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

2. Jahresbericht

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

für die Zeit vom 01. März 2015 bis zum 31. Dezember 2015

Vorgelegt im Januar 2016

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/

Jahresbericht 1.3.2015 – 31.12.2015

des Datenschutzbeauftragten der norddeutschen Diözesen

Inhalt:

Anhang:

Vorwort

Der nachfolgende Tätigkeitsbericht schließt an den 1. Jahresbericht an, der für die Zeit vom 01.03.2014 bis zum 28.02.2015, vorgelegt wurde. Der Zeitraum für die Berichterstattung wurde hierbei um zwei Monate verkürzt. Der Grund hierfür besteht in der geplanten Neugliederung der kirchlichen Datenschutzaufsicht für die kommenden Jahre.

Es wird eine Trennung der Zuständigkeit in Bezug auf das Erzbistum Berlin und das Bistum Magdeburg erfolgen. Die genannten Diözesen werden stattdessen gemeinschaftlich mit den Bistümern Dresden-Meißen, Erfurt und Görlitz einen hauptamtlichen Diözesandatenschutzbeauftragten bestellen. Zwischenzeitlich ist hierfür Herr Matthias Ullrich ernannt worden.

Die Aufsicht über die Nordbistümer bezieht sich daher nur noch auf das Erzbistum Hamburg, die Bistümer Hildesheim und Osnabrück und das Offizialat Vechta. Auch hier wird wie bisher ein gemeinsamer Datenschutzbeauftragter beauftragt. Personell wird diese Aufgabe ab Januar 2016 von Herrn Andreas Mündelein mit Dienstsitz in Bremen wahrgenommen. Der bisherige Datenschutzbeauftragte hätte nicht mehr für die nach der KDO vorgesehene Mindestbeauftragungszeit von vier Jahren zur Verfügung gestanden. Allerdings wird er als fachlicher Mitarbeiter von Herrn Mündelein der Datenschutzaufsicht weiter zur Verfügung stehen.

Der Bericht bezieht sich also auf den Zeitraum bis zum Ende meiner Beauftragung und erläutert noch einmal die wesentlichen Themen des kirchlichen Datenschutzes während der letzten zehn Monate.

Ich darf mich an dieser Stelle bei allen Mitarbeitern und Dienststellen bedanken, die meine Arbeit und meine Bemühungen um die Verbreitung des Datenschutzgedankens in den zurückliegenden 24 Jahren begleitet und unterstützt haben. Das gilt vor allem für die Generalvikare, die auch schon lange vor dem Urteil des Europäischen Gerichtshofs, die Unabhängigkeit des Diözesandatenschutzbeauftragen im vollem Umfange respektiert und gewährleistet haben. Die Ausübung einer Fach- oder Rechtsaufsicht hat auch zuvor niemals stattgefunden. Die Finanzierung des notwendigen Sachbedarfs ist stets ohne Anfragen oder Nachfragen erfolgt, so dass einer eingehenden und verantwortungsvollen Arbeitsweise nichts entgegengestanden hat. Mein Dank gilt auch den Datenschutzreferenten, den Justiziaren, den betrieblichen Datenschutzbeauftragten und den IT-Technikern der Bistümer, mit denen jederzeit eine vertrauensvolle Zusammenarbeit möglich war.

Hannover, den 31.01.2016

Lutz Grammann
Diözesandatenschutzbeauftragter

1. Rechtsänderungen

1.1 Beratungen in der Europäischen Union

Nach Abschluss des Trilog-Verfahrens, bei dem das Parlament, der Rat und die Kommission über die unterschiedlichen Entwürfe zum Erlass einer Europäischen Datenschutz-Grundverordnung (EU-DSGVO) verhandelt haben, liegt nunmehr ein endgültiger Gesetzestext vor[1], dem das Parlament zugestimmt hat. Die Grundverordnung wird zwanzig Tage nach ihrer Verkündung im Amtsblatt der Europäischen Union in Kraft treten (Art. 91 Abs.1 EU-DSGVO). Nach Übersetzung in 22 Sprachen, wird dies voraussichtlich im Februar/März 2016 geschehen. Von diesem Zeitpunkt an, gibt es dann eine Übergangsfrist von zwei Jahren bis die Bestimmungen unmittelbare Geltung in allen Mitgliedsstaaten der Union erlangen (Art. 91 Abs. 2 EU-DSGVO).

Art. 85 EU-DSGVO enthält eine unmittelbare Regelung für die Einbeziehung der öffentlichen Religionsgesellschaften. Dort wird in Absatz 1 festgestellt, dass Kirchen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung eigene Vorschriften zum Datenschutz erlassen haben, diese weiter anwenden können, wenn sie mit den Vorschriften des europäischen Rechts in Übereinstimmung gebracht werden können. In Absatz 2 wird verlangt, dass die Kirchen sich einer unabhängigen Aufsicht zu unterstellen haben. Hierfür kann eine besondere (kircheneigene) Aufsicht eingerichtet werden, vorausgesetzt, dass diese die Bedingungen erfüllt, die in Kapitels VI der Verordnung niedergelegt sind.

> "2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1, shall be subject to the control of an independent supervisory authority which may be specific, provided that fulfils the conditions laid down in Chapter VI of this Regulation."

Im Erwägungsgrund Nr. 100 wird angegeben, dass die Aufsichtsbehörden in jedem Mitgliedsstaat dieselben Aufgaben und Befugnisse haben sollen. Der Verweis auf die Vorschriften des Kapitel VI der Verordnung bedeutet für die Kirchen, dass sie trotz aller Selbstständigkeit in gleicher Weise, wie staatliche Aufsichtsbehörden dafür sorgen sollen, dass das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 der Charta der Grundrechte der Europäischen Union gewährleistet wird. Dabei werden grundsätzlich drei Forderungen zu erfüllen sein:

1. Die Datenschutzaufsicht muss einen vorgezogenen Rechtsschutz ermöglichen. Dabei muss die Art und Weise der Datenverarbeitung und die Berechtigung zur Erhebung, Speicherung und Verarbeitung personenbezogener Daten fachlich korrekt geprüft werden, bevor der Betroffene gezwungen ist, den gerichtlichen Rechtsweg in Anspruch zu nehmen.

[1] Der Text ist in englischer Sprache auf der Seite http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf zu finden.

2. Die Datenschutzaufsicht muss unabhängig sein. Dabei sind auch die Entscheidungsgründe aus dem Urteil des Europäischen Gerichtshofs zu berücksichtigen. Eine nebenamtliche Aufgabenerfüllung erfüllt diese Voraussetzung nicht, da der Amtsinhaber auch andere wichtige Aufgaben wahrzunehmen hat, die ihn von der Datenschutzaufsicht abhalten oder die Wahrnehmung seiner Aufgabe verzögern kann.
3. Die Datenschutzaufsicht muss über die personelle, sachliche Ressourcen verfügen und die Befugnisse besitzen, die erforderlich sind um ein datenschutzwidriges Handeln zu unterbinden. Von ihr wird ein erhebliches Durchsetzungsvermögen verlangt werden, wenn es um die Verteidigung der Grundrechte der Betroffenen geht.

Durch ihre Selbstständigkeit übernimmt die Kirche daher eine große Verantwortung, durch eigenes Engagement und angemessene organisatorische Vorkehrungen dafür Sorge zu tragen, dass auch insoweit die Rechte der Menschen bei uns in guten Händen sind.

Es sind schon eine Reihe von Änderungen bei der kirchlichen Datenschutzaufsicht geplant und zum Teil auch bereits in Angriff genommen worden. So wird es in Zukunft keine nebenamtlichen Datenschutzbeauftragten in den Bistümern mehr geben. Hauptamtliche Kräfte werden sich umfassend dem Schutz der informationellen Selbstbestimmung der EU-Bürger im kirchlichen Bereich widmen. Mit § 17 KDO-2013 wurden schon die hierfür notwendigen rechtlichen Voraussetzungen geschaffen. Stichworte, wie „fehlende Weisungsungebundenheit“, „angemessene Personal- und Sachausstattung“, „eigener Haushalt“ und „oberste Dienst- und Aufsichtsbehörde“ dürfen hier als Beleg zur Erfüllung der Anforderungen der Rechtsprechung des EuGH[2] und aus Kapitel VI der EU-DSGVO gesehen werden.

Die Umsetzung dieser Bestimmung in die Praxis erfolgt jedoch sehr langsam. In der überwiegenden Zahl der Bistümer wurde bisher kein hauptamtlicher Diözesandatenschutzbeauftragter bestellt. Lediglich für die norddeutschen Diözesen, die auf diesem Gebiet schon seit 1992 die Vorreiterrolle übernommen haben ist dies durch Bestellung von Herrn Mündelein als Nachfolger des ebenfalls hauptamtlich tätig gewesenen Herrn Grammann bereits verwirklicht.

Die angemessene Personal- und Sachausstattung ist ein weiter wichtiges Thema. Der Datenschützer als Einzelkämpfer reicht heute nicht mehr aus.

- Seine Behörde sollte zumindest über einen Verwaltungsmitarbeiter verfügen. Es macht hinsichtlich der Aufgabenerfüllung keinen Sinn, wenn sich der Datenschutzbeauftragte auch noch um die Büroorganisation kümmern und jedwede Korrespondenz sowie von ihm verfasste Schriften und Arbeitshilfen selbst schreiben muss. Ein Amtsinhaber, der sich darüber Gedanken machen muss,

[2] Siehe EuGH Urteil vom 09.03.2010, Az.: C-518/07 zur Unabhängigkeit der Datenschutzaufsicht
http://www.datenschutz-kirche.de/sites/default/files/file/download/EuGH-Urteil_Unabhaengigkeit_DS-Aufsicht.pdf

wo, wie und zu welchem Preis er Farbpatronen für seinen Drucker bestellen sollte, ist nicht vollständig auf seine Aufgabe konzentriert!

- Weiterhin braucht der Datenschutzbeauftragte die Unterstützung eines EDV-Technikers sowohl bei Prüfungen, Beratungen von Dienststellen, wie auch bei der Abfassung von Arbeitshilfen. Die Ausführungen zur modernen Datenverarbeitung im globalen Bereich machen dies ebenso deutlich, wie die Ausführungen zur Durchführung einer Datenschutzprüfung nach dem Standard-Datenschutzmodell.
- Letztlich wird zu klären sein, ob neben dem Diözesandatenschutzbeauftragten auch noch ein fachlicher, juristisch geschulter Mitarbeiter notwendig ist. Um die Bedeutung dieser Frage einmal zu veranschaulichen, nehme ich auf die Ausführungen von Prof. Lüdemann und Daniel Wenzel in einem Aufsatz „Zur Funktionsfähigkeit der Datenschutzaufsicht in Deutschland“[3] Bezug. Danach sind bei den Landesbeauftragten in Norddeutschland zahlenmäßig folgende Mitarbeiter beschäftigt, die sich mit Datenschutzkontrolle befassen:

Landesbeauftragte	Bremen	Hamburg	Nieders.	Sa.-Anhalt	Schl.-Holst.
Vollzeitstellen	13,1	12,35	35,6	12,5	15

Natürlich ist anzuerkennen, dass diese viele Ämter zu kontrollieren haben, die im kirchlichen Bereich nicht vorhanden sind, wie Polizei- und Ordnungsbehörden, die gesamte Ministerialverwaltung, zum Beispiel Finanzämter und auch im privaten Bereich haben sie es mit Großunternehmen, wie Facebook, Google und anderen zu tun. Insoweit kann der Personalbedarf nicht mit kirchlichen Anforderungen verglichen werden. Aber wir sollten auch sehen, dass Kirche nicht nur aus Bistümern und Pfarrgemeinden besteht, sondern auch aus dem großen Bereich caritativer Aufgaben, aus Kindergärten, Schulen, Krankenhäusern, Friedhöfen und vielen anderen Aufgaben, die oft genug einer besonderen Vertraulichkeit nach Außen unterliegen. Die Bistümer müssen hier eine grundlegende Entscheidung treffen, die erkennen lässt, dass die Rechte der Betroffenen ausreichend wahrgenommen werden.

