistümern übernommen.

Regelung des Arbeitnehmerdatenschutzes - § 10a KDO

Im Berichtszeitraum wurde durch den Erlass einer neuen Vorschrift, die als § 10a in die KDO eingefügt wurde, erstmalig eine Regelung zum Arbeitnehmerdatenschutz geschaffen. Insoweit wurde die entsprechende Bestimmung aus § 32 BDSG übernommen. Ergänzend hierzu wurde eine Definition des Beschäftigtenbegriffs geschaffen, die unter den normativen Begriffsbestimmungen des § 2 KDO in einem neuen Abs. 12 verbindlich festgelegt wurde.

Im Vorfeld dieser Neuregelung wurde unter den kirchlichen Datenschutzbeauftragten eine breit angelegte Diskussion über die Notwendigkeit einer solchen Änderung / Ergänzung geführt. Dagegen sprach vor allem, dass der Bundesgesetzgeber eine "große" Regelung des Beschäftigtendatenschutzes plant, die eine Fülle von Regelungen für eine Reihe von datenschutzrechtlich problematischen Verhaltensweisen, wie Videoüberwachung am Arbeitsplatz, Kontrolle durch den Einsatz von Ortungssystemen, Biometrische Verfahren oder auch beim Einsatz von Internet und E-Mail am Arbeitsplatz einer gesetzlichen Lösung zuführen will. Diese Regelungen würden in einem weiten Umfeld über die Regelung einer allgemein gehaltenen Verarbeitungserlaubnis des § 32 BDSG hinausgehen. Hiermit würde auch in der Personaldatenverarbeitung dem Bestimmtheitsgebot der verfassungsrechtlichen Rechtsprechung entsprochen. Hierzu verweise ich auf meine Ausführungen im Bericht 2004-2009. Schließlich bringt § 10a KDO auch gegenüber der geltenden Vorschrift des § 9 KDO (Zulässigkeit der Datenerhebung, wenn sie zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist), keine inhaltliche Erweiterung.

[10] Siehe FN 1
[11] Siehe hierzu meine Ausführungen unter 1.3

Für diese Lösung wurde jedoch angeführt, dass die Reform des Arbeitnehmerdatenschutzrechts im Bund wohl kaum noch in kürzerer Zeit zu erwarten ist. In der Tat ist auch zum Zeitpunkt der Abfassung dieses Berichts noch immer kein endgültiger Vorschlag für die Durchführung eines Gesetzesvorhabens geschaffen. Daher ist auch aus heutiger Sicht noch mit einer längeren Frist bis zum Inkrafttreten einer Regelung zu rechnen, wenn sie denn überhaupt noch erfolgen soll. In dieser Übergangszeit sollte nach den Befürwortern dieser Regelung, mit dem § 10a KDO die Bereitschaft der Kirche, die Personaldatenverarbeitung stärker in den Blick zu nehmen, unter Beweis gestellt werden.

Der Datenschutzbeauftragte der norddeutschen Bistümer hatte sich in der Konferenz der Datenschutzbeauftragten und gegenüber der Arbeitsgruppe Datenschutz-, Meldewesen-, IT-Recht gegen eine solche Änderung ausgesprochen, sich letztlich aber nicht damit durchsetzen können.

Die Schaffung einer bereichsspezifischen Regelung, wie oben beschrieben, ist nach meinem derzeitigen Kenntnisstand zurzeit nicht vorgesehen. Auch hier soll wieder die bundesgesetzliche Regelung abgewartet werden, obwohl gerade hier auf Grund der Besonderheit des kirchlichen Arbeitsrechts als „Drittem Weg“ eine eigenständige und nicht notwendigerweise mit dem staatlichen Recht übereinstimmende Lösung möglich wäre. Die besondere Verantwortung des kirchlichen Dienstes, die verpflichtet „die Persönlichkeit und Würde der einzelnen Mitarbeiterin und des einzelnen Mitarbeiters zu achten und zu schützen…[12]“, bei dem „die arbeitsrechtlichen Beziehungen zwischen den kirchlichen Anstellungsträgern und ihren Beschäftigten, dem religiösen Charakter des kirchlichen Auftrags entsprechen müssen[13]“ und die besondere „Dienstgemeinschaft als das maßgebende Strukturelement des kirchlichen Dienstes,[14]“ könnten hier in entsprechenden Regelungen zum Ausdruck kommen.

1.3.2 Die Anordnung über das kirchliche Meldewesen (KMAO)

In dem Tätigkeitsbericht 2004-2009 wurde ausgeführt:

> *"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 zu-*

[12] Siehe: Erklärung der deutschen Bischöfe zum kirchlichen Dienst, I. Präambel, Ziffer 3
[13] Siehe: Erklärung der deutschen Bischöfe zum kirchlichen Dienst, II. Eigenart des kirchlichen Dienstes
[14] Siehe: Erklärung der deutschen Bischöfe zum kirchlichen Dienst, V. Nr. 2

rückzuführen 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."

Zwischenzeitlich ist diese Einfügung erfolgt und somit eine zuverlässige Rechtsgrundlage für den Datenaustausch zwischen den Diözesen geschaffen worden.

1.4 Die Rechtsentwicklung im Bereich der norddeutschen Bistümer

1.4.1 Bischöfliches Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen im Erzbistum Hamburg und den Bistümern Hildesheim und Osnabrück

Im Bericht 2004-2009 ist über die beabsichtigte Schaffung einer eigenen Regelung zum Schutz von Kindern und Jugendlichen vor sexuellem Missbrauch und körperlicher Misshandlung berichtet worden[15]. Hierdurch wird den Dienstgebern die Verpflichtung auferlegt, keine Personen zu beschäftigen, die nicht durch Vorlage eines erweiterten Führungszeugnisses nach dem Bundeszentralregistergesetz belegen können, dass sie keine Straftaten gegen Kinder und Jugendliche begangen haben oder in dieser Hinsicht gegen sie ermittelt wird. Dabei sollten alle Mitarbeiter, die im kirchlichen Bereich mit Kindern und Jugendlichen arbeiten erfasst werden. Für Ehrenamtliche wurde in § 5 des Gesetztes eine spezielle Regelung geschaffen, die eine nachgewiesene Schulung (Juleica) und eine schriftliche Erklärung ihrerseits, nicht wegen der in § 30 BZRG genannten Tatbestände bestraft worden zu sein und auch kein hierauf gerichtetes Ermittlungsverfahren gegen sie eingeleitet wurde.

Inzwischen ist dieses Gesetz von den Bistümern erlassen worden. Das Erzbistum Hamburg hat es zum 01.10.2010, das Bistum Hildesheim am 01.08.2010 und das Bistum Osnabrück zum 01.09. 2010 in Kraft gesetzt. Die geltende Fassung ist im Anhang wiedergegeben.

1.4.2 Ordnung zur Prävention von sexuellem Missbrauch an Minderjährigen (Präventionsordnung) im Erzbistum Berlin, im Bistum Magdeburg und im Offizialat Vechta

Die übrigen Diözesen haben auf der Grundlage der von der Deutschen Bischofskonferenz im September 2010 erlassenen Rahmenordnung eine "Ordnung zur Prävention von sexuellem Missbrauch an Minderjährigen (Präventionsordnung)" erlassen. Der Wortlaut dieser Vorschriften ist nicht in allen Punkten gleich, so dass diese im Anhang in drei Fassungen, die jeweils in einem Bistum Gültigkeit haben, abgedruckt sind.

Somit ist die Kirche insgesamt ihrer Verpflichtung zum Schutz der Kinder- und Jugendarbeit vor Straftaten von Kindesmissbrauch nachgekommen. Besonders wichtig dabei

[15] Tätigkeitsbericht 2004 – 2009, Kap. 1.2.4, Seite 15

ist nicht nur die Verpflichtung der Dienststellen, sich insoweit erweiterte Führungszeugnisse vorlegen zu lassen, sondern auch der erkennbare Wille, durch Ausbildungs- und Schulungsmaßnahmen einen angemessenen Umgang mit Kindern und Jugendlichen zu fördern und Probleme zu erkennen.

1.4.3 Probleme bei der Umsetzung der Vorschriften

Die Präventionsordnungen vom Erzbistum Berlin und vom Offizialat Vechta beziehen auch die Betreuer erwachsener Behinderter mit ein und verlangen auch insoweit ein erweitertes Führungszeugnis nach § 30 BZRG. Auch Behinderte sind sicherlich schutzwürdig, auch im Erwachsenenalter. In vielen Fällen werden diese Personen auch nur den Reifegrad eines Kindes erreichen können. Das Bundeszentralregistergesetz stellt jedoch hierfür keinen Schutz zur Verfügung, so dass de lege lata in solchen Fällen kein Zeugnis ausgestellt werden darf. Ein Anforderungsschreiben der Einrichtung, das fälschlicherweise eine regelmäßige Arbeit mit Minderjährigen, also Menschen, die noch nicht das 18. Lebensjahr vollendet haben, erkennen lässt, stellt einen Missbrauch zur Erlangung einer gesetzlich nicht vorgesehenen Amtshandlung dar. Zu diesem Thema werden immer wieder Beschwerden von Mitarbeitern eingereicht.

Eine Beschwerde betraf sogar eine Krankenhausverwaltung, die von **allen** Mitarbeiterinnen und Mitarbeitern im medizinischen und organisatorischen Bereich die Vorlage von Zeugnissen nach § 30 BZRG verlangen wollte. Zur Begründung wurde angegeben, dass doch jeder Beschäftigte gelegentlich Kindern und Jugendlichen begegnet. Das geht sicherlich über den Bereich der erlassenen Verordnungen hinaus. Hierunter fallen nur solche Beschäftigte, die von der **Art ihrer Tätigkeit** her gesehen, mit Kindern und Jugendlichen Kontakt haben können. Dies mag auf Pflegepersonal in Bereichen, in denen auch Kinder behandelt werden zutreffen, nicht aber auf eine Verwaltungsangestellte, die auf dem Weg zur Kantine einem jugendlichen Patienten begegnet. Hier muss noch einmal über die Anwendung dieser Vorschriften nachgedacht werden. Es geht darum, Kinder und Jugendliche vor bestimmten Gefahren zu schützen. Und diese Gefahren dürften am größten sein, wenn

1. die erwachsene Person die Möglichkeit hat, eine Zeit lang mit dem Kind alleine zu sein,
2. das Kind sich in ihrer Obhut, Fürsorge oder Versorgung befindet und
3. sie durch ihre Tätigkeit ein Vertrauen des Kindes genießt, das eventuelle Handlungen aus Sicht des Kindes notwendig und somit unumgänglich machen.

2. Informations- und Kommunikationstechnik

2.1 Cloud Computing

Dienststellen und Einrichtungen wollen immer häufiger ihre Daten und Anwendungsprogramme auf einem fremden Server verwalten. Diese als Cloud-Computing bezeichnete Verfahrensweise bietet eine Fülle von Vorteilen. Einige wichtige Aspekte hierfür werden in der nachfolgenden Aufzählung benannt.

- Die Verwaltung der Hard- und Software erfolgt dabei durch den Dienstleister und entlastet somit die Mitarbeiter von aufwendigen Software-Upgrades, Installation von neuen Programmversionen und der Beseitigung von Hardwarestörungen.
- Es erfolgt eine dauerhafte, professionell ausgestaltete Datensicherung.
- Der Aufbau eigener großer Arbeitsspeicher wird vermieden. Das gilt insbesondere bei abgeschlossenen Fällen, die aber auf Grund von Aufbewahrungspflichten weiterhin gespeichert bleiben müssen (Archivverwaltung).
- Die Cloud-Daten sind in der Regel über Internetzugänge erreichbar und daher von allen angeschlossenen Geräten, unabhängig von ihrem Einsatzort, abrufbar. Hierdurch wird auch eine Datenverarbeitung außerhalb der Dienststelle möglich.
- Die Einheitlichkeit des Bearbeitungsstandes der Dateien ist vor allem beim Zugriff durch mehrere Sachbearbeiter leichter zu gewährleisten. Manche Clouds geben auch die Möglichkeit, Vorversionen des Dokuments einzusehen und ggf. wiederherzustellen.

Die genannten Vorteile sind so verlockend, dass sie immer mehr von den Einrichtungen in Betracht gezogen werden. Somit wird die Frage der rechtlichen Zulässigkeit immer dringender. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 82. Sitzung am 28./29. September 2011 in München eine Entschließung über eine „Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing“ verfasst und dabei eine Reihe von Mindestanforderungen benannt, die von den Cloud-Anbietern erfüllt werden sollen.

- Offene, transparente und detaillierte Information über die technisch-organisatorischen Maßnahmen einschließlich der Sicherheitskonzeption.
- Eindeutige vertragliche Regelungen, die auch den Ort der Datenverarbeitung und die Portabilität der Daten einschließt.
- Umsetzung der abgestimmten Sicherheitsmaßnahmen durch den Anbieter und die Anwender.
- Aktuelle und aussagekräftige Zertifizierung der in Anspruch genommenen Infrastruktur.

Die gesamte Entschließung ist im Anhang dieses Berichts im Originaltext wiedergegeben. Gleichzeitig haben die Arbeitskreise Technik und Medien der Konferenz eine Orientierungshilfe hierzu veröffentlicht[16].

Rechtlich ist Folgendes zu berücksichtigen:

- Die Inanspruchnahme von Dienstleistungen für Cloud-Services ist eine Auftragsdatenverarbeitung im Sinne von § 8 KDO. Der Auftraggeber bleibt daher in vollem Umfange für die Verarbeitung seiner Daten und den Schutz der Rechte der Betroffenen verantwortlich.
- Zwischen Auftraggeber und Auftragnehmer muss daher eine vertragliche Regelung bestehen, die schriftlich abzufassen ist und die in § 8 Abs. 2 Nr. 1 bis 10 KDO genannten Festlegungen enthält. Zur Hilfestellung der Anwender wurde insoweit ein Muster hierfür auf der Webseite des Diözesandatenschutzbeauftragten zur Verfügung gestellt[17].
- Für die Erhebung, Verarbeitung und Nutzung von Daten im Sozialbereich ist § 80 SGB X zu beachten. Dieser ist im Anhang dieses Berichts abgedruckt.
- Es muss gewährleistet sein, dass die verantwortliche Stelle ihre Löschungspflichten, Datenberichtigungspflichten, ihre Auskunftspflicht gegenüber dem Betroffenen erfüllen und gegebenenfalls eine Sperre der Daten vornehmen kann.
- Es muss für das Anlegen, Bearbeiten, Verändern, Sperren und Löschen der Daten eine Trennung nach der jeweiligen Zugriffsberechtigung erfolgen können (Rechteverwaltung).
- Ein unautorisierter Zugriff muss ausgeschlossen sein. Das gilt in besonderem Maße für Informationen, die der strafrechtlichen Verschwiegenheitspflicht, dem Sozialgeheimnis oder dem Seelsorgegeheimnis unterliegen.