Diese Änderungen müssen spätestens in zwei Jahren abgeschlossen sein. Es ist damit zu rechnen, dass die EU-DSGVO im Frühjahr 2018 verbindliches Recht in den Mitgliedsstaaten darstellt, auf das sich auch die Betroffenen unmittelbar berufen und vor Gericht geltend machen können. Dann müssen unsere Datenschutzaufsichtsbehörden den Festlegungen in Kapitel VI EU-DSGVO entsprechen.

1.2 Inkrafttreten des neuen Bundesmeldegesetzes (BMG)

Am 01. November 2015 ist das neue Bundesmeldegesetz (BMG) in Kraft getreten, dass das bisherige Melderechtsrahmengesetz und die Meldegesetzte der Länder ablöst. Eine Reihe von Veränderungen geht damit einher.
Den Kirchen werden jetzt auch die Daten von Lebenspartnerschaften mitgeteilt. Da man auf Seiten des Gesetzgebers besorgt war, dass die Kenntnis dieser Daten zu

[3] Abgedruckt in der Zeitschrift „Recht der Datenverarbeitung“, Heft 6/2015, Seite 285 ff

arbeitsrechtlichen Problemen bei kirchlichen Beschäftigungsverhältnissen führen könnte, hat man nunmehr in § 42 Abs. 1 BMG eine zusätzliche Einschränkung für die Nutzung der Daten eingefügt, die „… zur Erfüllung ihrer Aufgaben, nicht jedoch zu arbeitsrechtlichen Zwecken…“ übermittelt werden. Eine Einschränkung auf Lebenspartnerschaften ist dabei nicht vorgenommen worden, so dass dieses Nutzungsverbot für die Daten aller Katholiken und ihrer Familienangehörigen gilt. In einem Bewerbungsverfahren darf also noch nicht einmal die Religionszugehörigkeit der Bewerber über das Meldewesen festgestellt oder überprüft werden. Insoweit wird auf die Stellungnahme des Kirchenrechtlichen Instituts der Evangelischen Kirche in Deutschland von Herrn Prof. Heinig vom 16.10.2015[4] Bezug genommen.

Es wurde wieder eine Mitwirkungspflicht des Vermieters bei der An- und Abmeldung eingeführt, mit der Begründung, dass Scheinanmeldungen verhindert werden sollen. Der Wohnungsgeber hat nach § 19 Abs. 1 S. 2 BMG dem Mieter den Ein- oder Auszug schriftlich zu bestätigen. Nach Satz 3 kann er durch Rückfrage bei der Meldebehörde feststellen, ob der Mieter seiner Meldepflicht nachgekommen ist. In Abs. 3 sind die Daten festgelegt worden, die bei der Bestätigung anzugeben sind: Name und Anschrift des Wohnungsgebers, Art des meldepflichtigen Vorgangs mit Ein- oder Auszugsdatum, Anschrift der Wohnung sowie die Namen der meldepflichtigen Personen. Auch kirchliche Einrichtungen, die Wohnraum dauerhaft zur Verfügung stellen, haben diese Verpflichtungen zu erfüllen.

Die besondere Meldepflicht in Beherbergungsstätten nach § 29 Abs. 2, 3 BMG für Personen, die länger als 6 Monate aufgenommen werden, gelten nicht für Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften (§29 Abs. 5 Nr. 4 BMG). Das dürfte vor allem für Priesterseminare gelten.

Meldescheine für Beherbergungsstätten sind nach § 30 BMG weiterhin erforderlich. Sie wurden entgegen ursprünglicher Planungen nicht abgeschafft. Der Leiter muss sie ein Jahr lang aufbewahren und auf Verlangen, den nach Landesrecht zu bestimmenden Behörden vorlegen.

Das neue Bundesmeldegesetz ist von vielen Aufsichtsbehörden als wenig datenschutzgerecht kritisiert worden. Als Beispiel sei hier die Pressemitteilung des Berliner Datenschutzbeauftragten[5] vom 2. November 2015 angeführt, die im Anhang beigefügt ist.

1.3 Neue Durchführungsverordnung zur KDO

Die Rechtskommission des Verbandes der Diözesen Deutschlands hat in ihrer Sitzung vom 19.03.2015 eine neue Verordnung zur Durchführung der Anordnung über den kirchlichen Datenschutz (KDO-DVO) beschlossen, die von den Diözesen in Kraft ge-

[4] Schriftliche Stellungnahme des Kirchenrechtlichen Instituts der Evangelischen Kirche in Deutschland, Prof. Dr. Michael Heinig zur „Änderung des Bundesmeldegesetzes - § 42 Abs. 1 S. 1“ vom 16. Oktober 2015
[5] Pressemeldung des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 02.11.2015 zum Thema „Datenschutzrechtliche Hinweise zum neuen Melderecht“

setzt worden ist. Im Bistum Magdeburg ist dies mit Verkündung im kirchlichen Amtsblatt vom 01.07.2015, im Erzbistum Berlin im Amtsblatt vom 01.08.2015, im Bistum Hildesheim im Amtsblatt vom 25.09.2015, im Bistum Osnabrück im Amtsblatt vom 16.10.2015, im Erzbistum Hamburg im Amtsblatt vom 20.10.2015 und im Offizialat Vechta im Amtsblatt vom 01.12.2015 geschehen.

Gegenüber der früheren Verordnung von 2003 ist eine wesentliche Erweiterung vorgenommen worden. So sind für die Durchführung der erforderlichen technisch-organisatorischen Maßnahmen nach § 6 KDO unter Nr. IV der Durchführungsanordnung nunmehr zwei Anlagen beigefügt. In der Anlage 1 werden, wie bisher acht Anforderungen genannt, die von einer datenschutzgerechten Verarbeitung zu erfüllen sind. In der Anlage 2 sind nunmehr weitere Maßnahmen für Arbeitsplatzcomputer und Datenverarbeitungsanlagen benannt, die noch um eine IT-Richtlinie ergänzt wird, die einen Mindeststandard für alle dienstlich eingesetzten Arbeitsplatzcomputer und Datenverarbeitungsanlagen vorschreibt. Dabei wurden in vielen Punkten, die Bestimmungen aus der „Richtlinie zum Einsatz von Arbeitsplatzcomputern“ (APC-Richtlinie), die bereits seit 1994 übereinstimmend in den norddeutschen Bistümern (Erzbistum Hamburg, Bistum Hildesheim, Bistum Osnabrück, Offizialat Vechta) erlassen worden ist, übernommen. Mit Verkündung der neuen Anordnung in diesen Bistümern, ist daher gleichzeitig auch die APC-Richtlinie aufgehoben worden.

Neu ist, dass die IT-Richtlinie nicht nur für die Verarbeitung personenbezogener Daten gilt, sondern auch auf schützenswerte nicht personenbezogene Daten anzuwenden ist. Als Beispiele werden hier Buchhaltungs- und Kirchensteuerdaten genannt[6].

Alle verarbeiteten Daten sind nach ihrem Gefährdungsgrad in drei Schutzklassen einzuteilen, zu deren Schutz bestimmte Mindestmaßnahmen durchzuführen sind[7]. Bestimmte Daten, die dem Beicht- oder Seelsorgegeheimnis oder dem Adoptionsgeheimnis unterliegen, dürfen jedoch gar nicht elektronisch verarbeitet werden[8]. Mit dem Begriff Seelsorge kann hier nur die Ausübung eines Amtes gemeint sein, dessen Übertragung allein auf Priester erfolgen darf (Can. 150 CIC), die cura pastoralis. Insoweit gehe ich von einer inhaltlichen Gleichheit mit dem Zeugnisverweigerungsrecht des § 53 Abs. 1 der Strafprozessordnung (StPO) aus. Informationen, die nicht vor einem Gericht bekannt gegeben werden müssen, dürfen auch nicht durch Datenverarbeitung ausforschbar sein.

Die Nutzung privater Datenverarbeitungsanlagen zu dienstlichen Zwecken ist grundsätzlich unzulässig[9]. Unter bestimmten Voraussetzungen kann jedoch der Dienstellenleiter eine Ausnahme genehmigen. In den Nordbistümern ist eine solche Ausnahme für Lehrer an Schulen durch § 7 der Anordnung zum Schutz personenbezogener Daten in katholischen Schulen in freier Trägerschaft ausdrücklich geregelt.

[6] Siehe: Präambel zu Anlage 3 zu Abschnitt IV KDO-DVO (Anlage 2 zu § 6 KDO): „IT-Richtlinien“
[7] Siehe: Ziffer 2.1 – 2.3 der Anlage 3 zu Abschnitt IV KDO-DVO (Anlage 2 zu § 6 KDO): „IT-Richtlinien“
[8] Nr. 4.4 der Anlage 2
[9] Nr. 5.1 der Anlage 2

Darüber hinaus werden Maßnahmen für eine Reihe besonderer Gefahrenlagen, wie Fernwartung, Auftragsdatenverarbeitung, Wartungsarbeiten durch externe Auftragnehmer sowie die Verschrottung und Vernichtung von Datenträgern vorgegeben[10].

Viele Einrichtungen, vor allem aus dem karitativen Bereich erstellen Lastenhefte für ihre IT-Systeme. Dabei stellt sich natürlich auch die Frage, welche Vorschriften zur technischen Organisation anzuwenden sind. § 6 KDO gibt die Einhaltung der Vorschriften der KDO als Organisationsziel an, das durch die Anlage hierzu um acht Unterpunkte konkretisiert wird. Die jetzt neu geschaffene, zweite Anlage zu § 6 KDO (IT-Richtlinie) schafft hier eine wesentliche Erweiterung in der Form, dass die verarbeitenden Daten in verschiedene Schutzklassen eingeordnet werden und sich die zu treffenden Maßnahmen hieran ausrichten. Aus der praktischen Arbeit mit Mitarbeitern, die derartige Lastenhefte zu erstellen haben wird deutlich, wie sehr die Schaffung der IT-Richtlinie begrüßt wird.

Jedoch dürfen auch die Kritikpunkte an der neuen Ausführungsvorschrift nicht verschwiegen werden. Die weitgehende Übernahme der APC-Richtlinie, die schon zwanzig Jahre alt war, wirft eine Fülle von Fragen auf.

Datenverarbeitung ist heute nicht mehr mit der vor zwanzig Jahren zu vergleichen. Sie hat sich von einer statischen, allein auf den jeweiligen Arbeitsplatz oder die Einrichtung bezogenen Verfahrensweise, zu einer globalen, dynamischen Technik entwickelt, bei der sowohl die gespeicherten Daten wie auch die anzuwendenden Programme auf fremden Servern kostenlos oder gegen Gebühr zur Verfügung gestellt werden und somit weltweit verfügbar sind. Die Vorteile dieser Technik liegen auf der Hand: Einheitlichkeit des Datenbestandes, Verfügbarkeit auch außerhalb der Dienststelle, gemeinsame Bearbeitungsmöglichkeit durch verschiedene Mitarbeiter und geringerer technischer Aufwand. Notwendig hierfür sind die Nutzung von Cloud-Systemen und die Einbeziehung mobiler Endgeräte. Die Gefahren für den Bestand und die Vertraulichkeit der Daten wird auf diese Weise erheblich größer. Gerade mobile Endgeräte sind durch eine große Zahl ihrer Funktionen, aber auch durch den Gebrauch sogenannter „Mobile Apps“ zunehmenden Risiken ausgesetzt[11]. Für den Datenschutz muss es also darum gehen, die weltweit verfügbaren Daten abzuschotten, damit nur berechtigte Personen auf sie Zugriff nehmen können und sie gleichzeitig vor den kriminellen Aktivitäten von Hackern geschützt sind. Wichtige und notwendige Themen, wie „Cloud-Computing“, „Ende-zu-Ende-Verschlüsselung“, „Mobile Device Management“ sind nur unzureichend oder gar nicht angesprochen. Der Diözesandatenschutzbeauftragte hat im Dezember hierüber einen Vortrag auf der Geschäftsführerkonferenz beim Caritasverband Hildesheim gehalten, dessen Konzept im Anhang dieses Berichts beigefügt ist. Hier sind die fehlenden Regelungspunkte deutlich benannt worden.

[10] Ziffer 4.1 bis 4.7 der Anlage 3 zu Abschnitt IV. KDO-DVO (Anlage 2 zu § 6 KDO). IT-Richtlinien
[11] siehe den Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über „Die Lage der IT-Sicherheit in Deutschland 2015“

Zudem enthält die KDO-DVO Bestimmungen, die heute kaum noch einzuhalten sind. Das gilt beispielsweise für die Festlegung in Ziffer 3.4 der Anlage 2. Unter dem dritten Spiegelstrich wird im zweiten Satz bestimmt: „Die Benutzung privater Programme ist unzulässig." Wie soll das geschehen, wo viele Anbieter mobiler Endgeräte sich mit der Zahl fest eingebauter Apps brüsten? Solche Programme zu entfernen kann nicht vom Anwender geleistet werden, sondern nur von einem informierten Techniker, der in der Lage ist, die Festlegungen des Betriebssystems zu verändern.

Auch unter Ziffer 3.1 der IT-Richtlinie wird das Anlegen von Sicherungskopien der Originaldatenträger der eingesetzten Software-Programme verlangt, obwohl diese heute meistens nicht mehr auf CDs geliefert werden, sondern vom Hersteller unter Angabe der Lizenznummer heruntergeladen werden. Zudem werden diese Programme inzwischen so oft aktualisiert, dass eine Kopie der Originaldatenträger im Hinblick hierauf kaum noch Sinn macht.

> Es ist daher dem Verband der Diözesen Deutschlands zu empfehlen,
> die KDO-DVO noch einmal wesentlich zu überarbeiten.
> Dabei sollte das von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder entwickelte „Standard-Datenschutzmodell (SDM) inhaltlich übernommen werden. Das gilt für die Formulierung der Gewährleistungsziele wie auch für die Maßnahmen zu ihrer Umsetzung.

Das neue Standard-Datenschutzmodell ist im Oktober 2015 von den Mitgliedern der Konferenz angenommen und sodann veröffentlicht worden. Im nächsten Kapitel wird es im Einzelnen vorgestellt.

2. Informations- und Kommunikationstechnik

2.1 Das neue Standard-Datenschutzmodell (SDM)

Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben ein 40 Seiten umfassendes Handbuch zum „Standard-Datenschutzmodell (SDM)“ veröffentlicht[12]. Der Grund dafür war, dass das Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in erster Linie auf die Sicherung technischer Prozesse ausgerichtet ist und somit die Verwaltungsorganisation der betreffenden Einrichtungen schützen will. Der Datenschutz spielt dabei eine eher untergeordnete Rolle. In diesem Werk geht es allein um den Grundrechtsschutz der Menschen, deren Daten durch Organisationen verarbeitet werden[13].

Die gedankliche Vorgehensweise ist dabei gut nachzuvollziehen. Zunächst werden insgesamt sieben Schutzziele benannt, die sich aus den bestehenden Datenschutzregelungen des Bundes, der Länder und auch der Kirchen ergeben. Sodann wird unter Zugrundelegung dieser Anforderungen der Schutzbedarf ermittelt. Hierbei werden, wie auch in der KDO-DVO, drei Schutzbedarfsabstufungen (Datenschutzklassen) zugrunde gelegt. Unter ihrer Berücksichtigung sollen dann die notwendigen Schutzmaßnahmen entwickelt werden.

In der Anlage zu dieser Schrift ist das Grundkonzept am Beispiel der Durchführung einer Datenschutzprüfung dargestellt. Dort sind auch die zu verwirklichenden Schutzziele benannt. Nach dem gleichen Muster ließe sich auch ein Anforderungskatalog für eine verbesserte KDO-DVO entwickeln. Dieser könnte wie folgt aussehen:

- Notwendigkeit der Dokumentation der Rechtsgrundlagen auf die die Datenverarbeitung gestützt wird.
- Verpflichtung zur schriftlichen Dokumentation der Datenbestände und der für ihre Verarbeitung eingesetzten Hard- und Software.
- Verpflichtung zur Erreichung der sieben Schutzziele unter Berücksichtigung der Datenschutzklassen I bis III.
- Des Weiteren können Standard-Schutzmaßnahmen vorgegeben werden. Hier bieten sich die Notwendigkeit zur Verschlüsselung bei der Speicherung und Übertragung der Daten, der Einsatz von MDM-Programmen (Mobile Device Management) für den Anschluss mobiler Endgeräte und die Verpflichtung Sicherheitsupdates automatisch durchführen zu lassen oder zeitnah selbst vorzunehmen an.
- Erstellung eines Sicherheitskonzepts unter Einbeziehung der Mitarbeiter[14].

[12] Siehe hierzu den Bericht von Martin Rost, „Erweiterte Schutzziele“ in der Zeitschrift c‘t Heft 2/2016, Seite 138 f
[13] Veröffentlicht auf der Webseite des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf
[14] Die Notwendigkeit hierzu ist im Bericht des BSI (siehe Ziff. 11) auf den Seiten 22, 23 nachzulesen.

2.2 Anforderungen an Webauftritte nach dem Telemediengesetz (TMG)

Schwierigkeiten bereitet vielen Dienststellen, die Erfüllung der Anforderungen, die zur Kennzeichnung eines Webauftritts nach §§ 5, 6 TMG (Impressum) und § 13 TMG (Datenschutzerklärung) erforderlich sind. Der Datenschutzbeauftragte wurde daher vor allem auf eine Stellungnahme zur Fassung von Datenschutzerklärungen gebeten.

In einem Falle wurde auf die Notwendigkeit hingewiesen, den Einsatz sogenannter „Cookies“ auf der Webseite anzugeben. Hierbei muss die Dauer der Gültigkeit und der Speicherung ebenso angegeben werden, wie der Zweck zu dem die dabei ermittelten Informationen genutzt werden. Notwendig ist auch, dass bei Anbahnung vertraglicher Beziehungen, wie Bestellungen oder Buchungen für die Teilnahme an Veranstaltungen, zunächst die Datenschutzerklärung eingeblendet wird, bevor der Nutzer zum auszufüllenden Formular weitergeleitet wird. Erst dann, wenn er der Erhebung und Nutzung seiner personenbezogenen Daten zugestimmt hat, können die notwendigen Daten abgefragt werden. Bei der Angabe von Kreditkartendaten ist dabei eine sichere Webseite zu benutzen, die den Kunden vor Ausspähungen bewahrt.

2.3 Können Daten, die der Schweigepflicht nach § 203 StGB unterliegen auf fremden Servern verarbeitet werden?

Die Frage stellt sich vor allem in den caritativen Bereichen der Ehe-, Familien-, Erziehungs- oder Jugendberatung sowie für die Beratungen in Suchtfragen und in einer anerkannten Beratungsstelle nach dem Schwangerschaftskonfliktgesetz, die jeweils nach § 203 Abs. 1, Nr. 4, 4a StGB schweigepflichtig sind. Darüber hinaus werden auch staatlich anerkannte Sozialarbeiter und Sozialpädagogen durch § 203 Abs. 1, Nr. 5 StGB erfasst. Diese Verpflichtung erstreckt sich nach Absatz 3 der Vorschrift auch auf die bei diesen Stellen tätigen berufsmäßigen Gehilfen.

Verschwiegenheitspflicht bedeutet hierbei, dass der persönliche Lebens- und Geheimbereich der Betroffenen gerade von solchen Trägern sozial bedeutsamer Berufe geschützt wird, bei denen der Einzelne sich weitgehend anvertrauen muss. Die Verpflichtung gilt gegenüber jedermann, es sei denn, dass ein Gesetz ausdrücklich in bestimmten Fällen Ausnahmen zulässt. Es ist strafrechtlicherseits allgemein anerkannt, dass diese Verpflichtung auch gegenüber anderen Berufsangehörigen besteht und selbstverständlich auch gegenüber den Mitarbeitern bei der technischen Betreuung der Datenverarbeitung. Eine sichere Verschlüsselung der Daten, sowohl bei ihrer Speicherung, wie auch beim Transport vom Arbeitsplatzcomputer zum Server ist hier notwendige Pflicht! Dabei müssen die Daten schon auf dem Rechner des Anwenders verschlüsselt werden, bevor sie den Rechner verlassen (Ende-zu-Ende-Verschlüsselung). Es bleibt aber das Problem, dass bei technischen Wartungsarbeiten unverschlüsselte Daten benötigt werden und der Anbieter daher auch über den Key zur Entschlüsselung verfügen muss. Darüber hinaus werden beim Versand der Dateien weitere Daten übertragen, zum Beispiel wer mit wem kommuniziert (sog. „Metadaten“). Auch diese Daten geben oftmals Aufschlüsse über Geschäftsbeziehungen, die ebenfalls der Verschwie-

genheitspflicht unterliegen, ohne geschützt zu sein. Die Verschlüsselung des Filesystems ist daher ein notwendiger aber noch kein hinreichender Schritt zur Verhinderung der Einsichtnahme durch Unbefugte.

Verschlüsselungsexperten des Fraunhofer-Instituts haben hierfür eine Technologie entwickelt, die zugleich auf Verschlüsselung und Versiegelung der gespeicherten Daten beruht. Gleichzeitig wird eine logische Entkoppelung der Verkehrsströme durchgeführt. Diese als „Sealed Cloud" bezeichnete Technik schützt daher die Inhalte und die Metadaten. Zur Verfügung gestellt wird dieses Verfahren zurzeit nur von der Firma Uniscon in München durch das Programm iDGARD. Die TÜV Informationstechnik GmbH – Prüfstelle für Datenschutz – in Essen hat eine Vorbewertung der Version 5.2 auf die Entsprechung zum „Trusted Cloud Datenschutz Profil Vers. 0.9" vorgenommen.

Darin wird festgestellt:

> „Damit entspricht der Dienst den gesetzlichen Anforderungen an die Datenverarbeitung im Auftrag i.S.d. § 11 BDSG, wie sie im TCDP, Version 0.9, konkretisiert wurden.
>
> Der Schutz der Daten vor Verletzung der Vertraulichkeit und der Integrität entspricht der
>
> TCDP-Schutzklasse III.
>
> Der Schutz der Verfügbarkeit entspricht der
>
> TCDP-Schutzklasse II.
>
> Der Dienst iDGARD kann demnach für Daten mit dem Schutzbedarf I, II und III gemäß der Schutzbedarfsklassenbildung aus dem Arbeitspapier *Schutzklassen in der Datenschutz-Zertifizierung 1* des Pilotprojekts Datenschutz-Zertifizierung von Cloud- Diensten des BMWi genutzt werden."