Legt man diese Anforderungen zugrunde wird sehr schnell deutlich, dass eine öffentliche Cloud (Public Cloud) dem nicht gerecht werden kann. Gerade unter dem NSA-Skandal wird deutlich, dass eine verschwiegene Speicherung auf solchen Systemen illusorisch ist. Server, die in den USA stehen und Server, die in anderen Ländern von amerikanischen Firmen betrieben werden, unterliegen der Kontrolle der Sicherheitsbehörden und die Informationen werden gegebenenfalls auch an europäische Stellen weitergeleitet. Darüber hinaus hat es in den letzten Jahren eine Reihe von Fällen gegeben, in denen die Zugänge zu derartigen Dienstleistungen von Hackern in großem Umfang kompromittiert worden sind. Schließlich ist auch ein Vertrag nach § 8 KDO im Massengeschäft mit diesen Anbietern nicht möglich.

[16] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe - Cloud Computing, Version 1.0 vom 26.09.2011 (http://www.datenschutz.hessen.de/download.php?download_ID=237)
[17] Siehe: Mustervertrag zur Auftragsdatenverarbeitung nach § 8 KDO

Eine rechtlich unangreifbare Hilfestellung für Kircheneinrichtung lässt sich daher nur bei entsprechender Gestaltung von Private Clouds schaffen. Hierbei werden die IT-Dienstleistungen innerhalb einer Institution (einem Rechenzentrum) oder im internen kirchlichen Bereich einer verantwortlichen Stelle angeboten.

2.1.1 Aufbau einer Cloud-Datenverarbeitung für Pfarrgemeinden und KiTas

Das Bischöflich Münstersche Offizialat in Vechta und das Bistum Osnabrück planen den Aufbau einer Private Cloud, die gemeinsam mit dem Rechenzentrum ITEBO geschaffen wird und dann ihren Pfarrgemeinden und Kindertagestätten zur Verfügung gestellt werden soll.

Vorgesehen ist dabei:

- Eine sichere Verbindung auf dem Transportweg
- Eine Verschlüsselung der Daten auf dem Server
- Eine Trennung der Daten nach den einzelnen Rechtsträgern (Mandantenverwaltung)
- Eine Rechteverwaltung innerhalb des Rechtsträgers, die sowohl die zugriffsberechtigten Personen, wie auch die technischen Eingriffsmöglichkeiten (Anlage von Dateien, Bearbeiten, Verändern, Lesen, Löschen, Sperren) auf die Datenverarbeitung eingehend verwaltet.

Geplant ist eine Testphase mit zwei Kirchengemeinden durchzuführen, bevor das System allgemein für alle interessierten Träger freigegeben wird.

Das Offizialat Vechta ist in der Realisierung der Private Cloud schon weiter fortgeschritten und hat das System schon zum Jahresanfang insgesamt freigegeben.

Mit Beginn der Durchführung der Testphase beim Bistum Osnabrück ist eine eingehende rechtliche und technische Datenschutzprüfung geplant. Dabei wird der Diözesandatenschutzbeauftragte von einem Techniker der Datenschutz Nord GmbH unterstützt werden.

2.1.2 Einsatz der „Hamburg Cloud“ im Erzbistum Hamburg

Die Firma IT works! Consulting GmbH & Co. KG bietet in Hamburg Cloud-Dienste in drei Rechenzentren an, deren Sever alle ausschließlich in Hamburg installiert sind. Bei dem IT-Workshop am 23. Januar 2014 stellte ihr Geschäftsführer, Herr Sommerfeldt, die angebotenen Leistungen vor. Sie seien nach ISO 27001 (Internationaler Standard für Management der Informationssicherheit) zertifiziert, zudem seien Anwenderüberprüfungen durchgeführt worden, wobei auch die Datenschutz Nord GmbH zu zufriedenstellenden Ergebnissen gelangt sei.

Angeboten werden Kommunikations- und E-Mail-Dienste, Mobile Device Management, Virtuelle Desktops und Server sowie Backup und Systemüberwachung.

2.1.3 Cloud-Datenverarbeitung in der Friedhofsverwaltung

Das Offizialat Vechta und das Bistum Osnabrück haben mir einen gleichlautenden Vertrag mit dem Anbieter einer Cloud-Verwaltung für kirchliche Friedhöfe, die mit der Software „My Hades“ arbeitet, vorgelegt. Hierin fanden sich eine Reihe gravierender Fehler, die dazu führten, dass die Verarbeitung in der vorgelegten rechtlichen Form mit den Anforderungen aus § 8 KDO nicht zu vereinbaren war. Beanstandet wurde vor allem

- Dass die Datenverarbeitung auf dem Server eines nicht genannten Rechenzentrums erfolgen sollte, so dass auch nicht feststand, wo sich die Rechner dieses Zentrums befinden.
- Der Zugang zum Rechenzentrum wurde dem Auftraggeber nach § 4, Zi. 4.5 des Vertrages verweigert, so dass die Möglichkeit einer Prüfung nicht bestand.
- Dem Auftraggeber wurden in § 5 völlig unangemessene Pflichten auferlegt. So sollte nach Zi. 5.8 der Auftraggeber dafür verantwortlich sein, dass seine Website, die auf einem fremden und ihm nicht einmal bekannten Server geführt wird, von Hackern als Pool für das Verschicken und Weiterleiten von Spam-Mails missbraucht werden könnte. In diesem Fall sollte der Auftragnehmer das Recht haben, den Zugang zu den Daten zu sperren und sie sogar zu löschen!
- Keine Sicherheit für den Auftraggeber war bei einem Scheitern des Vertrages gegeben. Eine Verpflichtung des Auftragnehmers, zur Übertragung der Daten auf eine andere Anwendung zu sorgen und gegebenenfalls entsprechende Schnittstellen zur Verfügung zu stellen, gab es nicht.
- Die Software war nicht auf den nach unserer Friedhofsdatenschutzverordnung zulässigen Umfang der Speicherung, Verarbeitung und Nutzung von Daten ausgelegt.

Den beteiligten Diözesen wurden diese Beanstandungen durch Mail-Brief vom 08.08.2013 mitgeteilt. Eine Anfrage bei den übrigen Diözesen ergab, dass dieses Verfahren dort nicht eingesetzt wird und auch für die Zukunft hieran kein Interesse besteht. Vechta und Osnabrück haben sich bereit erklärt, die rechtlichen Probleme mit dem Anbieter neu zu klären. Erste Gespräche haben dazu geführt, dass der Auftragnehmer erklärt hat, sämtliche Punkte seien für ihn verhandelbar, um einen rechtlich zulässigen Vertrag zu erreichen. Dem Diözesandatenschutzbeauftragten ist bis heute jedoch kein neuer Vertragsentwurf vorgelegt worden.

2.1.4 Private Cloud für Caritas Wohnen in Hannover

Die Einrichtung betreibt fünf Wohnhäuser für behinderte Menschen in Hannover. Die hier anfallenden Personaldaten werden beim Caritasverband in Hildesheim verwaltet, die Daten der Bewohner jedoch unmittelbar vor Ort. Da die Einrichtungsleitung Zweifel

hatte, ob diese Verarbeitung datenschutzgerecht erfolge, bat sie den Diözesandatenschutzbeauftragten im März 2012 um eine Besichtigung der EDV in der Hauptstelle und um ein Gespräch, in dem die wahrscheinlich notwendigen Veränderungen geklärt werden könnten. Bei dem ersten Termin stellte sich heraus, dass keine ordnungsgemäßen technisch-organisatorischen Maßnahmen zum Schutz der Bewohnerdaten getroffen worden waren. Hierüber wurde ein Gesprächsvermerk gefertigt und der Einrichtungsleitung zur Verfügung gestellt.

Bei diesem Gespräch wurde von Seiten der Einrichtungsleitung die Frage gestellt, ob für die Zukunft eine Cloud-Verarbeitung durchgeführt werden könne. Nach zunächst geäußerten Bedenken, ob die Verarbeitung von Sozialdaten in einem Cloud-System datenschutzgerecht erfolgen könne, wurde dem Diözesandatenschutzbeauftragten im November 2012 ein Vertragsentwurf für die Errichtung einer privaten Cloud, ausschließlich für diese Einrichtung, zur Prüfung vorgelegt.

Hierbei wird von dem Anbieter ein virtueller Server zur ausschließlichen Nutzung durch Caritas Wohnen in einem Rechenzentrum in Hannover installiert. Der Server unterliegt dem alleinigen Zugriff des Anbieters. Er ist durch geeignete bauliche Maßnahmen (Serverschrank) vor dem Zugriff Dritter geschützt. Die Online-Verbindung über einen geschützten IPSEC-VPN-Tunnel, Installation und Betreuung der Verwaltungssoftware und benötigter Microsoft-Produkte sowie ein Backup über NAS/RAID-Systeme sind Bestandteil der erbrachten Dienstleistungen. Nach einem eingehenden Gespräch mit der Einrichtungsleitung und dem Auftragnehmer wurde der Dienstleistungsvertrag noch in einigen Punkten angepasst, so dass nunmehr eine Lösung besteht, die in allen Punkten datenschutzgerecht ist.

Dieser Fall legt beispielhaft dar, dass Systeme, die von einem gewerblichen Anbieter speziell für den Kunden, unter Berücksichtigung der für ihn geltenden Datenschutzbestimmungen, lokal eingerichtet werden, eine dauerhafte Stärkung der Bearbeitungsqualität und der rechtlichen Absicherung der Daten erbringen können. Notwendig hierfür ist die anfängliche Einbeziehung des Datenschutzbeauftragten bei Gestaltung der vertraglichen Regelungen und der technischen Rahmenbedingungen.

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

Dieses Thema wurde bereits im letzten Tätigkeitsbericht erörtert[18]. Erfreulicherweise hat die Firma Google auf die Kritiken und Bedenken der Datenschützer reagiert. Nach Gesprächen mit dem Hamburgischen Datenschutzbeauftragten wurde eine Lösung geschaffen, in der der Nutzer die Möglichkeit hat, der Verwendung seiner Daten zu widersprechen. Hierfür wird von Google ein Deaktivierungs-Add-On zur Verfügung gestellt, das in alle gängigen Browser eingebunden werden kann. Darüber hinaus wird auf Anforderung des Webseitenbetreibers die IP-Adresse des Users anonymisiert mit der Folge, dass er nicht mehr identifizierbar ist. Dem Internetnutzer wird somit sein

[18] Tätigkeitsbericht 2004 – 2009, Zi. 2.1, Seite 16

Recht, selbst darüber zu entscheiden, welche Stellen seine Daten erfassen dürfen, zurückgegeben.

Zur Durchführung dieses Verfahrens stellt die Firma Google einen Mustervertrag für die Webseitenbetreiber zur Verfügung, der deutschem Datenschutzrecht entspricht[19]. Darüber hinaus sind bestimmte Einstellungen auf der Webseite des Anbieters erforderlich[20]. Unter den dort genannten Voraussetzungen ist der datenschutzgerechte Einsatz von Google Analytics möglich.

Webseitenbetreiber haben die **Verantwortung**:

Für ein rechtlich zulässiges Angebot auf ihrer Internetseite.
Für den Schutz des Besuchers vor Ausspähung.

Die Firma Google kommt ihnen entgegen
durch einen datenschutzgerechten Mustervertrag.
Er sollte in jedem Fall von kirchlichen Dienststellen abgeschlossen werden!

[19] Im Internet zu finden unter der Adresse „http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/de//analytics/terms/de.pdf“
[20] Siehe die „Hinweise zum Einsatz von Google Analytics in Internet-Angeboten rheinland-pfälzischer Stellen“ des Landesbeauftragten für den Datenschutz Rheinland-Pfalz, veröffentlicht September 2011 (http://www.datenschutz.rlp.de/downloads/oh/oh_google_analytics.pdf)

3. Datenschutz in kirchlichen Einrichtungen

3.1 Meldewesen

3.1.1 Datenübermittlung von der Kirchenzeitung an das Pfarramt

Ein Pfarrer bat die Kirchenzeitung um Zurverfügungstellung einer Liste von Gemeindemitgliedern, die Bezieher der Kirchenzeitung sind. Der Verlag fragte bei mir an, ob sie diese aushändigen könnten. Eine Datenübermittlung im kirchlichen Bereich ist aber nach § 11 Abs. 1 KDO nur zulässig, wenn sie der Aufgabenerfüllung der anfordernden oder abgebenden Stelle dient und die Zweckbindung dabei gewahrt bleibt. Beides konnte im vorliegenden Fall nicht festgestellt werden. Daher wurde mitgeteilt, dass ohne die Benennung zwingender Gründe, die eine Preisgabe dieser Daten rechtfertigen könnten, eine Herausgabe nicht mit dem Datenschutz vereinbar sei.

3.1.2 Auskunft aus archivierten Heimakten

Eine Dame verlangte die Zusendung von Kopien einer Akte, die von einem katholischen Kinderheim über sie geführt worden ist, in dem sie sich in den Jahren 1961/62 aufgehalten hat. Das Bistumsarchiv fragte an, ob es dem Auskunftsersuchen entsprechen kann, obwohl innerhalb dieser Akte auch weitere Personen benannt werden. Es wurde mitgeteilt, dass aus Sicht des Datenschutzes kein Recht besteht, der Dame die Auskunft zu verweigern. Sie hat Anspruch darauf, ihre eigene Lebensgeschichte kennenzulernen. Soweit Mitarbeiter und Verantwortliche des Kinderheims in der Akte erwähnt werden, handelt es sich dabei um dienstliche Aussagen und Handlungen gegenüber dem Schützling. Insoweit muss eine Offenbarung hingenommen werden.

Inzwischen ist durch ein Merkblatt über "Auskunftsrechte ehemaliger Heimkinder", das auf der Stellungnahme basiert, die die Datenschutzbeauftragten des Bundes und der Länder gegenüber dem vom Bundestag eingerichteten "Runden Tisch" abgegeben haben, die Frage generell beantwortet worden.

3.1.3 Gratulationsschreiben zum 50. Geburtstag mit Probeabonnement vom "Tag des Herrn"

Der Benno Verlag fragte an, ob es möglich sei, den Kirchenmitgliedern, die ihren 50. Geburtstag feiern, ein Gratulationsschreiben des (Erz-)Bischofs hierzu zu übersenden, das gleichzeitig mit einem Probeabonnement der Zeitung versehen sei. Gemeinsam mit den Datenschutzbeauftragten der Bistümer Erfurt und Dresden-Meißen wurde geklärt, dass es den Ortsbischöfen nicht verwehrt werden könne, ihre eigenen Kirchenmitglieder anzuschreiben und ihnen Glückwünsche zu ihrem Festtag zu übermitteln. Hierdurch wird die Kirche als Gemeinschaft erlebbar. Es bestanden daher keine Bedenken für diesen Zweck eine Auswertung der kirchlichen Meldedatei zu verwenden.