Über die Handhabung des Programms im Einzelnen wurde auf der Webseite unter der Meldung „Einsatz eines Cloud-Dienstes für Berufsgeheimnisträger" vom 16.06.2015 berichtet. Die Vorbewertung der Prüfstelle vom TÜV Essen kann ebenfalls auf der Webseite eingesehen werden[15].

2.4 Die Web-Anwendung „ownCloud" als Kirchencloud?

Die amerikanische Firma ownCloud Inc. vertreibt eine Open Source Anwendung, die es ermöglicht, Daten zu verwalten, synchronisieren und zu teilen werden, wo immer sie gespeichert sind. Aktuell wird die Software in der Version 8.2 als Server oder Enterprise Edition (20.01.2016) angeboten. Eine erweiterte Version 9.0 ist in Vorbereitung.

Die Wirtschaftsgesellschaft der Kirchen in Deutschland (WGKD) hat mittlerweile einen Rahmenvertrag zur Nutzung dieser Anwendung abgeschlossen. Praktisch wird sie im Bereich der Evangelischen Kirche eingesetzt, wobei die KIGST GmbH für ihre Kunden

[15] Eintrag unter: http://www.datenschutz-kirche.de/sites/default/files/file/download/TUEV-IT%20TCDP%20Bewertung%20IDGARD%20v1-0.pdf

eine eigene ownCloud-Umgebung eingerichtet hat. Aber auch im Bereich der katholischen Kirche gibt es hiermit erste Versuche. So testet das Bistum Osnabrück, in Zusammenarbeit mit dem Rechenzentrum der ITEBO GmbH, augenblicklich die Nutzung dieses Verfahrens in zwei Kirchengemeinden.

In der kirchlichen Arbeitsstruktur sind vielfach nebenamtliche und hauptamtliche Mitarbeiter tätig, die aus organisatorischen Gründen oftmals gezwungen sind, ihre Anwendungsgeräte auch außerhalb eines festen Arbeitsplatzes einzusetzen. Hierbei werden vielfach mobile Geräte eingesetzt oder auf Computer zurückgegriffen, die im häuslichen Bereich installiert sind. Das schafft eine Reihe von Problemen für die Zusammenarbeit untereinander aber auch für die Sicherheit der Daten mit teilweise sensiblem Inhalt. Als Lösung dieses Problems wird es häufig angesehen, die Daten in einem gemeinsamen Verfahren zu verwalten. Hierbei müssen aus datenschutzrechtlicher Sicht jedoch folgende Anforderungen erfüllt sein:

1. Die Daten müssen vor dem Zugriff unberechtigter Personen geschützt sein. Es muss de facto eine sichere Abschottung gegenüber Nicht-Mitarbeitern erfolgen.
2. Auch die berechtigten Personen dürfen nur auf die Daten Zugriff nehmen, die zur Erledigung ihrer Arbeit benötigt werden.
3. Es muss sichergestellt sein, dass alle Beteiligten nur die Daten erheben, verarbeiten oder nutzen, die auf Grund einer Rechtsvorschrift oder die Einwilligung des Betroffenen verarbeitet werden dürfen (§§ 3 Abs. 1, 4 KDO). Das Datengeheimnis muss gewahrt werden, wobei naheliegender Weise eine arbeitsrechtliche Kontrolle hierauf wesentlich erschwert wird.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Berichtsjahr eine eingehende Analyse zur Verwendung des Systems für IT-Verantwortliche erstellt[16]. Dabei ist unter Berücksichtigung der dort gegebenen Hinweise ein sicherer Betrieb für normalen Schutzbedarf zu erreichen. Die Absicherung eines höheren Schutzbedarfs wird, soweit als möglich mit aufgezeigt. Maßnahmen zur Sicherheit der verarbeiteten Daten für einen sehr hohen Schutzbedarf sind nicht enthalten.

ownCloud lässt sich sowohl auf einem eigenen Server, wie auch auf einem Cloud-Server betreiben. Für kirchliche Dienststellen ist angesichts der notwendigen Maßnahmen ein Betrieb auf einem kircheneigenen Cloud-System meist die bessere Lösung, wenn die Übertragung der Daten dorthin eingehend gesichert werden kann. Die Erfahrungen hiermit sollten auch vom Datenschutz eingehend mitverfolgt werden.

[16] BSI: Betrieb und Sicherheit von ownCloud, Bonn 2015, 29 Seiten (Online-Einführung hierzu)

3. Datenschutz in kirchlichen Einrichtungen

3.1 Nachbericht zum Jahresbericht 1: Videoüberwachung

Im 1. Jahresbericht hatte der Unterzeichner über die Beanstandung einer Videoinstallation in einer Kirche in Hannover berichtet, weil sie den gesamten Innenraum erfasste und den Besuchern keine Möglichkeit gewährte, sich unbeobachtet und unkontrolliert in der Kirche aufzuhalten. Der Diözesandatenschutzbeauftragte hatte hierin eine massive Störung des Persönlichkeitsrechts und der individuellen Glaubensfreiheit der Betroffenen gesehen. Daraufhin hatte ein Gespräch mit den Beteiligten im Bischöflichen Generalvikariat stattgefunden, in dem die Beanstandung akzeptiert wurde, gleichzeitig aber vereinbart wurde, dass ein neue Planung der Videoüberwachung durchgeführt und vom Diözesandatenschutzbeauftragten einer Vorabkontrolle nach § 3 Abs. 5 KDO unterzogen werden solle. Dieses Verfahren wurde inzwischen eingeleitet.

Bei einem ersten Gespräch mit einer anschließenden Begehung des Kirchenraumes wurde Einigkeit unter den Beteiligten darüber erzielt, dass nur der Altarraum einer Überwachung ausgesetzt werden soll. Dieser Raum darf von Besuchern nicht betreten werden, und ist daher mit einer Kordel abzusperren, an der ein Schild anzubringen ist, dass das Betreten untersagt und darauf hinweist, dass dieser Teil videoüberwacht wird. Damit sind der Tabernakel mit dem eucharistischen Leib Christi sowie einige weitere Kunstgegenstände, insbesondere die sechs Silberleuchter gesichert.

Weiterhin wurde Einigkeit darüber erzielt, dass eine Überwachung der Opferstöcke nicht stattfinden soll, weil diese durch mechanische Wegnahmesperren gesichert werden können und ein Eingriff in das Persönlichkeitsrecht der Betroffenen daher nicht erforderlich ist. Auch eine Videoüberwachung des Marien-Altars soll nicht stattfinden, da bezüglich des Aufstellens von Kerzen (Teelichter) keine Brandgefahr gegeben ist. Das ungeeignete Abstellen der Lichter auf dem Fußboden kann durch eine mengenmäßige Begrenzung des Kerzenangebotes auf die Zahl der zur Verfügung stehenden ordnungsgemäßen Aufstellplätze erreicht werden.

Auf diese Weise könnte ein rechtmäßiges Verfahren durchgeführt werden, dass eine Öffnung der Kirche tagsüber, außerhalb von Gottesdiensten, ermöglichen würde.

Überraschend ist dann mit Mail-Brief des Referenten vom 3. Dezember 2015 mitgeteilt worden, dass der Ausschuss der Basilika auf seiner Sitzung am 30.11.2015 den Beschluss gefasst hat, den Maßnahmen, wie diese in meinem Aktenvermerk vom 09.09.2015 festgehalten worden sind, in Gänze nicht zuzustimmen und die Kirche weiterhin geschlossen zu halten. Eventuell werde die Beratung in 2016 wieder aufgenommen.

Der Diözesandatenschutzbeauftragte hat die Problematik der Videoüberwachung innerhalb eines Gotteshauses in einem Themenbeitrag vom 31.07.2015 auf der Webseite noch einmal grundlegend dargestellt.

3.2 Outsourcing des EBIS-Programms auf einen Server der GSDA GmbH

Der Caritas-Verband Berlin fragte an, ob eine Verwaltung von Daten der Sucht- und Schwangerschaftsberatung mit Hilfe des EBIS-Systems auf einen Rechner der Firma GSDA GmbH mit Sitz in München durchgeführt werden könne. Alle hierzu wichtigen Unterlagen wurden dem Datenschutzbeauftragten vorgelegt. Hierzu gehörten ein „Outsourcing-Vertrag“ nebst den Anhängen über den Wartungsvertrag und die Bedingungen für die Nutzung des SMS-Moduls. Auch die Allgemeinen Geschäftsbedingungen der Auftragnehmerin lagen abschriftlich vor.

Diese Unterlagen wurden, unter gleichzeitiger Einschaltung unseres externen Referenten für IT-Technik, Herrn Dr. Todt, eingehend geprüft. Dabei ergab sich eine Reihe von Fragen, die von der GSDA ausführlich beantwortet wurden. Im Mai 2015 wurde in einer ersten vorläufigen Stellungnahme eine Reihe von Empfehlungen zur Verbesserung des Schutzes der Datenverarbeitung formuliert. Offen blieb zu diesem Zeitpunkt allerdings, ob auch Daten, die unter die Schweigepflicht fallen, dort verarbeitet werden oder nur statistische Daten. Die Auftragnehmerin hat zu der Stellungnahme weitere Erklärungen und Erläuterungen zur Verfügung gestellt und auch die Bereitschaft gezeigt, die Empfehlungen umzusetzen. Schließlich blieb nur noch ein Problem zu klären. Da tatsächlich personenbezogene Daten mit Geheimnisschutz nach § 203 StGB verarbeitet werden, muss ausgeschlossen sein, dass Mitarbeiter der Auftragnehmerin hierzu Zugang haben. Schließlich haben sich die Parteien insoweit auf ein Verfahren geeinigt, dass eine Fernwartung nur nach dem Start des Programms „TeamViewer“ und der telefonischen Übermittlung der Rechner-Nummer sowie des Passworts eine Sitzung ermöglicht, bei der ein Mitarbeiter des Auftraggebers die ganze Zeit zugegen ist. Er kann jede Aktion auf dem Bildschirm verfolgen und bei unautorisierten Eingriffen einschreiten oder die Sitzung beenden.

3.3 Datenschutz in Schulen

Im 1. Jahresbericht wurde angegeben, dass der Datenschutz in Schulen Schwerpunktthema des laufenden Berichtsjahres werden sollte.

Hierzu sollte zunächst eine Befragung der Schulen zur Ermittlung des Ist-Standes der Datenverarbeitung durchgeführt werden. Dafür wurden insgesamt 64 kirchliche Schulen in den (Erz-)Bistümern Hamburg, Hildesheim und Osnabrück sowie im Offizialatsbezirk Vechta angeschrieben. Auf Grund eines einheitlichen Formulars wurden sie um Angabe gebeten über die vorhandene Ausstattung mit Schulverwaltungsrechnern, EDV-Systemen zur Nutzung durch Schüler und private Rechner der Lehrkräfte. Darüber hinaus wurde auch nach der Bestellung eines betrieblichen Datenschutzbeauftragten sowie dem Bestehen eines Datenschutz- und IT-Sicherheitskonzeptes gefragt. Der komplette Fragebogen ist als Muster in der Anlage zu diesem Bericht beigefügt.