Die Beifügung der von den Ortsdiözesanen selbst herausgegeben Zeitung "Tag des Herrn" als Aufmerksamkeit und getragen von dem Willen, auch in dieser Weise die Auseinandersetzung mit Kirche zu fördern, war von einem anzuerkennenden Zweck getragen. Der Benno Verlag wurde dabei verpflichtet, das Probeabonnement nicht mit einer Bezugsverpflichtung zu verbinden und die übermittelten Adressdaten nach Abschluss der Aktion vollständig zu löschen. Für den Fall, dass sich jemand entschließt, die Zeitung dauerhaft zu lesen, ist er in gewohnter Weise in die Abonnentenliste aufzunehmen.

Beschwerden hierzu hat es nicht gegeben.

3.1.4 Webbasierte Schematismus Datenbank "Isidor" im Erzbistum Hamburg

Das Erzbistum Hamburg hat die dienstlichen Anschriften und weitere Kommunikationsdaten von Mitarbeitern elektronisch in einer Datenbank unter dem Namen "Isidor" gespeichert. Einzusehen sind diese Informationen nur im internen Bereich, wobei der Account hierzu vom Erzbischöflichen Generalvikariat vergeben wird. Ein Mitarbeiterverzeichnis ist für eine angemessene Zusammenarbeit untereinander erforderlich. Die elektronische Form führt zu einer schnelleren Auffindbarkeit und ist in vielen Fällen aktueller, als die höchstens einmal im Jahr erscheinende Buchform. Bei einem persönlichen Gespräch mit den Verantwortlichen vor Ort konnten keine datenschutzrechtlichen Bedenken festgestellt werden.

3.2 Seelsorge / Fundraising

3.2.1 Auslage eines Totengedenkbuchs in einer Kirche

Datenschutz schützt an sich den Umgang mit Informationen lebender Personen. Das Bundesverfassungsgericht hat jedoch erkannt, dass auch das Persönlichkeitsrecht Verstorbener nicht vollständig erlischt und dieses von den nächsten Angehörigen gewahrt wird.

Eine Nennung verstorbener Gemeindemitglieder mit Vor- und Zunamen, Anschrift, Geburtsjahr und genauem Todesdatum aus jüngster Zeit, kann daher in vielen Fällen Probleme bereiten, wenn die Angehörigen hiermit nicht einverstanden sind. Daher ist die Eintragung einer Person hierin nur mit Einwilligung der Betroffenen statthaft.

Meine bereits im Tätigkeitsbericht 2004-2009, Nr. 3.2.3 geäußerte Auffassung hat sich nicht geändert.

3.2.2 Anreicherung von Meldedaten durch das Fundraisingbüro Hildesheim

Das Fundraisingbüro bat die Meldestelle um Angabe aller Anschriften von Haushaltsvorständen im Bistum Hildesheim, ohne Namensnennung jedoch mit Personenkenn-

ziffer, aus der man Alter und Geschlecht der Person erkennen kann. Diese Daten sollten dann von einem Fremdunternehmen mit Milieudaten angereichert werden, die die Wahrscheinlichkeit begründen, ob jemand gut situiert ist, eine bestimmte politische Richtung favorisiert und mehr. Diese Informationen sollten in einer "Schattendatenbank" zu der jeweiligen Anschrift hinterlegt werden und bei künftigen Fundraisingaktionen die Auswahl der anzusprechenden Personen erleichtern.

Die Datenübermittlung an das Fundraisingbüro entsprach der Rechtsgrundlage des § 2 Abs. 1 FundrO, problematisch war allerdings die Drittdatenverarbeitung, wobei es lediglich eine "Datenschutzerklärung" des Auftragnehmers gab, die nicht den Voraussetzungen der Auftragsdatenverarbeitung nach § 8 KDO entsprach. Gemeinsam wurde hier eine rechtlich einwandfreie vertragliche Lösung herbeigeführt, auf der das Projekt dann durchgeführt werden konnte.

3.2.3 Auftragsdatenverarbeitung durch das Fundraisingbüro Hildesheim für das Erzbistum Hamburg

Das Fundraisingbüro des Bistums Hildesheim legte dem Datenschutzbeauftragten den Entwurf einer Vereinbarung mit dem Erzbistum Hamburg zum Zweck der Durchführung von Spendenbriefmaßnahmen vor. Dieser entsprach zunächst nicht den Anforderungen nach § 8 KDO. Jedoch konnte mit dem auf der Webseite empfohlenen "Mustervertrag zur Auftragsdatenverarbeitung nach § 8 KDO" und Hinweisen durch den Unterzeichner auf notwendige Anpassungen hierzu und nach einem Gespräch mit dem Datenschutzreferenten im Erzbistum Hamburg in sehr kurzer Zeit eine datenschutzgerechte Vereinbarung erstellt werden.

3.2.4 Schein-Videoüberwachung des Vorplatzes einer Kirchengemeinde

Eine Kirchengemeinde in Hamburg hatte Probleme mit einer gegenüberliegenden Kneipe, nach deren Besuch eine Reihe von Gästen nachts den Vorplatz zum Urinieren nutzte und Türen beschmierten. Als Gegenmaßnahme wurde eine Attrappe als scheinbare Videoüberwachung installiert. Die Ähnlichkeit mit funktionsfähigen Geräten war sehr groß und beim Blick von unten kaum zu erkennen. Da hierbei jedoch tatsächlich keine personenbezogenen Daten erfasst, gespeichert und beobachtet werden, fällt diese Maßnahme nicht in den Bereich, der vom Datenschutz erfasst wird. Und das, obwohl mit einer solchen Pseudo-Überwachung die Einschränkung des Grundrechts auf informationelle Selbstbestimmung genauso stark wirkt, wie bei einer tatsächlichen Aufzeichnung. Eine Prüfungsmöglichkeit des Datenschutzbeauftragten besteht daher nicht, da § 5a KDO von der "Beobachtung öffentlich zugänglicher Räume" spricht. Eine Beobachtung findet aber hier nicht statt.

Es wurde trotzdem darauf hingewiesen, dass ein Gespräch mit dem Gastwirt und eine Einschaltung der Gaststättenaufsicht vielleicht auf einfachere Weise zu einer Lösung des Problems geführt hätten. Darüber hinaus ist zweifelhaft, ob eine scheinbare Überwachung überhaupt von den Störern ernst genommen wird, wenn durch das Fehlen

einer Beleuchtungsanlage (evtl. mit Bewegungsmelder) selbst eine tatsächliche Überwachung kaum brauchbare Ergebnisse liefern würde.

Zu der rechtlichen Problematik der Beobachtung öffentlicher Räume mit optisch-elektronischen Einrichtungen, die heute unter Berücksichtigung der Gründe aus dem Urteil des Bundesverfassungsgerichts vom 23.02.2007, Az.: 1 BvR 2368/06[21] zu beurteilen ist, hat der Unterzeichner inzwischen in einer Arbeitshilfe "Videoüberwachung - Eine Arbeitshilfe für kirchliche Einrichtungen" Stellung genommen.

3.2.5 Einrichtung einer Telefonanlagen-/Serverinstallation für das Katholische Internationale Zentrum in Hannover

Das Katholische Internationale Zentrum in Hannover umfasst eine deutschsprachige Kirchengemeinde, drei muttersprachliche Gemeinden und einen Kindergarten, der sich in Trägerschaft der Pfarrgemeinde befindet. Für diese Einrichtung ist eine gemeinsame IuK-Technik geplant. Von dem Koordinator dieses Projekts wurde ich gebeten, ihm eine datenschutzrechtliche Anforderungsliste für die Ausschreibung des Projekts zur Verfügung zu stellen. In meinem Antwortschreiben teilte ich mit, dass ich solch einen Katalog nur erstellen könne, wenn ich weitere Informationen zur Planung erhalten würde. Die mir zunächst in seinem Anschreiben gemachten Angaben waren insoweit nicht ausreichend für mich. Nachdem hierauf keine Antwort kam, habe ich ihm eine "Checkliste: Sicherheitsstatus einer Telekommunikationsanlage" des Bayerischen Landesbeauftragten für Datenschutz als Orientierungshilfe übermittelt und ein gemeinsames Gespräch angeboten. Leider wurde weder auf die Anfrage nach Informationen noch auf das Gesprächsangebot reagiert. Mit weiterem Schreiben meinerseits stellte ich dann die Anfrage, ob überhaupt eine weitere Zusammenarbeit mit dem Datenschutzbeauftragten gewünscht werde. Auch hierauf erhielt ich keine Antwort.

Der vorliegende Fall bestätigt, wie wichtig es wäre, der Datenschutzaufsicht auch einen IT-Techniker zur Unterstützung seiner Aufgaben zur Verfügung zu stellen. Der Datenschutz kann hier nur zum Tragen kommen, wenn er von eingehendem technischem Wissen begleitet wird und ein tiefes Verständnis der eingesetzten Technik und ihrer Risiken getragen wird. Wenn die Einstellung eines solchen Mitarbeiters möglich wird und erfolgt, wird der Unterzeichner an dieser Stelle eine eingehende Systemprüfung vornehmen.

3.2.6 Veröffentlichung von Webseiten der Pfarrgemeinden durch das Bistumsarchiv

Das Archiv des Bistums Hildesheim erfasst auch im Rahmen der Sicherstellung und Erschließung kirchlichen Wirkens die elektronischen Publikationen der Kirchengemeinden und speichert diese. Angefragt wurde, ob dieses Archivgut auch im Lesesaal zur Einsicht durch jede interessierte Person zugänglich gemacht werden kann.

[21] http://www.bundesverfassungsgericht.de/entscheidungen/rk20070223_1bvr236806.html

Kein Problem besteht damit, solange die Webseite unverändert in der Gestalt präsentiert wird, die sie zurzeit hat. Ein Leseplatz, der die Internetauftritte, in der von Gemeinden selbst veranlassten Veröffentlichung zur Verfügung stellt, bietet nicht mehr als der eigene Internetzugang zu Hause, an dem jedermann die Seite ungehindert lesen kann. Die Haftung für den Inhalt liegt in diesem Fall allein bei der Redaktion, die mit ihrer Erstellung beauftragt ist.

Problematisch ist es aber, inhaltlich nicht mehr aktuelle Seiten zugänglich zu machen, so dass hier Webpräsentationen zugänglich werden, die nicht mehr im Internet erreicht werden können. Hierdurch wird das Archiv selbst zum Medienanbieter im Sinne des Telemediengesetzes. Beispiel: Ein Gemeindemitglied hat die Veröffentlichung seines Fotos im Internet gestattet, weil er davon ausgegangen ist, dass es dort nur eine Zeit lang zu sehen sein wird, bis es von anderen aktuelleren Beiträgen abgelöst wird. Oder, er hat seine Einwilligung widerrufen und sein Foto ist daher von der Redaktion entfernt worden. Möglicherweise hat die Redaktion fehlerhafte Informationen eingestellt, die sie auf Grund der Gegendarstellung des Betroffenen inzwischen korrigiert hat. Für das Bistumsarchiv ist das nicht in jedem Fall erkennbar, aber es haftet dafür, wenn es eine Seite wie einen eigenen Auftritt zur Verfügung stellt.

Zum andern besteht das gleiche Problem bei Printpublikationen (z.B. Pfarrbriefen), bei denen unstreitig ein Einsichtsrecht auch für abgelegte Exemplare angenommen und von der Zeitungspresse auch praktiziert wird. Eine Einsichtnahme durch Besucher des Archivs allein auf einem hierfür zur Verfügung gestellten Rechner, halte ich daher für möglich. Dem Bistumsarchiv wurde das entsprechend mitgeteilt.

3.3 Kindertagesstätten

3.3.1 Vortrag vor Kita-FachberaterInnen des Caritasverbandes Hildesheim

Am 07. Marz 2013 hatten mich die Fachberater und Fachberaterinnen zu einem Informationsgespräch über datenschutzrechtliche Fragen im Kindergarten eingeladen. Erörtert wurde vor allem die Frage, ob Kindergärten den Umgang der Eltern mit sozialen Netzwerken wie Facebook reglementieren können. Vorgeschlagen wurde hierfür eine Anlage zum Betreuungsvertrag.

In der Diskussion wurde erörtert, ob einschränkende Bedingungen insoweit überhaupt unter Beachtung des Gesetzes über Allgemeine Geschäftsbedingungen möglich und tragbar sind und die Eltern in ihrem Erziehungsrecht nicht unangemessen benachteiligen. Es ist Sache der Eltern, ob und in welcher Form ihr Kind in sozialen Netzwerken präsentiert wird, ob sie aus elterlichem Stolz Fotos ihrer Jüngsten veröffentlichen oder in Kenntnis der Risiken eher hierauf verzichten. Reglementierungen führen insoweit zu einer Beschränkung ihrer allgemeinen Handlungsfreiheit[22] und des Rechts, über die

[22] Art. 2 Abs. 1 GG

Erziehung seiner Kinder selbst zu entscheiden[23]. Zudem stellt sich die Frage nach einer Kontrolle durch die Kindergartenverwaltung, die nur möglich wäre, wenn man die Eltern zwingen würde, den Kindergarten auf ihre „Freunde“liste zu setzen oder den Hinweisen, Beschwerden oder gar Anschwärzungen anderer Eltern nachzugehen. In jedem Fall würde massiv in das Elternrecht eingegriffen. Eine solche Einschränkung steht, in ausschließlich gravierenden Fällen, der staatlichen Aufsicht durch die Jugendämter zu.

Stattdessen habe ich vorgeschlagen, den Eltern ein Konzept in Form von „Social Media Guidelines“ vorzulegen. Dabei soll auf die gerade Kindern drohenden Gefahren aufmerksam gemacht und zulässige Strategien für einen verantwortungsvollen Umgang mit dem Netzwerk entwickelt werden. Eine Überprüfung oder Kontrolle der Eltern findet dabei nicht statt. Solche Guidelines werden oft als hilfreich betrachtet, vor allem von Eltern, die nicht genau über die Hintergründe informiert sind.

Zudem muss sich natürlich auch der Kindergarten selbst zuverlässig verhalten, wenn es um den Schutz der ihm anvertrauten Kinder geht. Und das bedeutet vor allem:

- Keine eigenen Facebook-Fan Pages einrichten!
- Keine Fotoveröffentlichung der Kinder bei Facebook.
- Keine Fotoveröffentlichung der Kinder auf der eigenen Webseite ohne ausdrückliche Einwilligung der Eltern.

Da dieses Problem in vielen Kindertagestätten auftauchen könnte, ist das Besprechungskonzept hier in der Anlage mit abgedruckt.