Insgesamt wurden 71 Schulen angeschrieben. Davon haben leider nur 32 geantwortet. Hieraus ergibt sich ein Rücklauf in Höhe von 45,07%. Das Erzbistum Hamburg hatte nach Einleitung der Aktion mitgeteilt, dass alle ihre Schulen zentral über das Schulamt

ausgestattet würden und manchem Schulleiter daher mangels Fachwissen die Möglichkeit fehle unsere Fragen konkret zu beantworten. Angesichts des Inhalts des Fragebogens kam es gar nicht auf EDV-Wissen an. Ob in der Schule ein Verwaltungsrechner vorhanden ist und ob Systeme zur Benutzung durch die Schüler bereitgestellt werden, müsste unschwer auch ein Schulleiter beantworten können. Einige Fragen dürfte dagegen das Schulamt nur schwer beantworten können, zum Beispiel die, nach der Anzahl der Beschwerden, die im vergangenen Schuljahr vorgelegen haben. Trotzdem wurde der uns benannte Referent für Datenschutz im Schulamt gebeten, uns die restlichen Fragebögen ausgefüllt zurückzureichen. Eine Antwort hierauf haben wir bis heute nicht erhalten. Lediglich zwei Schulen waren so nett uns zu informieren. Die Bereitschaft zur Zusammenarbeit mit dem amtlich bestellten Datenschutzbeauftragten scheint dort nicht allzu ausgeprägt zu sein. Rechnet man die Hamburger Schulen nicht mit, so ergebe sich eine Rücklaufquote in Höhe von 58,82%.

Statistisch ergab sich hierbei folgendes Bild:

Die in der Tabelle angegeben Schulen haben den Fragebogen zurückgeschickt. Die Auswertung kann nur sie berücksichtigen. Die jeweils angegebenen Zahlen geben den vorhandenen Bestand wieder.

	VR	SR	PR	bDSB	IT-B
Grundschulen (6)	5	4	3	2	3
Real- und Oberschulen (8)	8	8	3	3	6
Gymnasien und Gesamtschulen (11)	10	11	3	4	8
Berufsschulen (2)	2	2	1	2	2
Andere Schulen (4)	4	4	0	3	2
Schulen insgesamt (32)	**29**	**29**	**10**	**14**	**21**

In der Tabelle verwendete Abkürzungen:

VR: Verwaltungsrechner SR: Rechner für Schüler PR: private Rechner der Lehrer

bDSB: betrieblicher Datenschutzbeauftragter IT-B: IT-Beauftragten

Fast alle Schulen besitzen Rechner zur Verwaltung der Schulangelegenheiten. Drei Schulen haben jedoch angegeben, ihre Schülerakten allein in Papierform zu führen. Computerräume für Schüler sind ebenfalls in den meisten Schulen schon vorhanden. In aller Regel als EDV-Raum, der nur zu Unterrichtszwecken eingesetzt wird und in einem vom Schulrechner vollständig getrennten System betrieben wird. Private Rechner von Lehrkräften werden immerhin schon in knapp einem Drittel der Schulen eingesetzt. Von der Möglichkeit nach § 7 der Anordnung zum Schuldatenschutz wird demnach in vielen Fällen Gebrauch gemacht.

Auffällig ist, dass mehr IT-Beauftragte bestellt worden sind, als vergleichbar betriebliche Datenschutzbeauftragte. Hierfür werden häufig Lehrer eingesetzt, die fachlich die Möglichkeit besitzen, ein Computersystem zu betreuen. Für betriebliche Datenschutz-

beauftragte fehlt es an einer entsprechenden Lösung. § 2a der Schuldatenschutzordnung ist insoweit nur eine „Kann"-Bestimmung, die noch nicht einmal die Festlegung aus § 20 Abs. 2 KDO mit vollzieht, nach der die Bestellung zu einer „Soll"-Bestimmung wird, wenn mehr als zehn Personen mit der elektronischen Verarbeitung personenbezogener Daten befasst sind. Die Schulen, die keinen Datenschutzbeauftragten ernannt haben führten zur Begründung überwiegend an, dass ausschließlich Daten für eigene Zwecke erhoben werden und nicht mehr als 10 Personen mit der Datenverarbeitung beschäftigt sind. In einem Fall wurde dabei jedoch die Zahl der Lehrkräfte, die private Endgeräte einsetzen mit 40 angeben, die wohl bei der Berechnung nicht berücksichtigt worden sind.

Die weitere Erhebung bezog sich auf die Zahl eingesetzter Videoüberwachungssysteme. Erfreulicherweise haben nur 5 Schulen hiervon Gebrauch gemacht. Nur an 3 von ihnen erfolgt eine Aufzeichnung der Bilder. Beobachtet werden in 3 Fällen der Pausenhof, in 2 Fällen das Treppenhaus und in 2 Fällen andere Bereiche. In einem Fall wurde zusätzlich angegeben, dass die Aufzeichnung nur außerhalb der Schulzeit stattfindet, mit dem Ziel die Schule vor Vandalismus zu schützen.

Die Befragung gewährt angesichts des Rücklaufs der Fragebögen keinen umfassenden und abschließenden Überblick. Die bisher vorliegenden Ergebnisse sind zu einem großen Teil schon recht zufriedenstellend. Trotzdem sollte der Datenschutz weiter durch Bestellung betrieblicher Datenschutzbeauftragter gestärkt werden. Die Bistümer arbeiten daran, hier Lösungen für gemeinsame Datenschutzbeauftragte, die für eine bestimmte Region zuständig sind, zu finden. Die Ausbildung kann eventuell über das Datenschutzinstitut Niedersachsen oder die Datenschutzakademie Schleswig-Holstein erfolgen. Auch die datenschutz nord GmbH hat versprochen, in Zukunft Ausbildungslehrgänge mit Bezug auf das kirchliche Recht anzubieten.

Von der Möglichkeit zu einem persönlichen Gespräch über die datenschutzgerechte Organisation vor Ort, wie sie im Anschreiben bei Übersendung des Fragebogens angeboten wurde, hat nur eine Schule Gebrauch gemacht. Es wäre wünschenswert, wenn auch im Rahmen der zukünftigen Aufsicht dieses Thema stärker berücksichtigt werden kann.

3.4 Fortführung: Kindertagesstätten-Verwaltungsprogramm „KIDkita"

Im ersten Jahresbericht wurde bereits über die Prüfung des Kindertagesstätten-Verwaltungsprogramms „KIDkita" berichtet, dass aufgrund eines Rahmenvertrages, sowie Musterregelungen zur Datensicherheit und Datenschutz, als Auftragsdatenverarbeitung bei der Firma COMRAMO IT Holding AG in Hannover installiert werden soll. Der Referent für IT-Technik, Herr Dr. Todt, hatte hierzu im August 2014 eine Kurzstellungnahme erarbeitet. Damit war die Sache längst noch nicht abgeschlossen, so dass auch im Jahr 2015 die Prüfung weiter fortgesetzt wurde.

Eine Reihe von Fragen konnten einvernehmlich geklärt werden. Offen geblieben sind bis heute 3 Problemkreise:

1. Die Mandantentrennung. Zwar sind die einzelnen Datensätze mit der jeweiligen Mandantennummer versehen und dem Nutzer jeweils nur ein Mandant zugeordnet und somit eine ausreichende Zutrittskontrolle nach Ziffer 3 der Anlage 1 zu IV. KDO-DVO verwirklicht. Hier geht es aber um das Trennungsgebot nach Ziffer 8 der Anlage, so dass hier zusätzliche Maßnahmen, die im Falle eines Versagens der Zugriffssperre verhindern würden, dass der Anwender auf die Daten einer anderen Einrichtung Zugriff nehmen könnte.
2. Die Zugangskontrolle. Um Zugriffsversuchen über das Internet zu begegnen und eine mutwillige Störung des Systems durch Brute-Force-Attacken zu verhindern, sollte nach drei Fehlautorisierungen für den Nutzer ein Zugriff nicht mehr möglich sein. Eine solche Beschränkung, so wurde vom Anbieter mitgeteilt, sei programmtechnisch möglich. In diesem Fall ist gleichzeitig auch die Reaktivierung des Zugriffs zu regeln, um sicherzustellen, dass nur berechtigte Nutzer ein neues Passwort erhalten.
3. Das Berechtigungskonzept. Der Anbieter hat mitgeteilt, dass derzeit drei autorisierte Mitarbeiter Zugriff auf die Datenbank haben, der jedoch ausschließlich zur Softwareentwicklung und Fehleranalyse genutzt wird. Hier stellt sich die Frage, ob diese Arbeiten mit mandantenspezifischen Daten gemacht werden müssen oder ob hierfür nicht der Einsatz von Testdaten oder zumindest anonymisierten Echtdaten möglich ist.

Diese Fragen sind zurzeit noch nicht ausreichend geklärt, so dass eine Fortsetzung der Prüfung erforderlich ist.

3.5 Einsatz von Adobe Reader DC

Die heutige Entwicklung neuer Software-Versionen bringt häufig weitere Probleme. So beispielsweise beim Einsatz des PDF-Readers von Adobe. Insoweit wurde ich angefragt, ob dieses Programm allen Mitarbeitern in einer Dienststelle zur Verfügung gestellt werden kann.

Die Firmen wollen heute nicht nur Programme, sondern gleichzeitig auch ihre Cloud-Systeme verkaufen. Eine Installation der Software auf dem eigenen Rechner, mit der Aufgabe nur ein Lesen von PDF-Dokumenten zu ermöglichen, wird heute wesentlich erschwert. Mit jeder Programminstallation wird eine Speicherung der bearbeitenden Dateien in der Adobe-Cloud angeboten. Eine generelle Abschaltung ist nicht vorgesehen, so dass es im Belieben des jeweiligen Nutzers steht, hiervon Gebrauch zu machen. Um ein „Hochladen“ zu verhindern muss der Anwender, unter dem Fenster „Zuletzt verwendet“ am unteren Bildrand der Darstellung den Hinweis „Mobile Link EIN“ auf „Mobile Link AUS“ setzen. Darüber hinaus können unter dem Fenster „Konto hinzufügen“ noch weitere Cloud-Dienste, wie „Dropbox“ oder „Microsoft Share Point“ zur Nutzung ausgewählt werden. Für einen Einzelanwender mag das ausreichend sein, da er nur die Entscheidung für sich selbst zu treffen hat. Für den Einsatz in einer Behörde besteht nach hiesiger Kenntnis keine Möglichkeit die Verfahrensweise administrativ festzulegen.

3.6 Einsatz von Instant Messenger Systemen in Pflegediensten

Der Malteser Hilfsdienst in Hamburg hatte beim Berliner Datenschutzbeauftragten angefragt, ob er Messenger-Dienste benennen könne, die im Bereich des ambulanten Pflegedienstes datenschutzgerecht eingesetzt werden können. Dieser hatte in seinem Tätigkeitsbericht 2014 festgestellt, dass deren Einsatz in empfindlichen Bereichen nicht grundsätzlich unzulässig ist. Die Anfrage wurde an mich weitergeleitet und dankenswerter Weise gemeinsam mit den Kollegen aus Berlin geklärt.