3.3.2 Veröffentlichung von Fotos im Internetauftritt der katholischen Kindertagesstätten im Erzbistum Hamburg

Die Veröffentlichung von Bildern auf Internetseiten, auf denen Personen eindeutig zu erkennen sind, bedarf der Zustimmung der Betroffenen. Das gilt insbesondere für Fotos von Kindern und Jugendlichen. Hierzu haben die Datenschutzbeauftragten der evangelischen und katholischen Kirche in einer gemeinsamen Stellungnahme schon 2008 eine eingehende Erklärung abgegeben. Der Caritasverband für das Erzbistum Hamburg hat darum gebeten, die von ihm diesbezüglich entworfenen Einwilligungserklärungen aus datenschutzrechtlicher Sicht zu überprüfen. Sie entsprachen den gesetzlichen Anforderungen und waren insoweit nicht zu beanstanden.

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.

[23] Art. 6 Abs. 2 GG

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.

3.3.3 „kita.web“ in Niedersachsen. Freischaltung von Daten für die Jugendämter

Nach dem hierzu veröffentlichten Handbuch des Niedersächsischen Kultusministeriums[24] verwirklicht die webbasierte Anwendung „kita.web“ das E-Government im Bereich des KiTaG. Durch die Benutzung einer sicheren SSL-Seite, den Verzicht auf aktive Inhalte wie Java und eine Anmeldung durch Benutzernamen und Passwort. Letzteres muss aus acht Zeichen bestehen und dabei mindestens einen Buchstaben und zwei Zahlen enthalten. Dadurch ist von vornherein ein umfangreicher Schutz vorgesehen.

Die Träger der Kindertagesstätten können hier eine Reihe von Daten eingeben und für die Jugendämter freischalten. Das KiTaG gibt hierfür die gesetzliche Grundlage. So können verpflichtende Auskünfte zur Finanzierung, Struktur und personelle Qualifikation übermittelt werden. Bezüglich der Daten von Kindern besteht nach § 14 KiTaG ein Auskunftsanspruch auf Übermittlung der Namen, Anschriften und Geburtsdaten für die Ermittlung des Bedarfs an Tagesplätzen. Diese Informationen können wie bisher über normale Post verschickt werden. Das kita.web ist ein freiwilliges Angebot[25] zur Arbeitserleichterung. Dabei wurden die gesetzlich festgelegten Bedingungen beachtet.

Dem Caritasverband für das Bistum Hildesheim wurde daher mitgeteilt, dass derzeit keine datenschutzrechtlichen Bedenken bestehen, an dem Verfahren teilzunehmen.

3.3.4 Vortrag vor KiTa-Leiterinnen in Hamburg

Am 13.02.2014 war der Diözesandatenschutzbeauftragte Gast einer Konferenz der KiTa-Leiterinnen im Erzbistum Hamburg. Für etwa eine Stunde bestand die Gelegenheit, über datenschutzrechtliche Fragestellungen zu sprechen. Die Sitzung wurde insoweit vorbereitet, als ein Überblick über die geltenden Rechtsgrundlagen sowie grundlegendes Wissen für die Praxis in einer Tischvorlage überreicht wurden. In einer sehr lebhaften Veranstaltung wurden dann noch spezielle „drückende“ Fragestellungen erörtert.

Der Diözesandatenschutzbeauftragte wies bei dieser Gelegenheit auch darauf hin, dass die Kollegen von den Baden-Württembergischen Diözesen, Herr Dr. Fachet, und der Evangelischen Landeskirche in Württemberg, Herr Dr. Gutenkunst, gemeinsam

[24] Nds. Kultusministerium: „kita.web. Handbuch. Rolle Jugendamt (einmalige Beschreibung Stand März 2013), S. 4
[25] Handbuch, S. 11

eine Handreichung zum Datenschutz in Kindertagestätten geschrieben haben, die inzwischen vom Baden-Württembergischen Ministerium für Kultus, Jugend und Sport übernommen wurde und in sehr leicht verständlicher Art über den „Datenschutz in Kindertageseinrichtungen – zum Schutz des Kindes“ informiert. Die Schrift richtet sich in erster Linie an Eltern und ist hierfür in einer Fülle von übersetzten Fassungen erschienen. Dieser Hinweis fand großes Interesse. Allen Kindertagesstätten ist zu empfehlen, diese Handreichung zu verwenden[26].

3.4 Schulen

3.4.1 Datenschutzrechtliche Beratung der Edith-Stein-Schulstiftung im Bistum Magdeburg

Vor dem Bezug eines neuen Schulgebäudes entstanden Fragen zur IT-Gestaltung in der Verwaltung und bezüglich des Netzwerks der Unterrichtsräume. Zur Klärung wurde der Diözesandatenschutzbeauftragte angesprochen.

Dabei wurde darauf hingewiesen, dass die Rechner für die Verwaltung und die Rechner für Unterrichtszwecke vollständig voneinander getrennt sein müssen. Auch eine Verbindung durch ein gemeinsames Netzwerk muss ausgeschlossen sein. Beide Systeme dienen völlig unterschiedlichen Zwecken und werden auch von völlig getrennten Personengruppen genutzt. Der Schulverwaltungsserver ist vor unbefugtem Gebrauch, insbesondere durch EDV-technisch begabte Schüler, zu schützen.

Darüber hinaus ist für die Schulverwaltungssoftware eine Rechteverwaltung erforderlich, die die Zugriffsmöglichkeiten nach dem Tätigkeitsprofil der Mitarbeiter festlegt.

3.4.2 Überprüfung von Facebook-Aktivitäten von Schülern

Ein Vater führte bei mir Beschwerde über das Verhalten eines Schulsozialarbeiters, der auf die Beschwerde einer Mitschülerin Veranlassung sah, seinen 13-jährigen Sohn nicht nur zu Rede zu stellen, sondern ihn auch zu zwingen, unter Preisgabe seines Passwortes ihm seinen Facebook Zugang zu öffnen und dort selbst Feststellungen zum Verhalten des Jungen zu treffen und ihn weiter zu zwingen, den Link zu der Mitschülerin zu löschen. Der Junge hatte ein von dem Mädchen selbst unter YouTube veröffentlichtes Video in seinen Facebook-Account übernommen und mit dem Kommentar „Ha ha“ kommentiert.

Mag das Verhalten des Schülers gegenüber dem Mädchen auch unangemessen gewesen sein, hat die Schule dennoch kein Recht, in eigener Regie quasi „strafrechtliche Ermittlungen“ anzustellen. Selbst ein Staatsanwalt hat gegenüber dem Beschuldigten nicht das Recht, ihn zur Preisgabe seines Passwortes zu zwingen. Der pädagogische

[26] Kann kostenlos heruntergeladen werden unter http://kultusportal-bw.de/KINDERGAERTEN-BW,LDE/Startseite/Datenschutz, die deutsche Fassung steht auch auf der Webseite des Diözesandatenschutzbeauftragten unter http://www.datenschutz-kirche.de/sites/default/files/file/download/Merkblatt%20DS%20in%20Kindertageseinrichtungen.pdf

Auftrag der Schule berechtigt sie nicht, in dieser Form in das Privatleben der Schüler einzugreifen. Sie kann lediglich durch ihren Bildungsauftrag dafür sorgen, dass die Risiken sozialer Netzwerke besser verstanden werden und persönliche Verhaltensweisen, die zu einer Bloßstellung oder Verächtlichmachung anderer Personen führen, dort zu unterbleiben haben, weil solche Auseinandersetzungen von weiteren Usern aufgegriffen werden könnten und dann zu einer vollständigen „Niedermachung“ des Opfers führen können.

Ich hatte daher das Verhalten des Schulsozialarbeiters zu beanstanden und gleichzeitig der Schule nahezulegen, dass sie gemeinschaftlich Lehrer und Sozialarbeiter darauf hinweist, dass die Möglichkeiten eigener Ermittlungen zur Aufdeckung von Mobbing oder anderer Straftaten eng begrenzt sind.

3.5 Krankenhäuser

3.5.1 Gemeinsame Orientierungshilfe Krankenhausinformationssysteme

Schon 2009 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem Beschluss eine datenschutzkonforme Nutzung von Informationstechnik in Krankenhäusern gefordert. Als Problem wurde erkannt, das bei elektronischer Datenverarbeitung bei den eingesetzten Systemen oftmals keine datenschutzgerechte Verfahrensweise vollständig möglich ist. Andererseits werden die Möglichkeiten, die diese Systeme bieten, von den Krankenhäusern nicht vollständig ausgeschöpft. Es wurde daher eine Unterarbeitsgruppe aus den Kreisen "Gesundheit & Soziales" und "Technik" mit der Erarbeitung einer Orientierungshilfe beauftragt, die sowohl den Anwendern wie auch den Anbietern Hilfestellung zum Einsatz und zur Schaffung solcher Systeme geben sollte. Der Datenschutzbeauftragte der norddeutschen Bistümer und der Datenschutzbeauftragte der EKD wurden eingeladen hierbei mitzuwirken. Auf diese Weise sollten auch die kirchlichen Krankenhäuser angesprochen werden. Beide haben von dieser Möglichkeit Gebrauch gemacht und sich aktiv in die gemeinsamen Beratungen eingebracht.

Die Arbeitshilfe wurde dann im März 2011, nach vielen Beratungen, Expertenanhörungen von Mitarbeitern der wichtigsten Anbieter, Betreibern und Datenschutzbeauftragten von Krankenhäusern, verabschiedet. Sie wurde sowohl von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dem "Düsseldorfer Kreis", in dem Datenschutzbeauftragte der Länder mit Vertretern der freien Wirtschaft konferieren und auch von den Tagungen der Datenschutzbeauftragten sowohl in der Evangelischen wie auch der Katholischen Kirche angenommen.

Sie besteht aus zwei Teilen. Der erste Teil ist eine Zusammenstellung und Erläuterung der rechtlichen Anforderungen an eine datenschutzgerechte Verarbeitung von Patientendaten, soweit sie sich einheitlich den Landesgesetzen und den kirchlichen Vorschriften hierzu entnehmen lassen. Das Ergebnis war die Formulierung der "Normativen

Eckpunkte zur Zulässigkeit von Zugriff auf elektronische Patientendaten im Krankenhaus". Im zweiten Teil wurde auf die Möglichkeit der technischen Umsetzung und die hierbei zu beachtenden Anforderungen an die Gestaltung der Systeme seitens der Hersteller und die Nutzung bereits bestehender Möglichkeiten von Seiten der Krankenhausbetreiber hingewiesen. Natürlich sind die technischen Ausführungen insofern nicht verbindlich, als auch andere Lösungen möglich sind. Diese müssen dann aber den gleichen Zielerreichungsgrad zum Schutz der Patientendaten erreichen. Die "Technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen" sind daher ein wichtiger Teil für die Verbesserung des Datenschutzes in Kliniken.

Aufgrund der Anmerkungen und Kritiken aus der Praxis zu diesem Arbeitspapier ist die Orientierungshilfe weiter fortgeschrieben worden und liegt nunmehr in einer zweiten Fassung vor[27]. Dabei wurde eine redaktionelle Überarbeitung vorgenommen und vor allem der erste Teil im Sinne einer besseren Lesbarkeit und Verständlichkeit präzisiert. Die Gespräche mit Verbänden, insbesondere der DKG, haben dazu beigetragen, dass einige Ausführungen, die Anlass zu Missverständnissen gegeben haben, berichtigt wurden. Weiterhin wurden für einrichtungs- und mandantenübergreifende Zugriffe verschiedene Szenarien dargestellt. Im zweiten, technischen Teil wurde der Bezug zu den rechtlichen Rahmenbedingungen verdeutlicht und damit zum Ausdruck gebracht, dass diesen Anforderungen durch verschiedene Systeme und Verfahren entsprochen werden kann.

Das Verfahren wird von den Teilnehmern vorläufig als abgeschlossen betrachtet. Die Notwendigkeit einer dritten Version stellt sich zurzeit nicht. Es bleibt also zunächst abzuwarten, wie die Orientierungshilfe in der Praxis umgesetzt werden kann.

3.5.2 Prüfung eines Berliner Krankenhauses in kirchlicher Trägerschaft

Im Tätigkeitsbericht 2004 - 2009 hatte ich unter Punkt 5.4 über die bis dahin noch offene Zusammenarbeit mit dem Berliner Datenschutzbeauftragten für die Prüfung von Krankenhäusern berichtet. Die dort genannten Fragen konnten kurze Zeit später befriedigend gelöst werden. Bei der Prüfung eines von mir ausgewählten Hauses wurde ich dankenswerter Weise in Amtshilfe von einer Juristin und einem Techniker des Berliner Datenschutzbeauftragten unterstützt.

Die Untersuchung fand vor Ort am 24. Februar 2012 statt. Dabei konnten wir das System, ein "Siemens Medico//s" und die vom Anwender getätigten Einstellungen in Augenschein nehmen und prüfen. Vom Krankenhaus stand uns die Betriebsleiterin, ein Vertreter der Firma, die die technische Betreuung vornimmt und zeitweise ein Arzt und eine Helferin für Gespräche zur Verfügung. Die Klinik verfügt nicht über eine vollständige Patientenverwaltung auf dem KIS. Patientendaten werden nach wie vor in

[27] Abgedruckt auf meiner Webseite unter „http://www.datenschutz-kirche.de/sites/default/files/file/OH_KIS_v2(1).pdf

Papierakten geführt. Das elektronische System unterstützt aber die Arbeit der Ärzte und Helfer, indem es Arztberichte, Befunde, Laborwerte und radiologische Ergebnisse speichert. Die Technik ist räumlich gut untergebracht und durch einen elektronischen Schließmechanismus und eine handfeste Vergitterung der Fenster vor dem Zutritt Unberechtigter geschützt. Insoweit gab es nichts zu beanstanden.

Es ergaben sich aber vier wesentliche Punkte, die mit dem Datenschutz nicht zu vereinbaren sind:

1. Die Absicht, die Verwaltung der Patientendaten komplett auf einen Drittdienstleister zu übertragen. Der Klinikleitung wurde gesagt, dass dies im Widerspruch zu ihrer gesetzlichen Verpflichtung nach §§ 24 VI LKG stehe, die Verarbeitung der Daten selbst durchzuführen.
2. Das Fehlen einer aufgabenspezifischen Rechteverwaltung, die sicherstellt, dass nur Ärzte und Pfleger die Daten einsehen können, wenn sie unmittelbar mit der Behandlung des Patienten zu tun haben. Eine Einsichtsmöglichkeit in der Form, dass allen Ärzten der Einblick in sämtliche Patientenakten möglich sei, ist mit der ärztlichen Verschwiegenheitspflicht nicht zu vereinbaren, da diese auch die Ärzte untereinander bindet.
3. Unzulässigkeit der ungeschützten Speicherung von Arztberichten. Sie wurden von dem Programm Medico in einem Dateisystem des Servers abgelegt, der nicht den Zugriffsbeschränkungen des Klinikinformationssystems unterliegt. Hier wurde empfohlen, durch das Betriebssystem zu verhindern, das Verbindungen zu Netzlaufwerken auf dem Server hergestellt werden können. Die temporären Dateien sollten möglichst auf einem Arbeitsplatzrechner in Verzeichnissen, die ausschließlich dem Zugriff des Arztes unterliegen, gespeichert werden.
4. Fehlende Protokollierung über die Zugriffe auf Patientenakten. Eine Kontrolle darüber, wer, wann und welche Daten bearbeitet oder genutzt hat und ob der Zugriff insoweit im Hinblick auf die Aufgaben des Betreffenden nachvollziehbar ist, ist so nicht möglich.