Als Ergebnis lässt sich danach folgendes feststellen:

- Eine Sicherheit der übermittelten Inhalte ist nur bei einer Ende-zu-Ende-Verschlüsselung gegeben. Nur dann bleiben die Nachrichten auf dem Transportweg unlesbar.
- Der Einsatz der Verfahren zur Vornahme einer solchen Verschlüsselung ist bei Open-Source-Programmen gut zu überprüfen. Bei gewerblich hergestellter Software ist man jedoch allein auf die Angaben des Herstellers angewiesen. Daher sollten die quelloffenen Programme bevorzugt werden.
- Ein Schutz der Daten, wer mit wem Nachrichten ausgetauscht hat (Metadaten), ist nur beim Einsatz eines eigenen Servers möglich. Es muss daher vorher entschieden werden, ob die Sicherung der Metadaten erforderlich ist. Dabei spielen vor allem arbeitsrechtliche Gesichtspunkte eine Rolle. Für den Fall von Gruppenchats, an denen immer die Zentrale beteiligt ist, kann dieser Punkt vernachlässigt werden.

In der Sache selbst sind wir zu dem Ergebnis gekommen, dass der Einsatz von WhatsApp unter Sicherheitsanforderungen absolut ungeeignet ist. Die höchste Sicherheit bieten Programme wie „Conversations (nur für Android)“, „Signal“ und „Text Secure“ (beide für Android und iOS ab Vers. 8.0). Bei „Threema“ handelt es sich um ein proprietäres Programm, das jedoch von der Universität Amsterdam in einer Studie nach umfangreichen Untersuchungen als gut umgesetzt und sicher eingestuft wurde.

Da sich die Software-Versionen ständig ändern und auch in ihren Sicherheitsaspekten verändert werden, kann zur aktuellen Information in diesem Falle die eingehende Auflistung bei Wikipedia zu Rate gezogen werden.
→ Liste von mobilen Instant-Messengern

3.7 Cloud-System im Krankenhaus

Ein Berliner Krankenhaus fragte an, ob Patientendaten auch in einem Cloud-System gespeichert und verarbeitet werden können. Nach dem Berliner Krankenhausgesetz, das auch für kirchliche Häuser gilt, wird in § 24 Abs. 7 bestimmt, dass Patientendaten auf einem Server der Einrichtung selbst zu führen sind. Ausnahmen bestehen nur dann, wenn aus organisatorischen Gründen, sich ein Krankenhaus der Hilfestellung durch eine andere Klinik bedient. Die Datenverarbeitung durch nichtklinische Stellen ist nur dann erlaubt, wenn durch technische Schutzmaßnahmen sichergestellt ist, dass

der Auftragnehmer keine Möglichkeit hat, die gespeicherten Daten einzusehen. Augenblicklich gibt es nur ein Verfahren, dass diese Anforderung erfüllt und daher auch für Daten, die nach § 203 StGB der Verschwiegenheitspflicht unterliegen, geeignet ist. Es handelt sich dabei um iDGARD, das unter Ziffer 2.3 in diesem Bericht besprochen worden ist.

3.8 Verpflichtungserklärungen für hauptamtliche und ehrenamtliche Mitarbeiter

Ein Mitglied des Kirchenvorstandes einer Pfarrgemeinde fragte an, warum sich die Formulare für die Verpflichtungserklärungen von Haupt- und Ehrenamtlichen unterscheiden. Schnell geantwortet war natürlich darauf hinzuweisen, dass Ehrenamtliche nicht auf disziplinarrechtliche und arbeitsrechtliche Folgen hingewiesen werden können. Aber das war nicht das Problem, um das es in dieser Frage dem KV-Mitglied ging. Er wollte vielmehr wissen, warum der Hinweis auf die KDO und die Belehrung über die hiernach geltenden grundlegenden Bestimmungen im Formular für Ehrenamtliche fehlen, obwohl dies durch Ziffer III in Absatz 1 Nr. 2 KDO-DVO ausdrücklich vorgeschrieben ist.

In Abschnitt II Abs. 1 werden die Ehrenamtlichen ausdrücklich auch zu den tätigen Personen im Sinne von § 4 KDO gezählt. Daher ist davon auszugehen, dass der Inhalt der Datenschutzerklärung, wie er von Abschnitt III KDO-DVO vorgegeben wird, auch für Ehrenamtliche gilt. Da es sich um eine verpflichtende Bestimmung handelt (… hat zum Inhalt) muss dringend geklärt werden, ob das verordnete Formular für Ehrenamtliche nicht den Festsetzungen der KDO-DVO zuwiderläuft.

4. Öffentlichkeitsarbeit / Unterrichtung der Dienststellen

4.1 Internetauftritt – Bedeutung

In § 18 Abs. 1 S.1 KDO wird die Aufgabe des Diözesandatenschutzbeauftragten grundsätzlich wie folgt beschrieben:

> *„Der Datenschutzbeauftragte wacht über die Einhaltung der Vorschriften dieser Anordnung sowie anderer Vorschriften über den Datenschutz."*

Diese Aufgabe kann er nicht allein durch das Abhalten von Vorträgen, Schulungsmaßnahmen und persönlichen Gesprächen mit den Dienststellenleitern, ihren IT-Beauftragten und betrieblichen Datenschutzbeauftragten erfüllen, so wichtig solche Begegnungen auch sind. Zu groß ist dafür das Gebiet der räumlichen Zuständigkeit. Ein Einzelner kann dies nicht umfassend personell versorgen.

Es muss also darüber hinaus auch eine umfangreiche Information zur Verfügung stehen. So muss eine Möglichkeit geschaffen werden, wo Mitarbeiterinnen und Mitarbeiter sich jederzeit über die datenschutzgerechten Anforderungen ihrer Tätigkeit informieren können. Da heute alle Dienststellen über Internetzugänge verfügen, ist die Einrichtung einer Webseite hierbei das geeignete Mittel zur Aufklärung. Der Diözesandatenschutzbeauftragte hat daher in seiner Amtszeit großen Wert auf die Schaffung eines solchen Angebots gelegt und immer wieder versucht, den Internetauftritt im Hinblick auf die Zielgruppe „Mitarbeiter in kirchlichen Dienststellen" zu verbessern. Dieses Angebot ist zur Ergänzung der persönlichen Beratung gedacht.

Darüber hinaus muss sich auch die Öffentlichkeit über den Datenschutz in den Nordbistümern informieren können. § 18 Abs. 3 KDO bestimmt hierzu nunmehr:

> „Der Diözesandatenschutzbeauftragte erstellt jährlich einen Tätigkeitsbericht, der dem Bischof vorgelegt und der Öffentlichkeit zugänglich gemacht wird."

Die Bekanntmachung der Tätigkeitsberichte erfolgte bereits in Abstimmung mit den Bistümern vor Erlass der neuen KDO, erstmalig mit dem Bericht von 2004-2009. Auf diese Weise geht auch die Kirche offen mit ihrer Verantwortung zum Schutz des informationellen Selbstbestimmungsrechts der Bürger um.

Dem dient auch die Projektpartnerschaft im „Virtuellen Datenschutzbüro", der zentralen Portalseite die gemeinsam von allen öffentlichen Datenschützern des Bundes und der Länder, unter Einbeziehung der beiden Kirchen erstellt wird. Sie macht die Eigenständigkeit kirchlichen Handelns auf diesem Gebiet auch in der Öffentlichkeit deutlich. Und sie bewirkt, dass Kirche auch als aktiv Handelnde wahrgenommen wird, wenn es um den Schutz des Persönlichkeitsrechts der Bürger geht.

Mein Nachfolger, Herr Mündelein, hat bei einem ersten Treffen zur Übernahme der Tätigkeit bereits zu verstehen gegeben, dass er die Webseite komplett übernehmen und weiterführen will.

4.2 Internetauftritt – Inhaltliche Gestaltung

Bereits im 1. Jahresbericht (2014/15) wurde die Erneuerung und Verbesserung der Webseite dargestellt. Im Berichtsjahr ist hieran im Grunde nichts verändert worden. Die Veränderungen, insbesondere die tabellarische Darstellung im Bereich „Themen“ haben sich nach den Reaktionen vieler Beteiligter bewährt.

Es sind jedoch neue Inhalte hinzugekommen oder vorhandene Beiträge aktualisiert worden.

- Eine neue Arbeitshilfe mit einer „Einführung in das Datenschutzrecht der katholischen Kirche“ wurde veröffentlicht. Sie dient als Erstinformation für Mitarbeiterinnen und Mitarbeiter, zu ihrer Unterrichtung vor Abgabe der Datenschutzerklärung nach § 4 KDO. (Oktober 2015)
- Es wurden „Hinweise zur Anforderung an Schul-EDV“ veröffentlicht (Juni 2015)
- Die „Hinweise zur Veröffentlichung personenbezogener Daten auf Internetseiten von Schulen in kirchlicher Trägerschaft“ wurde aktualisiert (2. Aufl. Mai 2015)
- Die Arbeitshilfe „Datenschutz im Pfarrbüro“ wurde im Hinblick auf das neue Melderecht erneuert. (2. Aufl., Dezember 2015)

Die datenschutz nord GmbH, die uns in der Beratung und Kontrolle auf technischem Gebiet unterstützt, hat ein Datenschutzhandbuch „ISO 27001 und andere Normen“ geschaffen und zum Download zur Verfügung gestellt. Darin werden Normen und Standards zur Sicherheit in der Informationstechnologie nach Empfehlungen des BSI dargestellt.

Zudem sind viele aktuelle Themen, auch aus dem staatlichen Bereich, wie das Prüfmodell für datenschutzgerechte Installationen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder oder das BSI-Magazin „Mit Sicherheit“ über die Modernisierung des IT-Grundschutzes und das neue IT-Sicherheitsgesetz des Bundes dargestellt und die Anlagen hierzu veröffentlicht worden.

Nach Zustimmung durch die Teilnehmer unseres IT-Workshops sind auch die Newsletter weiter fortgeführt worden. Im Berichtsjahr sind insgesamt 15 allgemeine Newsletter für betriebliche Datenschutzbeauftragte und IT-Verantwortliche und 3 speziell für betriebliche Datenschutzbeauftragte in Krankenhäusern versandt worden.

Der Inhalt des Bereichs „Recht“ wurde ständig aktualisiert und gibt derzeit den aktuellen Rechtsstand in den norddeutschen Bistümern wieder. Das gilt für die neue KDO-DVO, die Änderungen an der KMAO und der KAO. Im Berichtsjahr sind auch die Vorschriften über die Prävention vor sexualisierter Gewalt an Minderjährigen und hilflosen Erwachsenen aufgenommen worden, da das Verfahren insoweit ebenfalls von datenschutzrechtlichen Regeln beeinflusst wird.

Auch der Rechtsprechungsteil wurde behutsam um Urteile ergänzt, die den Datenschutz betreffen und 2015 ergangen sind.

4.3 Vorträge

Im Berichtszeitraum ist der Unterzeichner nur zwei Mal zu Vorträgen eingeladen worden. Am 18. März hat er eine Pfarrsekretärinnenschulung in Magdeburg abgehalten. Am 8. Dezember war er zu einem Treffen der Geschäftsführerkonferenz des Caritasverbandes für die Diözese Hildesheim e.V. eingeladen, wo die Teilnehmer über die neue KDO-DVO und die mit ihr erlassenen IT-Richtlinien informiert werden wollten. Inhaltlich wurde hierzu schon durch meine Ausführungen unter Ziffer 1.2 dieses Berichts eingegangen.

5. Zusammenarbeit

5.1 Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands

Im Berichtszeitraum sind zwei Konferenzen durchgeführt worden. Am 21./22.04 in Fulda und am 03./04.12. in Köln. Der Diözesandatenschutzbeauftragte hat an der ersten Konferenz teilgenommen, für die zweite Konferenz, die kurz vor Ende seiner Bestellung lag, hat er seinen Nachfolger gebeten, hieran teilzunehmen, da dabei Themen erörtert würden, die für die zukünftige Arbeit von Bedeutung seien.