Es wurde ein Prüfungsbericht hierüber erstellt. Mit der Klinikleitung wurde vereinbart, sie bei der Herstellung datenschutzgerechter Bedingungen zu unterstützen und die notwendigen Veränderungen zu begleiten. Da es sich hierbei um gravierende Maßnahmen handelt, deren Umsetzung nicht kurzfristig möglich sind, dauert das Verfahren noch an.

3.5.3 Angebot externer Archivierung von Patientenakten durch die Firma Rhenus

Bereits im letzten Bericht wurde zur rechtlichen Problematik der Auslagerung nicht mehr benötigter Patientenakten durch Krankenhäuser ausführlich berichtet[28]. Auch im abgelaufenen Zeitraum musste das Thema wieder bearbeitet werden.

[28] Siehe Tätigkeitsbericht 2004 – 2009, Nr. 3.5.1, Seite 25

Die Firma Rhenus hatte einem Krankenhaus die Einlagerung in ihrem Sicherheitsarchiv angeboten. Dies sollte in der Weise geschehen, dass die Klinik spezielle Kartons des Anbieters mit den zu archivierenden Akten füllt und der jeweilige Inhalt protokolliert und anschließend verplombt wird. Auf dem Karton sollte sich ein Barcode befinden, der vom Anbieter eingescannt wird. Hierdurch kann sein Inhalt eindeutig dem Auftraggeber zugewiesen werden. Die Protokolle mit den Aufzeichnungen, welche Akten sich in welchem Karton befinden, sollten allein im Besitz des Auftraggebers verbleiben. Für die Wiederanforderung einer so ausgelagerten Akte bot der Auftragnehmer drei Möglichkeiten an:

1. Eine Versendung des Kartons an die Klinik, die in diesem Fall die Plombe entfernt und nach Erledigung wieder mit dem Karton zurück übermittelt.
2. Öffnen der Plombe und Überbringen der angeforderten Akte durch Mitarbeiter des Auftragnehmers.
3. Öffnen der Plombe durch den Auftragnehmer, Scannen der angeforderten Akte mit anschließend digitalem Versand an den Auftraggeber.

Die Klinik wollte wissen, ob ein solches Verfahren datenschutzgerecht ist. Ihr wurde gesagt, dass

1. die Akten im Gewahrsam des Krankenhauses bleiben müssen, was nur dann der Fall ist, wenn aus Sicht der Klinik genau feststünde, wo sich die Akte befindet, sie jederzeit darüber verfügen könne und sie imstande sei, Dritte vom Zugriff auszuschließen;
2. sie auch nachträglich feststellen kann, wer auf welche Akte und aus welchen Gründen Zugriff genommen hat;
3. die Verantwortlichkeiten für eine Anforderung der Akte, die Dokumentation der Entnahme und die Rückführung ins Archiv klar und nachprüfbar geregelt sein müssen.

Darüber hinaus sei das Verfahren in einer Vereinbarung nach § 8 KDO zu regeln. Die Klinik hat von dieser Möglichkeit dann letztlich keinen Gebrauch gemacht und die Akten wie bisher auf dem eigenen Gelände archiviert.

3.5.4 Änderungen am Klinikinformationssystem für Krankenhäuser im Bistum Osnabrück

Das Marienhospital und das Kinderhospital Osnabrück (Pädiatrie, Kinder- und Jugendpsychiatrie) hatten bisher schon eine gemeinsame Datenbank zur Verwaltung der Patientenakten. Mit der Entstehung des neuen Christlichen Kinderhospitals Osnabrück soll dieses die Pädiatrie übernehmen und gleichzeitig Kinderchirurgie durchführen, während das Kinderhospital Osnabrück nur noch die Kinder- und Jugendpsychiatrie versorgt. Es soll ebenfalls an die gemeinsame Datenbank angeschlossen werden. Alle drei Häuser sind mit einer eigenen IK-Nummer im Krankenhausverzeichnis eingetragen. Bei der insoweit notwendigen Neugestaltung des Klinikinformationssystems

(AGFA Orbis) entstanden Umsetzungsschwierigkeiten im Hinblick auf die Orientierungshilfe Krankenhausinformationssysteme (siehe Zi. 3.5.1). Diesbezüglich haben die Verantwortlichen mit dem Diözesandatenschutzbeauftragten Kontakt aufgenommen, um die bestehenden Probleme zu klären. Am 01.12.2011 fand in Hannover hierzu ein gemeinsames Gespräch statt.

Dabei wurde von mir deutlich gemacht, dass für drei eigenständige Krankenhäuser zwar ein gemeinsames Datenverarbeitungssystem vorgesehen werden könne, dabei müsse jedoch eine Trennung nach den einzelnen Kliniken erfolgen. Die Datenbank müsse in diesem Sinne „mandantenfähig“ sein. Dies entspricht den Ausführungen unter Ziff. 30 der OH KIS. Dabei sollte berücksichtigt werden, dass der Patient in der Regel damit rechnet, dass seine Gesundheitsdaten nur in der Klinik bekannt sind, in der er auch behandelt wird. Mit der Organisation des Trägers und bestehenden Krankenhausverbünden kennt er sich meistens nicht aus. Mitarbeiter eines anderen Krankenhauses, auch wenn es mit dem behandelnden Haus organisatorisch verbunden ist, sind „Dritte“ im Sinne von § 4 der Ordnung zum Schutz von Patientendaten. Strafrechtlich gesehen besteht die Schweigepflicht auch gegenüber anderen Ärzten, die selbst nicht an der Behandlung des Patienten beteiligt sind.

Jedes Krankenhaus hat zudem im Rahmen seiner Mandatsberechtigung eine eigene Rechte- und Zugriffsverwaltung zu installieren, die nur den versorgenden Fachbereichen einen Zugriff auf Patientendaten ermöglicht.

Da es zwischen den beteiligten Kliniken gelegentlich zu einem Behandlungswechsel kommt, bei dem der Patient, der zuerst im Christlichen Kinderkrankenhaus behandelt wurde, vom Marienhospital übernommen wird, bestehen vor allem Schwierigkeiten mit den Patientenstammdaten, die häufig, vor allem bei Patienten mit Migrationshintergrund bestehen und abweichende Schreibweisen oder andere Fehleingaben enthalten. In anderen Systemen, wie Nexus Healthcare wird insoweit eine Mehrmandantendatenbank in Form eines „Master Patient Index“ eingerichtet, bei der allerdings nur die Patienten-ID, der Name, die Anschrift und das Geburtsdatum aufgenommen werden. Den Verantwortlichen sind hierzu Ausführungen des Hessischen Datenschutzbeauftragten und eine Stellungnahme der Nexus AG übermittelt worden, mit der Bitte um Prüfung, ob diese Lösung für sie gangbar wäre und sich auch auf einem System von AGFA verwirklichen ließe. Eine Antwort hierauf hat der Unterzeichner bisher nicht erhalten.

In der Sache halte ich diesbezüglich eine Gesamtprüfung des Systems für erforderlich. Dabei müsste mit Unterstützung eines Technikers des Datenschutzbeauftragten, unter Einbeziehung des IT-Leiters und bei Anwesenheit von Anwendern (ein Arzt und eine Krankenschwester), das System vor Ort in Augenschein genommen werden. Sollten sich dabei Feststellungen ergeben, die mit dem Datenschutz nicht vereinbar sind, sollten in einem gemeinsamen Verfahren die notwendigen Änderungen schrittweise herbeigeführt werden. Ziel ist hierbei nicht eine „Beanstandung“ sondern eine fachliche

Zusammenarbeit zwischen den Beteiligten zur Herstellung eines datenschutzgerechten Verfahrens. Nur steht mir hier, anders als in Berlin (siehe Zi. 3.5.2), kein Mitarbeiter des Landesbeauftragten im Wege der Amtshilfe zur Verfügung und über einen eigenen technischen Mitarbeiter verfügt der Diözesandatenschutzbeauftragte derzeit nicht.

3.5.5 Erweiterung des Projekts „Babylotse“ durch Einbeziehung niedergelassener Ärzte

Das beim Katholischen Kinderkrankenhaus Wilhelmsstift in Hamburg erfolgreich praktizierte Projekt „Babylotse“ der Stiftung SeeYou sollte auf die Einbeziehung niedergelassener Gynäkologen erweitert werden. Hierbei galt es, die Einwilligungserklärungen der Mütter entsprechend anzupassen und die Aufbewahrungsfrist für die Akten von SeeYou festzulegen. An den Gesprächen war auch der Hamburgische Datenschutzbeauftragte im Hinblick auf die Zuständigkeit seiner Datenschutzaufsicht über niedergelassene Ärzte beteiligt. Nach längerer Diskussion wurde das Ergebnis erzielt, die Akten gemäß § 630f Abs. 3 BGB zehn Jahre lang aufzubewahren. Zwar schreibt das Hamburgische Krankenhausgesetz eine 30-jährige Aufbewahrungsfist vor, die Stiftung SeeYou ist jedoch eine unselbständige Einrichtung des Katholischen Krankenhauses Wilhelmstift und unterliegt somit den kirchlichen Regelungen. Die für das Bistum geltende Krankenhausdatenschutzordnung sieht aber keine feste Frist vor. Sie bestimmt lediglich, dass Patientendaten zu löschen sind, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind und keine vorgeschriebenen Aufbewahrungsfristen mehr bestehen. Soweit das Bürgerliche Gesetzbuch als allgemeines Gesetz eine Frist von zehn Jahren vorsieht, ist diese auch für kirchliche Einrichtungen verbindlich. Allerdings ist wegen der Abweichung ein Hinweis hierauf an die Behörden sinnvoll.

3.6 Soziale Einrichtungen

3.6.1 E-Mail-Übermittlung von Daten des Kinder- und Jugendnotdienstes an das Sozialamt

Eine Kinder- und Jugendnotdienststelle der Caritas Brandenburg-Ost fragte hier an, ob Erstinformationen der in Obhut genommenen Personen gem. § 42 Abs. 1 SGB VIII durch Mail-Schreiben an das Sozialamt der Stadt Frankfurt/Oder weitergeleitet werden können. Hierzu wolle man den personenbezogenen Teil der Daten mit der Software „FreePDF“ verschlüsseln und als Anhang beifügen. Da mit der Stadt Frankfurt/Oder auch eine Stelle beteiligt war, die der Datenschutzaufsicht der Brandenburgischen Landesbeauftragten untersteht, wurde hier eine gemeinsame Stellungnahme angestrebt.

Mit Schreiben von April 2011 teilte die Landesaufsicht mit, dass gegen ein solches Verfahren dann keine Einwände bestehen, wenn folgende Rahmenbedingungen beachtet werden:

- Die eingesetzte Software müsse den aktuellen Stand der Verschlüsselungstechnik einsetzen (zur Zeit AES-Verschlüsselung mit mindestens 128-bit Schlüssellänge) und sicher eingebunden sein. Dem entsprechen derzeit Tools wie beispielsweise

„AxCrypt“, „FileCrypter“ und „PDFCreator“. Die Software „FreePDF“ enthalte jedoch nur ein rudimentäres Verschlüsselungsverfahren der Firma Adobe und sei daher für geschützte Sozialdaten ungeeignet.
- Es muss ein sicheres Passwort verwendet werden (mind. 16 Zeichen mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).
- Das Passwort darf nicht per E-Mail weitergegeben werden, sondern muss durch eine zuverlässige Weise (z.B. Telefon) an den Empfänger übermittelt werden.

Mit der Beachtung dieses Verfahren waren die beteiligten Stellen einverstanden. Seither wirbt der Diözesandatenschutzbeauftragte im Sozial- und Gesundheitsbereich dafür, diese preisgünstige und einfache Lösung zu verwenden, wenn ein Versand durch E-Mails wegen der Schnelligkeit des Transports notwendig ist.

3.6.2 Social Office in der Caritas Jugendsozialarbeit

Aufgrund der Eingabe einer Mitarbeiterin wurde der Einsatz des Programms „Social Office“ der Firma EasyData OHG geprüft. Dabei wurde zunächst ein Gespräch mit der Fachleiterin geführt, die dabei Gelegenheit hatte ihre Bedenken mitzuteilen und dann mit dem Einrichtungsleiter eine genaue Prüfung durchgeführt.

Das System ist so ausgelegt, dass es von 9 Mitarbeitern gleichzeitig genutzt werden kann, obwohl 14 Mitarbeiter vorhanden sind. Es gibt eine eingehende Rechteverwaltung, wobei die Nutzungsmöglichkeiten hinsichtlich der Module sowie auch nach den Eingriffsrechten (Schreiben, Lesen, Verändern, Löschen) nach der eingenommenen Rolle (Administrator, Sozialpädagoge, usw.) verteilt werden. Hierdurch ergeben sich folgende Rahmenbedingungen:

- Die Adressverwaltung ist für alle Beteiligten zugänglich
- Notizen waren ebenfalls für alle sichtbar, weil sie programmtechnisch der Adressverwaltung zugeordnet sind. Es wurde vereinbart, die Notizen aus der Adressverwaltung herauszunehmen und damit ebenfalls vertraulich zu machen.
- Fallakten sind nur nach Eingabe des entsprechenden Accounts sichtbar.

Programmupdates werden automatisch ohne Mitwirkung des Anbieters durchgeführt.

Im Falle eines notwendigen Supports oder einer Wartung wird diese online erledigt. Hierbei wird eine Verbindung, auf Veranlassung des Administrators über Netviewer One2One, in gesicherter Form hergestellt. Der Mitarbeiter von EasyData kann hierbei nur die Seiten sehen, die vom Auftraggeber aufgerufen werden. Es besteht somit eine vollständige Kontrolle über die Zugriffe bei Wartungsarbeiten.

Zu beanstanden war allerdings, dass mit der Firma EasyData kein schriftlicher Vertrag bestand und trotz der Mitarbeiterzahl kein betrieblicher Datenschutzbeauftragter bestellt worden ist. Mittlerweile konnten diese Punkte, teilweise unter Mitwirkung des Diözsandatenschutzbeauftragten, erledigt werden.