Angesichts der momentanen Situation haben auf der Tagung im April die Schaffung einer Europäischen Datenschutzgrundverordnung und hiermit verbunden die Änderung der kirchlichen Datenschutzaufsicht und die Erstellung und Veröffentlichung von Tätigkeitsberichten im Vordergrund gestanden. Darüber hinaus wurde über das neue Melderecht und OSCI-X-Meld und das Forschungsvorhaben Sexueller Missbrauch gesprochen. Herr Schmid von der Genossenschaft der Werkstätten für behinderte Menschen Hessen und Thüringen eG präsentierte den Anwesenden die Anforderungen an eine ordnungsgemäße Aktenvernichtung.

5.2 IT-Workshop

Im Berichtsjahr haben zwei IT-Workshops am 28.01.2015 und 15.07.2015 in Hannover stattgefunden. Dabei hat sich wiederum eine verstärkte Zusammenarbeit zwischen den betrieblichen Datenschutzbeauftragten der Bistümer, der Datenschutzreferenten und der IT-Leiter der Ordinariate/Generalvikariate weiterhin bestens bewährt. In der Diskussion aller Beteiligten wurde vereinbart, künftig zwei Tagungen pro Jahr durchzuführen. Die Veranstaltungen waren in guter Teilnehmerzahl besucht.

Die Themen des 6. IT-Workshops wurden bereits im 1. Jahresbericht dargestellt.

Auf dem 7. Workshop im Juli 2015 wurde die Frage diskutiert, ob die Nordbistümer, ähnlich wie die Evangelische Kirche eine „Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung – ITSVO-EKD) erlassen sollten. Die Teilnehmer konnten sich nach eingehender Diskussion nicht entschließen, eine solche Regelung ihren Diözesen vorzuschlagen. Als Gründe hierfür wurden die neue KDO-DVO nebst IT-Richtlinie und die Entwicklung von Sicherheitskonzepten der Bistümer angeführt.

Herr Dr. Todt informierte dann über die Weiterentwicklung des Konzepts iDGARD, vor allem im Hinblick auf die Vorbewertung seitens der TÜV Informationstechnik GmbH, auf die bereits oben eingegangen wurde. Dabei liegt bisher nur eine konzeptionelle Prüfung vor. Eine technische Prüfung kann erst dann stattfinden, wenn die Prüfmethoden und deren Tiefe im TDCP festgelegt sind, was aber erst in der Version 1.0 erfolgen soll.

Dass Cloud-Systeme augenblicklich hohe Bedeutung in der datenschutzrechtlichen Beratung haben, zeigte sich bei einem weiteren Referat von Herrn Dr. Todt über die Webanwendung „ownCloud“. Dabei handelt es sich um ein Open-Source-Programm, das sowohl auf eigenen Servern, wie auch auf verlässlichen Dienstservern Dritter eingesetzt werden kann. Die Software ist im Bereich „Informationstechnik“ in diesem Bericht näher erläutert.

Darüber hinaus wurde der Newsletter über Updates und Sicherheitslücken allgemein begrüßt und inhaltlich als wichtig und informativ eingeschätzt. Auf Grund dieses positiven Feedbacks besteht die Bereitschaft ihn auch künftig fortzuführen.

Als nächster Termin für den kommenden IT-Workshop wurde der Januar 2016 vorgeschlagen.

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

Die Zusammenarbeit mit den Datenschutzbeauftragten und Datenschutzreferenten der Evangelischen Kirche wurde auch im Berichtsjahr weiter fortgeführt.

Von den Landeskirchen, die sich bisher nicht der gemeinsamen Datenschutzaufsicht der EKD angeschlossen haben, wurde am 19. November 2015 eine Tagung der Datenschutzbeauftragten in Dessau-Roßlau durchgeführt. Hierzu waren der Diözesandatenschutzbeauftragte der Nordbistümer wie auch der Vorsitzende unserer Datenschutzkonferenz, Herr Dr. Fachet, als Gäste eingeladen, die beide teilgenommen haben.

Ebenso war der Unterzeichner am 17.06.2015 als Gast Teilnehmer der Referentenkonferenz im Kirchenamt der EKD. Am zweiten Tag der Konferenz, an dem Themen aus den Bereichen Meldewesen und Kirchenmitgliedschaftsrecht erörtert wurden, hat er allerdings nicht teilgenommen. Die nächste Sitzung soll am 8./9.06.2016 stattfinden.

Insgesamt ist mit den Fachkollegen auf Seiten der EKD ein intensiver und fruchtbarer Austausch erfolgt.

5.4 Zusammenarbeit mit den Datenschutzbeauftragten der Länder

Weiterhin finden regelmäßige Kontaktgespräche nur mit dem Landesbeauftragten der Freien und Hansestadt Hamburg statt. Dabei erfolgt jedes Mal ein intensiver Austausch ohne vorher festgelegte Tagesordnung und Themen. An den Treffen nehmen die evangelischen und katholischen Datenschutzbeauftragten zu gleicher Zeit teil.

Die Zusammenarbeit mit anderen Datenschutzbehörden bezüglich der Absprache der Behandlung von Fällen, die beide Seiten betreffen, funktioniert im gegenseitigen Einvernehmen und mit Unterstützung in der gleichen Sache. Beschwerden, die fälschlicherweise an den Landesbeauftragten gerichtet werden, aber den Datenschutz der

katholischen Kirche betreffen, werden kurzfristig an die kirchliche Aufsichtsstelle weitergeleitet. Dabei wird der Betroffene über die besondere Zuständigkeit informiert.

Soweit erforderlich, ergibt sich eine sehr angenehme Zusammenarbeit mit den Datenschutzaufsichtsbehörden der Länder.

5.5 Projektpartnerschaft im Virtuellen Datenschutzbüro

Der Diözesandatenschutzbeauftragte der norddeutschen Bistümer hat auch während des Berichtsjahrs seine Projektpartnerschaft im Virtuellen Datenschutzbüro fortgesetzt. Er hat sich weiterhin mit einem festen Betrag in Höhe von 500,00 EUR pro Jahr an den Kosten des Betriebs der Seite www.datenschutz.de beteiligt. Die Kosten haben sich insgesamt im Jahre 2015 auf 41.412,00 EUR belaufen, von denen 33.350,00 EUR durch die Projektpartner zur Verfügung gestellt wurden. Es lag also eine Unterdeckung in Höhe von 8.062,00 EUR vor, die allein vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein getragen wurde.

Die Umgestaltung der Webseite wurde energisch vorangetrieben. Die Projektpartner haben sich auf der Sitzung am 24.02.2015 entschlossen,

- das Konzept gemeinsam mit einer Hochschule umsetzen zu lassen,
- eine Arbeitsgruppe zu bilden, die mit der Hochschule zusammenarbeitet
- und die bestehenden Kooperationspartnerschaften zu beenden.

Die Beschlüsse sind in einer Mail-Abstimmung auch mit den Projektpartnern, die nicht auf der Konferenz vertreten waren, abgestimmt worden.

In der Praxis wurde dann mit Hilfe der Fachhochschule Lübeck, Fachbereich Elektrotechnik und Informatik, eine Studentin mit einer Bachelorarbeit als Abschlussarbeit ihrer Ausbildung beauftragt, eine Neugestaltung des Internetauftritts des Virtuellen Datenschutzbüros zu entwerfen. Gleichzeitig wurde eine Arbeitsgruppe aus sechs Personen gebildet, in der auch der Unterzeichner mitgewirkt hat, die regelmäßig die vorliegenden Entwürfe begleitet, kommentiert und mit Änderungswünschen versehen hat. Die Treffen der Projektpartner fanden jeweils in Hannover, im Niels-Stensen-Haus statt. In der letzten Sitzung am 14. Dezember wurde die abschließende Gestaltung der Webseite besprochen und festgelegt. Die Umsetzung der Neugestaltung soll nun schnell vorgenommen werden. Als Termin für eine Freischaltung wird der 1. März 2016 angestrebt, wobei die Projektpartner schon einen Monat zuvor Zugang zu der Testseite bekommen sollen.

Der Unterzeichner ist nach wie vor der Meinung, dass die Teilnahme an diesem Projekt wichtig ist. Das gilt umso mehr, als die Zielgruppe dieser Plattform der Normalbürger ist, der in der Regel keine genauen Kenntnisse über Datenschutz mitbringt. Hier sollte die Kirche mit ihrer Eigenständigkeit und ihren eigenen Verordnungen und Aufsichtsinstanzen deutlich in Erscheinung treten.

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 31. Januar 2016

Lutz Grammann
Diözesandatenschutzbeauftragter

Anhang:

- Berliner Beauftragter für Datenschutz und Informationsfreiheit: Datenschutzrechtliche Hinweise zum neuen Melderecht (Presseerklärung vom 2. November 2015)
- Durchführung einer Datenschutzprüfung nach dem Handbuch zum „Standard-Datenschutz-Modell (SDM)“
- Vortrag vor der Geschäftsführerkonferenz beim Caritasverband Hildesheim am 08.12.2015 „Vergleich zwischen den Bestimmungen der KDO-DVO 2003 und der KDO-DVO 2015“
- Fragenkatalog zur strukturierten Erhebung über die IT-Ausstattung in Schulen

**Berliner Beauftragter für
Datenschutz und Informationsfreiheit**

Friedrichstr. 219
10969 Berlin

Tel: (030) 13889 - 0
Fax: (030) 13889 201

711.353.1

2. November 2015

Datenschutzrechtliche Hinweise zum neuen Melderecht

Am 1. November 2015 ist das Bundesmeldegesetz in Kraft getreten. Es weist erhebliche datenschutzrechtliche Defizite auf, die wir im Gesetzgebungsverfahren wiederholt kritisiert haben.

Unter anderem wird es zulässig bleiben, allein durch die Glaubhaftmachung eines berechtigten Interesses anstelle des Nachweises eines rechtlichen Interesses eine erweiterte Meldeauskunft und damit unter anderem Geburts- und Sterbedaten, Angaben über den Familienstand von Personen und über deren Ehegatten oder Lebenspartner sowie frühere Anschriften zu erhalten. Auch wurde die Hotelmeldepflicht nicht, wie ursprünglich geplant, abgeschafft, obwohl sie eine unverhältnismäßige, da umfangreiche und verdachtslose Datenerhebung und -speicherung auf Vorrat zur Folge hat.

In vielen Punkten stellt das neue Meldegesetz sogar eine Verschlechterung gegenüber der bisherigen Rechtslage dar. Zum Beispiel wurde die Mitwirkungspflicht des Wohnungsgebers bei der An- und Abmeldung zur Verhinderung von Scheinanmeldungen wieder eingeführt, obwohl sie 2001 aus dem Melderechtsrahmengesetz mit der Begründung gestrichen worden war, dass sie nur in den wenigsten Fällen hierzu geeignet ist. Darüber hinaus wurden sämtliche Einwilligungslösungen bei Melderegisterauskünften in besonderen Fällen abgeschafft. Zudem besteht keine Widerspruchsmöglichkeit mehr gegen die Erteilung einfacher Melderegisterauskünfte über das Internet. Zukünftig wird es auch nicht mehr möglich sein, der Meldebehörde Daten einer Person zu benennen, die benachrichtigt werden soll, falls einem etwas zustößt.