3.6.3 Zentrale Datenverarbeitung für zehn Beratungsstellen

Im Bericht 2004 – 2009 war über die Planung einer zentralen Datenverarbeitung für zehn psychologische Beratungsstellen im Bistum Osnabrück berichtet worden[29]. Der Datenschutzbeauftragte nahm an einer Mitarbeiterversammlung im September 2010 teil, bei der es um die Umstellung der vorhandenen EDV-Anlagen auf eine Lösung mit einem Zentralserver ging. Dabei machte er noch einmal deutlich, dass hier personenbezogene Daten verarbeitet werden, die der Verschwiegenheitspflicht nach § 203 StGB unterliegen und daher sehr hohe Sicherheitsmaßnahmen erfordern. Er verlangte unter anderem, dass die Übertragung der Daten auf den Server, wie auch die Speicherung dort, zu verschlüsseln seien. Einige Zeit später erfuhr er dann durch die Mitarbeitervertretung, dass die Abteilungsleiterkonferenz des Bischöflichen Generalvikariats entgegen seiner Forderung entschieden hatte, eine Verschlüsselung nicht durchzuführen. Hierzu nahm er mit Schreiben vom 07.02.2011 an den Generalvikar noch einmal Stellung und machte dabei deutlich, dass die Inbetriebnahme des Verfahrens in der geplanten Form im Widerspruch zum geltenden kirchlichen Datenschutzrecht stehe und drohte wegen der gravierenden Mängel mit einer Beanstandung nach § 18 Abs. 1 KDO.

Das Bistum hat hierauf reagiert und inzwischen eine Sicherung des Servers mit Symantec PGP NetShare 10 durchgeführt. Dem Datenschutzbeauftragten wurden inzwischen auch ausreichende Unterlagen zur eingesetzten Software SoPart EBuCO und eine ausführliche Verfahrensbeschreibung zur Verfügung gestellt. Mit dem Bistum wurde vereinbart eine Systemprüfung vor Ort durchzuführen, an der auch der inzwischen vorhandene externe Techniker, ein Mitarbeiter der Firma Datenschutz Nord GmbH, teilnehmen wird.

3.6.4 Einsatz von De-Mail in verschwiegenheitspflichtigen Beratungsstellen

Die Bundesregierung hat die Schaffung von De-Mail gefördert, um einen besseren Schutz von E-Mails zu gewährleisten, die ansonsten als „offene Postkarte“ versandt werden müssen. Hieraus ergibt sich für viele Dienststellen die Frage, ob dieses Konzept auch für den Versand personenbezogener Informationen, die einer Verschwiegenheitspflicht nach § 203 StGB oder dem Sozialgeheimnis unterliegen, in Betracht kommt. Problematisch ist dabei, dass De-Mail keine Ende-zu-Ende-Verschlüsselung vornimmt, sondern lediglich den Übertagungsweg sichert. Die Mails bleiben aber in den Postfächern der Provider im Klartext gespeichert. Deshalb hat der Bundesbeauftragte für den Datenschutz in einer hierzu herausgegebenen Stellungnahme erklärt, De-Mail sei für den normalen Gebrauch zu empfehlen, nicht jedoch für den Versand von Daten im Rahmen von § 203 StGB oder Sozialdaten[30].

[29] Siehe Tätigkeitsbericht 2004 – 2009, Kap. 3.6.2, Seite 28

[30] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail vom 01.03.2013, veröffentlicht unter der Webadresse: http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailHandreichung.pdf?__blob=publicationFile

3.7 Personalangelegenheiten

3.7.1 Einführung des Programms „MediFox-Mobil“ bei einem ambulanten Pflegedienst

Durch das Schreiben einer Mitarbeitervertretung wurde ich darauf aufmerksam, dass der Einsatz einer mobil arbeitenden Software für die ambulante Betreuung durch Pflegedienste geplant war. Hierfür wollte der Dienstgeber eine Dienstvereinbarung mit der MAV abschließen. Dabei sollten die Beschäftigten ein mobiles PDA mit GPS-Empfänger erhalten, in das sie die geleisteten Arbeiten nach Art und Umfang einzugeben haben um sie dann an die zentrale Datenerfassung weiterzuleiten. Als Systembestandteile des Programms wurden benannt:

1. Stammdatenverwaltung
2. Abrechnung und Verwaltung
3. Personaleinsatzplanung
4. Mobile Datenerfassung
5. Pflegeplanung und Pflegedokumentation
6. Management Informationssystem

Dabei stellten sich folgende Probleme:

1. Eine vollständige Überwachung der Mitarbeiter mittels GPS-Ortung und der Möglichkeit der Erstellung kompletter Bewegungsprofile ist weder notwendig noch statthaft. Nur in Fällen, in denen dies zum Schutz des Mitarbeiters notwendig ist (Beispiele sind Sicherheitsdienste) verstößt eine solche Beobachtung nicht gegen den Schutz der Menschenwürde.
2. Erfasst werden sensible Gesundheits- und Sozialdaten, die einem besonderen Schutz unterliegen und daher vor fremden Zugriff durch eine verschlüsselte Übertragung gesichert werden müssen.
3. Die Software darf nur die Erfassung solcher Patientendaten erlauben, die nach den Vorschriften des SGB XI für die Behandlungsdokumentation und die spätere Vergütung erforderlich sind.
4. Mitarbeiterdaten sind im Umfang auf den Teil zu beschränken, der für die Durchführung der ambulanten Leistungen und zeitabhängige Vergütungen notwendig ist.
5. Gefährdungspotential durch zusätzliche Privatnutzung der mobilen Endgeräte.

Das gesamte Verfahren muss technisch ausreichend beschrieben und dokumentiert werden. Dabei müssen auch die Verantwortlichkeiten klar geregelt werden. Insbesondere sind konkrete Bestimmungen zu Systemadministration, Vergabe von Zugriffsrechten und Zuständigkeiten für die ordnungsgemäße Auswertung der Dateien erforderlich. Auch für notwendige Vertretungsfälle oder Änderungen der Bearbeitungszuständigkeit sind datenschutzgerechte Verfahren zu benennen.

Diesen Anforderungen wurde der erste Entwurf einer Betriebsvereinbarung nicht gerecht, so dass ein Reihe von Änderungen hieran erfolgen mussten. In der letzten Fassung, die dann auch vereinbart wurde, sind wesentlich bessere Regelungen getroffen worden.

- Ein Verbot der privaten Nutzung der Geräte,
- die Benennung der erforderlichen Personaldaten beim Betrieb des Systems,
- ein Verbot der Nutzung zur Leistungs- und Verhaltenskontrolle und
- eingehende Nutzerprofile.

Nach Regelung des Einsatzes von MediFox-Mobil wurde auch eine Meldung nach § 3a KDO dem Diözesandatenschutzbeauftragten vorgelegt.

3.7.2 Probleme mit dem Postgeheimnis

Das heutzutage noch Probleme mit dem Postgeheimnis auftreten können, ist mehr als verwunderlich. So wurde von einer Mitarbeitervertretung angefragt, ob Post, die eindeutig an die MAV gerichtet ist, von der Posteingangsstelle der Einrichtung geöffnet werden dürfe. Selbstverständlich nicht! Sie ist in Anwendung von § 20 MAVO als vertrauliche Post verschlossen an die berechtigten Empfänger auszuhändigen.

In einem weiteren Fall wurde die Post an einen Krankenhausseelsorger durch seine Kollegin der anderen Konfession geöffnet. Das ist nur dann statthaft, wenn sich die beteiligten Personen hierzu ausdrücklich legitimieren. Der Schutz des Vertrauensverhältnisses zwischen Patient und Seelsorger muss in jedem Fall gewahrt bleiben.

3.7.3 Erweiterte Führungszeugnisse

Häufig wurde gefragt, wie mit erweiterten Führungszeugnissen umzugehen sei. Vor allem die Aufbewahrung einmal vorgelegter Zeugnisse, die Tragung der Kosten, die hierdurch entstehen und die Beibringung durch den Mitarbeiter selbst, waren immer wieder Gegenstand von Fragen. Dabei war zunächst einmal auf die Informationen hinzuweisen, die das Bundesministerium der Justiz hierzu zeitweilig herausgegeben hatte[31]. Darüber hinaus haben sich im Umgang hiermit folgende Maßnahmen bewährt:

- Die Anforderung beim Meldeamt ist durch den Mitarbeiter vorzunehmen.
- Er hat dabei ein Schreiben des Dienstgebers vorzulegen, durch das die Notwendigkeit der Beibringung und die Gründe hierfür benannt werden.
- Die Kosten hierfür sind im Bewerbungsverfahren von den Bewerbern zu tragen.
- Im Beschäftigungsverhältnis hat der Dienstgeber die Kosten zu übernehmen.
- Eine Aufbewahrung durch den Dienstgeber ist wegen der Nachweismöglichkeit erforderlich. Das Zeugnis sollte dabei in einem verschlossenen Umschlag zur Personalakte genommen werden.

[31] Frühere Seite: http://www.bundesjustizamt.de/DE/Themen/Buergerdienste/BZR/ErwFZ/ErwFZ__node.html?__nnn=true

Andere Formen bieten erheblich mehr Komplikationen. Die Aufbewahrung in einem gesonderten Ordner ist wegen der Einheitlichkeit der Personalakte zumindest im Beamtenrecht nicht statthaft und als „Geheimordner“ auch im Angestelltenrecht nicht tunlich. Die Verarbeitung durch einen Aktenvermerk unter Rückgabe des Originaldokuments an den Beschäftigten kommt der Dokumentations- und Nachweispflicht nicht ausreichend nach. Das gilt vor allem für die Ausnahmeregelungen nach § 32a BZRG.

3.7.4 Behandlung von Arbeitsunfähigkeitsbescheinigungen

Einen schwierigen Fall hatte der Caritasverband für Berlin. Arbeitsunfähigkeitsbescheinigungen sollten nicht mehr der zentralen Personalabteilung vorgelegt werden, sondern der regional tätigen Einrichtung, bei dem der Betreffende beschäftigt ist. Hierdurch würde der Name des ausstellenden Facharztes (möglicherweise ein Psychologe oder Psychiater) auch dem Betriebsleiter vor Ort bekannt. Eine gesetzliche Regelung zu dieser Frage gibt es bisher nicht. In Anlehnung an die Ausführungen des Unabhängigen Landeszentrums für Datenschutz in Kiel musste ich feststellen, dass auch bei Vorlage an die zentrale Personalabteilung eine Information an den Dienstvorgesetzten statthaft ist, da dieser über die Verwendbarkeit der Mitarbeiter informiert sein muss. Weiter hat das ULD Kiel ausgeführt:

> *„Soweit der AG rechtmäßig in den Besitz von Daten über den Gesundheitszustand der AN gelangt ist, ist er auch befugt, diese im Rahmen der Erforderlichkeit für das Arbeitsvertragsverhältnis zu speichern und weiter zu verarbeiten. Die Daten unterliegen in der Personalabteilung des AG nicht mehr dem Patientengeheimnis, auch wenn die Daten ursprünglich von einem Arzt übermittelt wurden. Sie unterliegen wohl aber einer* ***Zweckbindung****, deren Umfang entweder durch die Einwilligung des AN bestimmt wird oder durch den vertraglichen Zweck der Datenerhebung. Die Zweckbindung wird i.d.R. durch den Arbeitsvertrag definiert; so dürfen z.B. für Zwecke der Entgeltberechnung gespeicherte krankheitsbedingte Fehlzeiten auch für eine krankheitsbedingte Kündigung verwendet werden. U.U. können aber engere Zwecke vereinbart sein."*

Dabei können sich gegebenenfalls weitere Fragen stellen. Ist eine Betriebsärztliche Untersuchung des Betroffenen zur Feststellung der Arbeitsfähigkeit erforderlich? Und bei häufiger Fortdauer der Arbeitsunfähigkeit, ist in diesem Falle ein Krankengespräch zu führen? Diese Angelegenheiten sind sehr sensibel zu handhaben.

3.7.5 Unbeaufsichtigter PC für Mitarbeitervertretung

Die Mitarbeitervertretung eines Krankenhauses in Berlin hatte für ihre Arbeit zwar einen MAV-PC zur Verfügung. Dieser konnte nach eigenen Angaben aber vom Dienstgeber kontrolliert werden. E-Mails, besuchte Webseiten und Zeitprotokolle konnten von ihm oder beauftragten Mitarbeitern mitgelesen werden. Ich habe darauf hingewiesen, dass Mitarbeitervertreter nach § 20 MAVO zur Verschwiegenheit verpflichtet sind. Dies gilt auch gegenüber dem Dienstgeber. Ein Mitarbeiter muss die Zusammenarbeit und

Hilfestellung der MAV in Anspruch nehmen können, ohne dabei vom Dienstgeber beobachtet zu werden. Ich habe empfohlen in diesem Fall zunächst die Schlichtungsstelle anzurufen.

4. Öffentlichkeitsarbeit / Unterrichtung der Dienststellen

4.1 Internetauftritt

Die Webseite www.datenschutz-kirche.de wurde in der seit 2006 bestehenden Form weitergeführt und laufend inhaltlich ergänzt. Sie ist nach wie vor die einzige Internetadresse zum Datenschutz in der Katholischen Kirche. Besondere Bedeutung kommt dabei den Hilfestellungen in der Form von Orientierungshilfen zu. Hierbei ist vor allem auf die in letzter Zeit veröffentlichten Schriften „Videoüberwachung“ und „Datenschutz im Pfarrbüro“ hinzuweisen.

Für die Zukunft ist eine Veränderung der Seite „Veröffentlichungen“ geplant mit dem Ziel, ein schnelleres Auffinden benötigter Informationen zu ermöglichen. Es wird dann eine Darstellung in einer dreispaltigen tabellarischen Form geben. In der linken Spalte werden dann die Themen benannt, zu denen Informationen zur Verfügung gestellt werden, in der mittleren Spalte soll eine kurze Erläuterung hierzu gegeben werden und im rechten Teil sollen dann die Links zu dem aufgerufenen Thema erscheinen. Die derzeitige Gliederung nach den Namen der Stellen, die die Informationsbroschüren geschaffen haben, hat sich nach unserer Auffassung nicht bewährt, da zu gleichen Themen mehrere Schriften an verschiedenen Stellen zu finden sind.

Die Homepage ist weiterhin die Voraussetzung für die Mitgliedschaft im Virtuellen Datenschutzbüro der öffentlichen Datenschutzaufsichtsbehörden in Deutschland.

Die Homepage „Datenschutz in der Katholischen Kirche“
wird weiterhin im Blickpunkt der Arbeit stehen.

Sie soll alle Dienststellen und Einrichtungen
über die Aufgaben und Anforderungen kirchlichen Datenschutzes unterrichten.

Sie soll auch in die Öffentlichkeit hineinwirken.

4.2 Broschüren, Handreichungen

An neuen Handreichungen sind in dem Berichtszeitraum Folgende erschienen:

- Datenschutz in der kirchlichen Erwachsenbildung (Juni 2010)
- Auskunftsrechte ehemaliger Heimkinder (September 2010)
- Veröffentlichung personenbezogener Daten in Pfarrbriefen und auf den Internetseiten der Pfarrgemeinden (September 2010)
- Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internetangeboten (September 2010)
- Videoüberwachung – Eine Arbeitshilfe für kirchliche Einrichtungen (Juli 2012)
- Datenschutz im Pfarrbüro (Februar 2013)

Von der Deutschen Bischofskonferenz:

- „Social Media Guidelines" für kirchliche Mitarbeiter. Empfehlungen und Muster
- Ständige AG Datenschutz, Melderecht und IT-Recht sowie Ständige AG Urheberrecht der Rechtskommission des VDD: Nutzung sozialer Netzwerke (social networking) in Einrichtungen der katholischen Kirche

Von Datenschutzinstitutionen des Bundes und der Länder:

- Orientierungshilfe Cloud-Computing (AK Technik und Medien, September 2011)
- Datenschutz in Kindertageseinrichtungen (KuMi B-W, 2012)
- Orientierungshilfe „Soziale Netzwerke“ (Konferenz der DSB Bund und Länder, 2013)
- Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail (Bundesbeauftragter für den Datenschutz, März 2013)
- Orientierungshilfe Krankenhausinformationssysteme, 2. Fassung (AK Gesundheit und Soziales und AK Technische und organisatorische Datenschutzfragen, März 2014)

Damit stehen im Vergleich zum letzten Bericht eine Vielzahl neuer Handreichungen und Orientierungshilfen zur Verfügung.

Diese Broschüren sind vollständig auf der Webseite des Diözesandatenschutzbeauftragten zu finden und können kostenlos heruntergeladen werden.

4.3 Schulungen und Vorträge

Wie auch in den vergangenen Jahren ist der Diözesandatenschutzbeauftragte wieder häufig gebeten worden Vorträge vor Mitarbeitern, die in bestimmten Bereichen tätig sind, zu halten. Diese Aufgabe wird in aller Regel gerne wahrgenommen, weil sie es ermöglicht, jeweils eine größere Zahl von Mitarbeitern anzusprechen und hierdurch das Datenschutzbewusstsein im jeweiligen Arbeitsbereich zu vergrößern. Ganz besonders erfreulich sind dabei jene Veranstaltungen, in denen sich eine rege Diskussion mit den Teilnehmern ergibt.

Im zurückliegenden Zeitraum wurden zum Beispiel folgende Veranstaltungen durchgeführt:

- Datenschutz im Pfarrbüro (Pfarrsekretärinnenfortbildung, Kloster Nütschau am 16.04.2013)
- Datenschutz im Pfarrbüro (Pfarrsekretärinnen des Dekanats Unterelbe, Nütschau am 28.02.2013)
- Datenschutz Kindertagesstätten (Fachberaterinnen des CV Hildesheim am 07.03.2013)
- Datenschutz im Arbeitsrecht (DiAG MAV Osnabrück am 08.05.2012)

- Datenschutz für Mitarbeitervertreter (DiAG MAV Berlin am 26.05.2011)
- Datenschutz für Administratoren (St. Pius-Stift Cloppenburg am 13.10.2010)
- Datenschutz in der ambulanten Pflege (Ludgerus-Werk Lohne am 20.09.2010)

Eine Reihe von Vorträgem konnten infolge meiner Erkrankung nicht durchgeführt werden. Dabei ist es sogar in einem Fall passiert, dass der Termin nicht abgesagt werden konnte. Mir tut dies aufrichtig leid, aber es war nicht zu verhindern, da ich aus gesundheitlichen Gründen nicht hierzu imstande war und mir zu der Zeit ein Mitarbeiter oder eine Mitarbeiterin, die das hätten übernehmen können, nicht zur Verfügung stand.

5. Zusammenarbeit

5.1 Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands

Der Unterzeichner hat regelmäßig an den Sitzungen der Konferenz teilgenommen. Sie führt zwei Tagungen im Jahr durch. Folgende Bereiche wurden unter anderem in dieser Zeit behandelt:

- Erörterungen über die Änderungen in der neuen KDO
- Stellungnahme zur Änderung der „Archivordnung“
- Stellungnahme zum Forschungsvorhaben „Sexueller Missbrauch“ der KFN Hannover
- Möglichkeiten des Einsatzes von DeMail
- Datenträger- und Aktenentsorgung (mit Vorführung durch die Fa. Rhenus)
- Facebook, Informationen zu sozialen Netzten
- Einsatz von Google Analytics
- Stellungnahme zu einer geplanten „Richtlinie zum Einsatz von Arbeitsplatzcomputern“
- Stellungnahme zu einer geplanten „Fundraisingordnung“
- Anforderungen an eine datenschutzrechtlich sichere Online-Beratung
- Behandlung des erweiterten Führungszeugnis nach § 30a BZRG

Darüber hinaus wurde noch eine Fülle von Einzelthemen erörtert, die hier nicht alle aufgeführt werden können. 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.

Für die Zukunft sind etliche organisatorische Änderungen zu erwarten. Im Hinblick auf die neue KDO-2014 und die von ihr vorgenommene Stärkung der Arbeit der Diözesandatenschutzbeauftragten werden die Bistümer gravierende Änderungen vornehmen müssen. Das gilt insbesondere im Hinblick auf § 16 Abs. 2 Satz 4 KDO, nachdem anderweitige Tätigkeiten das Vertrauen in die Unabhängigkeit und Unparteilichkeit nicht gefährden dürfen. Die überwiegend bisher durchgeführte Kombination zwischen Datenschutz- und weiteren Tätigkeiten im Auftrag der Diözesen, dürfte dieser Vorgabe kaum noch entsprechen. Insoweit dürfte es künftig mehr hauptamtliche Datenschutzbeauftragte geben, die sich allein auf diesem Gebiet betätigen. Somit lässt sich eine Stärkung der „Professionalität“ der Datenschutzaufsicht erhoffen.

Ähnlich wie im Bereich der Datenschutzbeauftragten des Bundes und der Länder sollte daher nicht nur zwei Mal jährlich eine gemeinsame Konferenz stattfinden, sondern es sollten zu allen wichtigen Themen Arbeitskreise gebildet werden, die ihre besondere Fachkompetenz einbringen und ihre Ergebnisse den Diözesandatenschutzbeauftragten

zur Verfügung stellen. Mitglieder dieser Arbeitskreise sollten nicht allein Teilnehmer der Konferenz, sondern auch IT-Techniker und Fachleute aus den bestimmten Bereichen sein. So könnte beispielsweise ein „AK Archive“ auch einige Archivare mit einbeziehen, damit Ergebnisse entstehen, die auch praktisch umsetzbar sind. Die Arbeitsergebnisse dieser Arbeitskreise müssen jeweils von der Konferenz bestätigt werden.

5.2 IT-Workshop

Seit November 2012 findet im Niels-Stensen-Haus in Hannover ein interner IT-Workshop statt. Hierzu eingeladen werden die IT-Beauftragten der Bistümer, die Datenschutzreferenten und die betrieblichen Datenschutzbeauftragten der Generalvikariate bzw. Ordinariate. Gemeinsam erörtert werden Themen, die in allen Diözesen, dort meist in dringlicher Form, anstehen. Die Tagungsordnungspunkte werden dabei nicht vom Diözesandatenschutzbeauftragten vorgegeben, sondern in Abstimmung mit den Teilnehmern festgelegt.

Bisher waren vier Tagungen vereinbart, von denen eine jedoch nicht stattfinden konnte, da die Beschreibungen der Verfahren über die gesprochen werden sollte, nicht rechtzeitig fertiggestellt werden konnten. Die Sitzungen haben am 08.11.2012, 24.01.2013 (abgesagt), 11.06.2013 und 23.01.2014 stattgefunden. Das nächste Treffen ist für den 24.07.2014 geplant.

Die Zusammenkünfte haben sich durch Verstärkung der Zusammenarbeit und die Schaffung einheitlicher Haltungen zu wichtigen Fragen bisher bestens bewährt.

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

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

Ebenso ist der Diözesandatenschutzbeauftragte regelmäßig zu den Sitzungen der Referentenkonferenz für Datenschutz, Meldewesen und Kirchenmitgliedschaftsrecht im Landeskirchenamt in Hannover eingeladen worden und hat hier regelmäßig teilgenommen.

Durch die Neuordnung des Datenschutzes im Bereich der Evangelischen Kirche in Deutschland wird es künftig keine Sitzungen der Datenschutzbeauftragten in Berlin mehr geben. Stattdessen wird ein „Beauftragter für den Datenschutz der EKD“ die Aufsicht über die Datenverarbeitung in allen Landeskirchen, mit Ausnahme der Kirchen in Sachsen, Nordelbien, Anhalt, Braunschweig und der Pfalz übernehmen. Hierzu ist Herr Jacob ernannt worden. Welche Tagungen dann in Zukunft durchgeführt werden, ist noch offen.

Auf der letzten Konferenz der Datenschutzbeauftragten der EKD in Berlin am 8./9. Mai 2014 habe ich folgenden Vorschlag gemacht:

Die Datenschutzbeauftragten des Bundes und der Länder tagen zwei Mal jährlich zusammen. Sie haben darüber hinaus eine Reihe von Arbeitskreisen gebildet, die sich wichtigen Themen in bestimmten Fachgebieten annehmen und der Konferenz zuarbeiten. Die Erstellung von Orientierungshilfen ist dabei eine wichtige Aufgabe. Hierdurch wird Fachkompetenz gebündelt und allen Mitgliedern gemeinsam zur Verfügung gestellt. Solch eine Zusammenarbeit wäre auch im Rahmen einer „gelebten Ökumene“ für den kirchlichen Datenschutz wünschenswert. Die Bildung gemeinsamer Facharbeitskreise, die ihre Ergebnisse sowohl dem Datenschutzbeauftragten der EKD und den noch selbstständigen Landeskirchen, wie auch der Konferenz der Datenschutzbeauftragten der Bistümer in Deutschland vorstellen, wäre eine wesentliche Erleichterung für die Aufsichtsbehörden.

Kein Datenschutzbeauftragter ist perfekt!

Niemand kann alle Themen, wie beispielsweise
Pfarreien, Kindergärten, Schulen, Erwachsenenbildung, Seelsorge,
Krankenhäuser, Friedhöfe, Archive,
Soziale Dienste, ambulante oder stationäre Pflege, Kinder- und Jugendhilfe,
Behindertenhilfe, Arbeitshilfe und vieles andere mehr
vollständig überblicken!
Zumal die Rechtsvorschriften für alle Bereiche unterschiedlich sind.

Hinzu kommen noch Fragen aus dem Bereich der
Informations- und Kommunikationstechnik und der Medien.

Aber jeder hat Spezialgebiete!

Facharbeitskreise geben die Möglichkeit,

- das eigene Fachwissen weiterzugeben
- und gleichzeitig vom Fachwissen der Kollegen zu profitieren!

5.4 Zusammenarbeit mit den Datenschutzbeauftragten der Länder

Regelmäßige Kontaktgespräche mit Landesbeauftragten finden im Augenblick nur in Hamburg statt. Die bestehende Tradition solcher Gespräche mit den evangelischen und katholischen Datenschutzbeauftragten wird von Prof. Dr. Casper fortgeführt.

Ein weiterer und intensiver Kontakt zu den Landesbeauftragten ergibt sich daraus, dass sie jeweils zu den Sitzungen der Datenschutzbeauftragten der EKD und im Bereich der Katholischen Kirche eingeladen werden. Bei diesen Treffen werden wir über die Fragen und Probleme, die derzeit im Datenschutz des jeweiligen Landes eine wichtige Rolle spielen, informiert.

Die Zusammenarbeit in den Fällen, in denen staatliche und kirchliche Stellen betroffen sind, erfolgt schnell und im gemeinsamen Interesse nach vernünftigen, tragbaren Lösungen. Beschwerden, die bei den Landesbeauftragten eingereicht werden aber kirchliche Einrichtungen betreffen, werden mit kurzem Anschreiben an den Diözesandatenschutzbeauftragten zur Übernahme der Bearbeitung übersandt. Beide Seiten pflegen eine gute, sachlich fundierte Zusammenarbeit.

5.5 Projektpartnerschaft im Virtuellen Datenschutzbüro

Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer war auch während des Berichtszeitraums weiterhin Projektpartner des Virtuellen Datenschutzbüros, einer gemeinsamen Internetplattform der öffentlichen Datenschutzaufsichtsinstanzen. Er hat sich mit einem festen Betrag in Höhe von 500 € / Jahr an den Kosten des Betriebs der Seite http://www.datenschutz.de beteiligt, die sich insgesamt auf etwas mehr als 40.000,- € belaufen.

Da die Seite des Diözesandatenschutzbeauftragten noch immer den einzigen datenschutzrechtlichen Internetauftritt der Katholischen Kirche in Deutschland darstellt, ist die Mitgliedschaft auch weiterhin zur Darstellung des eigenen kirchlichen Anteils in diesem Bereich und zur aktiven Wahrnehmung ihres Selbstverwaltungsrechts auf diesem Gebiet erforderlich. Die Evangelische Kirche ist durch die EKD und den Datenschutzbeauftragten der ELK Württemberg dort vertreten.

An dem Angebot dieser Seite ist im Berichtszeitraum nicht sehr viel geändert worden. Das soll sich jedoch in naher Zukunft ändern. Dabei ist bisher geplant, ein neues Konzept zu erstellen. Hierüber wurde schon auf der letzten Sitzung, die Ende März in Hannover stattgefunden hat, ausgiebig diskutiert. Dabei standen vor allem die Ausrichtung der Seite auf den Informationsbedarf interessierter Bürger, die Aufrechterhaltung oder Deaktivierung des Artikelbereichs und die Einbeziehung der Kooperationspartner im Vordergrund. Damit alle Projektpartner, auch diejenigen, die nicht an der Sitzung teilnehmen konnten, sich an der Entscheidung beteiligen können, wird in

der Zeit bis zum 1. Juli d.J. ein formloses Widerspruchsverfahren per E-Mail durchgeführt. Ein positives Ergebnis vorausgesetzt, wird dann der Artikelbereich der Seite deaktiviert unter der Maßgabe, dass ein neues tragfähiges Konzept erstellt wird.

Die letzte Sitzung der Projektpartner fand zum ersten Mal nicht in Kiel, in den Räumen des Unabhängigen Landeszentrums für Datenschutz, sondern im Niels-Stensen-Haus in Hannover in einem der dort zur Verfügung stehenden Vortragsräume statt. Ganz sicherlich ein Zeichen dafür, dass auch die kirchliche Beteiligung am Projekt gern gesehen wird. Für den Januar 2015 ist erneut ein Treffen im Niels-Stensen-Haus vorgesehen.

6. Entwicklung der Dienststelle

Die Entwicklung der Dienststelle hat sich zum Abschluss des Berichtszeitraums in positiver Weise verändert.

6.1 Einstellung eines Verwaltungsmitarbeiters

Es wurde mit den Bistümern vereinbart, dem Diözesandatenschutzbeauftragten wieder einen halbtags beschäftigten Mitarbeiter zur Verfügung zu stellen. Nach Durchführung eines Bewerbungsverfahrens konnte Herr Walter für diese Aufgabe gewonnen werden. Er ist seit dem 1. März 2014 zunächst mit Zeitvertrag für ein Jahr angestellt worden. Hierdurch wird die im Anfang meiner Tätigkeit geübte Praxis der Inanspruchnahme einer Sekretärin, die wegen zeitweilig bestehender finanzieller Engpässe der Kirche ausgesetzt wurde, wieder aufgenommen.

Herr Walter wird in erster Linie die Organisation der Dienstelle übernehmen und somit den Unterzeichner von den notwendiger Weise zu erledigenden nicht juristischen Arbeiten entlasten. Hierdurch wird mehr Konzentration auf die datenschutzrechtlichen Fragestellungen möglich sein.

6.2 Beauftragung eines externen Technikers

Mit Schreiben vom 30.01.2014 hat mir der Generalvikar des Bistums Hildesheim mitgeteilt, dass nach Abstimmung aller beteiligten Diözesen nunmehr die Finanzierung einer externen technischen Unterstützung für die Aufgaben des Datenschutzbeauftragten erfolgen werde. Daraufhin wurde die Datenschutz Nord GmbH zur Übernahme dieser Aufgabe gewonnen, die mir zwischenzeitlich Herrn Dr. Sascha Todt als Ansprechpartner benannt hat.

In der seither vergangenen, kurzen Zeit sind bereits wichtige Beauftragungen an die Datenschutz Nord GmbH erfolgt. So soll in absehbarer Zeit die interne Cloud des Bistums Osnabrück für verschiedene Caritasberatungsstellen einer technischen Überprüfung unterzogen werden. Eingeschaltet wurde der externe Berater auch bei der Begleitung eines gemeinsamen Patientenaktenarchivs von zwei Krankenhäusern in Flensburg. Geplant ist ein Vortrag mit Vorlage eines Pflichtenhefts für den Einsatz von Mobile Device Management Systemen (MDM) auf dem nächsten IT-Workshop. Auch in einfachen, kleineren Fragen erhält der Diözesandatenschutzbeauftragte sehr schnell eine Reaktion auf technische Problemstellungen, die bei einer datenschutzgerechten Lösung zu beantworten sind.

Hierdurch wird die Schlagkraft des Datenschutzes wesentlich verbessert! Der Vorteil liegt auch auf Seiten der anfragenden Dienststellen, die künftig nicht mehr allein auf juristische Anforderungen reagieren müssen, sondern hierzu auch technisch einwandfrei umsetzbare Lösungen erhalten werden.

6.3 Änderung und Erweiterung der technischen Ausstattung der Dienststelle

Die Ausstattung der Datenverarbeitung wurde vollständig erneuert und teilweise auch erweitert. Angeschafft wurden:

- Zwei Arbeitsplatzcomputer mit dem Betriebssystem Windows 7 Ultimate.
- Eine neue Hardwarefirewall,
- Ein neuer All-in-One Office-Drucker
- Erweiterung durch einen NAS-Speicher
- Ein neuer WLAN-Router

Mit dem Bistum Hildesheim wurde abgesprochen, dass der alte PC, der noch unter Windows XP lief durch einen neuen ersetzt werden sollte. Für die Tätigkeit des Verwaltungsmitarbeiters wurde zudem ein zweiter PC angeschafft. Da beide Arbeitsplätze auf einen einheitlichen Datenbestand zugreifen müssen, wurde ein separates Speicherlaufwerk angeschafft, das zugleich auch eine gemeinsame Datennutzung bei der Verwendung von MS-Outlook (Kalender, Adressbuch, Aufgaben) ermöglicht.

Im Laufe der Arbeiten stellte sich ein technischer Defekt an der bis dahin vorhandenen Firewall heraus, so dass auch hier die Anschaffung eines Neugerätes erforderlich wurde.

Der bis dahin genutzte All-In-One Drucker konnte schon vor diesem Zeitpunkt nicht mehr Scannen und lieferte zudem nur unbrauchbare Kopien (in blassrosa). Eine technische Überprüfung des Geräts machte deutlich, dass die Scan-Funktion beschädigt war und eine Reparatur wegen der damit verbundenen Kosten im Verhältnis zu einer Neuanschaffung nicht lohnend sei. Auch hier wurde ein Neugerät installiert.

Der bisher benutze WLAN-Router entsprach nicht mehr den heute gegebenen technischen Voraussetzungen, da eine Absicherung des Zugangs nur in WPA, nicht aber in WPA-2 erfolgen konnte. Die erste Lösung ist in der Vergangenheit kompromittiert worden und bietet daher keine ausreichende Sicherheit mehr. WPA-2 ist der zurzeit gültige Standard. Dieser reicht nach der Rechtsprechung des Bundesgerichtshofs[32] aus, um eine Mithaftung des WLAN-Betreibers für Urheberrechtsverstöße eines unberechtigten Drittnutzers auszuschließen.

Zudem ist durch die Erneuerung des Routers nunmehr auch eine Verbesserung des Funknetzwerks erfolgt, so dass jetzt eine Übertragung mit der Schnelligkeit des IEEE 802.11ac Standards anstelle des alten IEEE 802.11g möglich geworden ist.

[32] BGH Urt. v. 12.05.2010 zu Az: I ZR 121/08

6.4 Renovierung der Dienststelle

Schließlich ist auch eine Gesamtrenovierung der Räume der Dienstelle erfolgt. Dabei wurden die Büroräume durch Streichen der Wände, Verlegung eines neuen Bodenbelags, Erneuerung und Veränderung der Fensterdekoration und dem Abriss eines brüchigen Wandregals mit einem Spülbecken und dem Ersatz durch einen neuen Unterschrank mit einer neuen Wasserstelle wieder in einen ordnungsgemäßen Zustand versetzt. Auch dies hat zu einer wesentlichen Verbesserung der Arbeitssituation beigetragen.

Schlussbemerkung:

Der Bericht gibt nur den wichtigsten 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 30.06.2014

Diözesandatenschutzbeauftragter

Das geltende Datenschutzrecht in den norddeutschen Diözesen

A. Erzbistum Berlin

- Anordnung über den kirchlichen Datenschutz (KDO) vom 01.03.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 01.10.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 03.01.2011
- Datenübermittlung im Zusammenhang mit den Fusionen der Kirchengemeinden vom 01.10.2003
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche (Kirchliche Archivordnung – KAO) vom 01.02.2014
- Benutzungsordnung für das Diözesanarchiv Berlin (BODAB) vom 01.02.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien vom 13.02.2008
- Ordnung zur Prävention sexualisierter Gewalt an Minderjährigen im Bereich des Erzbistums Berlin (Präventionsordnung) vom 01.04.2012

B. Erzbistum Hamburg

- Anordnung über den kirchlichen Datenschutz – KDO – vom 07.03.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 15.11.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 15.12.2010
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Erzbistum Hamburg vom 15.02.2009
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft vom 15.03.2005
- Sozialdatenschutz in der freien Jugendhilfe in der katholischen Kirche (Erläuterungen)
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück vom 01.04.1990
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück vom 01.09.1992
- Anordnung über die Sicherung und Nutzung der kirchlichen Archive im Erzbistum Hamburg (Kirchliche Archivanordnung – KAO) vom 18.03.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien 13.02.2008
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück vom 15.12.1995
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte Vom 17.01.1996
- Untersagung des Einsatzes von „Google Analytics“ vom 15.02.2010

- Einsatz von sog. „Like-Buttons“ auf kirchlichen Webseiten vom 15.01.2013
- Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen im Erzbistum Hamburg vom 30.09.2010

C. Bistum Hildesheim

- Anordnung über den kirchlichen Datenschutz – KDO – vom 01.03.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 31.10.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 01.11.2010
- Veröffentlichung von persönlichen Daten (z.B. Altersjubiläum) in Pfarrbriefen und ähnlichen Publikationen vom 24.01.1998
- Anordnung zum Schutz personenbezogener Daten bei der Durchführung von Fundraising-Maßnahmen im Bistum Hildesheim – FundrO – vom 31.03.2006
- Ordnung zur Regelung der Betreuungsverhältnisse in katholischen Tageseinrichtungen für Kinder im Bistum Hildesheim vom 01.08.2010
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Hildesheim vom 07.03.2008
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft vom 17.08.2004
- Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft (Erläuterungen)
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim vom 01.03.1990
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Hildesheim vom 01.12.1992
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche (Kirchliche Archivanordnung – KAO) vom 01.03.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien vom 13.02.2008
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Hildesheim vom 01.11.1994
- Besonderer Schutz von Computerprogrammen nach dem Urheberrechtsgesetz vom 01.11.1994
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte vom 01.11.1992
- Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen im Bistum Hildesheim vom 25.08.2010

D. Bistum Magdeburg

- Anordnung über den kirchlichen Datenschutz – KDO – vom 01.05.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 07.11.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 13.01.2011
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche

(Kirchliche Archivordnung – KAO) vom 10.01.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien vom 13.02.2008
- Ordnung zur Prävention von sexuellem Missbrauch an Minderjährigen (Präventionsordnung) vom 21.12.2011

E. Bistum Osnabrück

- Anordnung über den kirchlichen Datenschutz – KDO – vom 19.02.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 07.11.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 13.01.2011
- Pfarrbrief und Datenschutz vom 30.07.1999
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft in der Diözese Osnabrück vom 21.04.2008
- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft vom 16.11.2004
- Sozialdatenschutz in der freien Jugendhilfe in der katholischen Kirche (Erläuterungen)
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück vom 01.04.1990
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft in der Diözese Osnabrück vom 01.09.1992
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche (Kirchliche Archivanordnung – KAO) vom 20.03.2014
- Benutzungsordnung für die Archive in der Diözese Osnabrück vom 20.03.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien vom 13.02.2008
- Richtlinien zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück vom 27.07.1994
- Datenschutz bei der Übermittlung personenbezogener Daten über Telefaxgeräte vom 14.11.1991
- Gesetz zur Vermeidung von Kindeswohlgefährdungen im Umgang mit Kindern und Jugendlichen im Bistum Osnabrück vom 25.08.2010

F. Offizialat Vechta

- Anordnung über den kirchlichen Datenschutz – KDO – vom 15.04.2014
- Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) vom 15.12.2003
- Anordnung über das kirchliche Meldewesen – KMAO vom 15.12.2011
- Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft im Offizialatsbezirk Oldenburg vom 16.06.2011

- Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft vom 15.06.2004
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern im Offizialatsbezirk Oldenburg vom 01.04.1990
- Ordnung zum Schutz von personenbezogenen Daten bei Friedhöfen in kirchlicher Trägerschaft vom 15.12.1992
- Anordnung über die Sicherung und Nutzung der Archive der Katholischen Kirche (Kirchliche Archivordnung – KAO) vom 15.04.2014
- Grundsätze zur Nutzung gesperrten kirchlichen Schrift- und Dokumentationsgutes aufgrund von Sondergenehmigungen
- Empfehlung der Deutschen Bischofskonferenz zur Vervielfältigung von Pfarrmatrikeln und kirchlichen Archivalien vom 13.02.2008
- Richtlinien zum Einsatz von Arbeitsplatzcomputern im oldenburgischen Teil des Bistums Münster vom 15.11.1994
- Ordnung zur Prävention von sexuellem Missbrauch an Minderjährigen im Oldenburgischen Teil der Diözese Münster (Offizialatsbezirk Oldenburg) (Präventionsordnung) vom 30.09.2011

Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

– aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[1] der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

[1] http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

Sozialgesetzbuch X (Auszug)

§ 80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag

(1) Werden Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzbuches und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 82 bis 84 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Eine Auftragserteilung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 78a zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz von Sozialdaten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Die Auftragserteilung an eine nicht-öffentliche Stelle setzt außerdem voraus, dass der Auftragnehmer dem Auftraggeber schriftlich das Recht eingeräumt hat,

1. Auskünfte bei ihm einzuholen,
2. während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen und
3. geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen,

soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist.

(3) Der Auftraggeber hat seiner Aufsichtsbehörde rechtzeitig vor der Auftragserteilung

1. den Auftragnehmer, die bei diesem vorhandenen technischen und organisatorischen Maßnahmen und ergänzenden Weisungen nach Absatz 2 Satz 2 und 3,
2. die Art der Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden sollen, und den Kreis der Betroffenen,
3. die Aufgabe, zu deren Erfüllung die Erhebung, Verarbeitung oder Nutzung der Daten im Auftrag erfolgen soll, sowie
4. den Abschluss von etwaigen Unterauftragsverhältnissen

schriftlich anzuzeigen. Wenn der Auftragnehmer eine öffentliche Stelle ist, hat er auch schriftliche Anzeige

an seine Aufsichtsbehörde zu richten.

(4) Der Auftragnehmer darf die zur Datenverarbeitung überlassenen Sozialdaten nicht für andere Zwecke verarbeiten oder nutzen und nicht länger speichern, als der Auftraggeber schriftlich bestimmt.

(5) Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn

1. beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder
2. die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben.

(6) Ist der Auftragnehmer eine in § 35 des Ersten Buches genannte Stelle, gelten neben den §§ 85 und 85a nur § 4g Abs. 2, § 18 Abs. 2 und die §§ 24 bis 26 des Bundesdatenschutzgesetzes. Bei den in § 35 des Ersten Buches genannten Stellen, die nicht solche des Bundes sind, treten anstelle des Bundesbeauftragten für den Datenschutz insoweit die Landesbeauftragten für den Datenschutz. Ihre Aufgaben und Befugnisse richten sich nach dem jeweiligen Landesrecht. Ist der Auftragnehmer eine nicht-öffentliche Stelle, kontrolliert die Einhaltung der Absätze 1 bis 5 die nach Landesrecht zuständige Aufsichtsbehörde. Bei öffentlichen Stellen der Länder, die nicht Sozialversicherungsträger oder deren Verbände sind, gelten die landesrechtlichen Vorschriften über Verzeichnisse der eingesetzten Datenverarbeitungsanlagen und Dateien.

(7) Die Absätze 1, 2, 4 und 6 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann. Verträge über Wartungsarbeiten sind in diesem Falle rechtzeitig vor der Auftragserteilung der Aufsichtsbehörde mitzuteilen; sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten, ist der Vertrag unverzüglich mitzuteilen.