Gerade wegen der datenschutzrechtlichen Unzulänglichkeiten des neuen Melderechts ist es wichtig, seine Betroffenenrechte zu kennen und wahrzunehmen:

- Es ist weiterhin nicht erforderlich, der Meldebehörde bei einer Anmeldung den Mietvertrag vorzulegen.
- Nach wie vor können unerwünschte Wahlwerbebriefe von Parteien oder anderen Trägern von Wahlvorschlägen durch einen rechtzeitigen Widerspruch gegen die Weitergabe eigener Meldedaten an diesen Kreis vermieden werden.

Zentraler Bereich
beim Berliner Beauftragten für Datenschutz und Informationsfreiheit
Verantwortlich: Anja-Maria Gardain
Geschäftsstelle: Cristina Vecchi

Informationen zu Datenschutz und Informationsfreiheit

- Zukünftig ist ein Widerspruch auch dann erforderlich, wenn die eigenen Meldedaten nicht an Adressbuchverlage oder bei Alters- oder Ehejubiläen an Mandatsträger, Presse oder Rundfunk weitergegeben werden sollen. Bisher war für eine solche Datenübermittlung die Einwilligung des Betroffenen notwendig.

- Die Weitergabe von Meldedaten für Zwecke der Werbung oder des Adresshandels ist hingegen weiterhin nur mit Einwilligung möglich. Eine solche Einwilligung kann jederzeit widerrufen werden.

- Im Rahmen einer gebührenfreien Selbstauskunft gegenüber der Meldebehörde ist es den betroffenen Personen unter anderem möglich zu erfahren, welche Daten über sie gespeichert sind, woher diese Daten stammen und wer Empfänger regelmäßiger Datenübermittlungen ist.

Dix: „Das Bundesmeldegesetz ist in vielen Teilen nicht datenschutzfreundlich ausgestaltet. Bestehende Betroffenenrechte sollten daher aktiv genutzt werden. Bestimmte unerwünschte Datenübermittlungen aus dem Melderegister an Dritte können zum Beispiel durch die Nutzung der vorgesehenen Widerspruchsmöglichkeiten unterbunden werden.“

Durchführung einer Datenschutzprüfung

nach dem Handbuch zum „Standard-Datenschutz-Modell (SDM)“
der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Beginn der Datenschutzprüfung

Besteht eine Rechtsgrundlage? Liegen die Einwilligungen der Betroffenen vor?

Ist das Verfahren prüffähig? Liegt dafür eine hinreichende Dokumentation vor? Sind die Datenbestände, die eingesetzte Hard- und Software einschließlich der Schnittstellen, Prozesse und Datenflüsse in diese Dokumentation vollständig einbezogen?

Zu erreichende Schutzziele unter Berücksichtigung der Datenschutzklassen I bis III.
(Nach der Anlage 2, Ziffer 4.0 bis 4.4 der KDO-DVO)

1. Sind die Daten auffindbar und liegen im Zugriff der Berechtigten? **(Verfügbarkeit)**
2. Ist die Vollständigkeit, Unversehrtheit und Aktualität der Daten gewährleistet? **(Integrität)**
3. Können die Daten nur von berechtigten Personen eingesehen und verarbeitet werden? **(Vertraulichkeit)**
4. Ist die Datenverarbeitung in all ihren Schritten vollständig nachvollziehbar? Ist das Verfahren ausreichend dokumentiert und werden die Tätigkeiten protokolliert? **(Transparenz)**
5. Ist die Datenverarbeitung so eingerichtet, dass sie jederzeit in Bezug auf neue rechtliche Anforderungen oder geänderte tatsächliche Verhältnisse angepasst werden kann? Kann auch auf sicherheitstechnische Probleme sofort reagiert werden? Wie hoch liegt der Schutzbedarf? **(Intervenierbarkeit)**
6. Sind die eingesetzten Verfahren ausreichend voneinander getrennt? Ist ein Datenaustausch zwischen ihnen nur unter festgelegten und rechtlich geprüften Bedingungen möglich? Erfolgt insoweit eine Kontrolle? **(Wahrung der Zweckbindung)**
7. Ist die **Datensparsamkeit** ausreichend gesichert? Können die Aufgaben auch mit einem geringeren Datenbestand durchgeführt werden?

Ende der Datenschutzprüfung

Folgen, wenn eine der Fragen mit „nein“ beantwortet wird: Beanstandung, Anordnung, Nachprüfung.

Vortrag

Geschäftsführerkonferenz beim Caritasverband Hildesheim am 8. Dezember 2015

Vergleich zwischen den Bestimmungen der KDO-DVO 2003 und der KDO-DVO 2015

KDO-DVO 2003			KDO-DVO 2015	
I.	Zu § 3a KDO	Keine Änderung	I.	Zu § 3a KDO
II.	Zu § 4 KDO	Keine Änderung	II.	Zu § 4 KDO
III.	Zu § 4 KDO	Keine Änderung	III.	Zu § 4 KDO
IV.	Anlage zu § 6 KDO		IV.	Anlage zu § 6 KDO
		= Anlage zu § 6 KDO-DVO 03		Anlage 1
		Neu!		Anlage 2
V.	Zu § 12 Abs. 3 KDO	Keine Änderung	V.	Zu § 12 Abs. 3 KDO
VI.	Zu § 13 Abs. 1 KDO	Keine Änderung	VI.	Zu § 13 Abs. 1 KDO
VII.	Zu § 13a KDO	Keine Änderung	VII.	Zu § 13a KDO
VIII.	Zu § 14 KDO	Keine Änderung	VIII.	Zu § 14 KDO
IX.	Aufhebung der KDO-DVO 1994		IX.	Aufhebung der KDO-DVO 2003
Anlagen:			**Anlagen:**	
	Hinweis zur Meldung von Verfahren automatisierter Verarbeitungen	Bisher nicht neu erlassen.	1.	
	Meldung von Verfahren automatisierter Verarbeitungen	Bisher nicht neu erlassen.	2.	
	Verpflichtungserklärung gem. § 4 KDO	Bisher nicht neu erlassen.	3.	
	Verpflichtungserklärung für Ehrenamtliche gem. § 4 KDO	Bisher nicht neu erlassen.	4.	
		Neu!		Zu Abschnitt IV. KDO-DVO (Anlage 2 zu § 6 KDO): IT-Richtlinien

A. Erhaltung der KDO-DVO 2003 bei gleichzeitiger Erweiterung durch zwei neue Teile

Die 2015 neu erlassene KDO-DVO hat eine Vielzahl der Bestimmungen der Verordnung von 2003 übernommen. Das gilt in wörtlicher Textgleichheit für die Bestimmungen unter den Punkten I bis III und V bis VIII. Auch der bisherige Punkt „IV Anlage zu § 6 KDO“, der die acht wesentlichen Gebote zur Datensicherung enthält, ist nunmehr unverändert als Anlage 1 zu Punkt IV übernommen worden. Insoweit ist die KDO-DVO in vollem Umfang erhalten worden.

In zwei wesentlichen Punkten ist die neue Durchführungsverordnung jedoch erweitert worden. Als Anlage 2 zu § 6 KDO ist die früher in den Nordbistümern geltende „Richtlinie zum Einsatz von Arbeitsplatzcomputern“ (APC-Richtlinie) in die KDO-DVO eingearbeitet worden und zudem sind die zu ihrer Umsetzung notwendigen Maßnahmen in einer „IT-Richtlinie“ festgehalten worden.

Die APC-Richtlinie wurde bereits im Jahre 1994, also vor mehr als 20 Jahren geschaffen! Seitdem hat sich die Computer-Landschaft wesentlich verändert. Der Diözesandatenschutzbeauftragte hatte daher mehrfach darauf hingewiesen, dass eine Überarbeitung und Modernisierung dieser Vorschrift erforderlich sei. Die Arbeiten hieran sind dann durch eine schwerwiegende Erkrankung des Verfassers im Jahre 2011 unterbrochen und nach seiner Rückkehr nicht wieder aufgenommen worden, mit der Begründung, dass mittlerweile der VDD daran arbeite, eine für alle Bistümer in Deutschland einheitliche Lösung auf diesem Gebiet zu schaffen. Durch die Erweiterung der KDO-DVO ist dies nunmehr geschehen, jedoch ohne die „Reformvorstellungen“ des Unterzeichners zu berücksichtigen. An vielen Stellen wird dies sichtbar.

B. Fortführung der bisherigen Vorschriften mit fehlendem Neuerlass der Muster (Anlagen)

1. Meldepflicht und Verzeichnis nach § 3a KDO, Ziffer I KDO-DVO

An dem Verfahren der Meldung von automatisierten Datenverarbeitungen (§ 3a KDO) hat sich nichts geändert. Nach der Bestimmung in Absatz 2 soll hierfür, wie bisher, ein Muster laut Anlage verwandt werden. Das Bistum Hildesheim hat jedoch bisher kein neues Muster verkündet und die Geltung der alten KDO-DVO durch Ziffer IX außer Kraft gesetzt. Da sich an diesem Teil des Verordnungstextes gegenüber der KDO-DVO 2003 nichts geändert hat sollte daher weiterhin, bis zum Erlass eines neuen Musters, die bisherige Form weiter verwendet werden.

Die Meldung ist nach wie vor dem Diözesandatenschutzbeauftragten vorzulegen (§ 3a Abs. 1 KDO). Diese Verpflichtung entfällt jedoch nach Absatz 3, wenn ein betrieblicher Datenschutzbeauftragter bestellt worden ist. Dann ist dieser der Empfänger der Meldung, § 21 Abs. 2 KDO.

2. Datengeheimnis, § 4 KDO, Ziffer II und II KDO-DVO

Die Verpflichtung zur Abgabe der Verpflichtungserklärung (§ 4 KDO) und das hierfür vorgeschriebene schriftliche Formular (III. Zu § 4 KDO) sind ebenfalls gleich geblieben. Das Bistum Hildesheim hat jedoch auch hier bisher keine neuen Muster erlassen. Da sich an der gesetzlichen Verpflichtung auch im Wort-

laut nichts geändert hat, sollten die bisherigen Muster, bis zu einem eventuellen Neuerlass weiter verwendet werden. Es sind dabei zwei unterschiedliche Vordrucke für hauptamtliche und ehrenamtliche Mitarbeiter vorgesehen.

Wichtig ist auch die Mitarbeiter dabei auf die wesentlichen Grundsätze des Datenschutzes hinzuweisen (II. Abs. 1 Ziff. 1). In der Regel geschieht dies aus zeitlichen und fachlichen Gründen nicht. Der Datenschutzbeauftragte hat deshalb hierfür eine „Einführung in das Datenschutzrecht der katholischen Kirche“ als Erstinformation für Mitarbeiter geschaffen. Sie ist als Arbeitshilfe auf der Webseite >www.datenschutz-kirche.de< unter > Themen < in der Rubrik > Datenschutz allgemein< veröffentlicht. Sie kann dort jederzeit heruntergeladen und zur Erfüllung dieser Belehrungspflicht verwendet werden.

Der VDD plant im Hinblick auf die jetzt geltende KDO-2014 und die KDO-DVO-2015 auch eine Neuauflage seiner Arbeitshilfe 206 zum Thema „Datenschutz und Melderecht der katholischen Kirche 2006“. Sobald diese Arbeitshilfe in aktualisierter Form vorliegt, kann und soll sie ebenfalls zur Unterrichtung der Mitarbeiter eingesetzt werden.

Auch mit den Gesetzestexten sind die Mitarbeiter vertraut zu machen. Auch hier empfiehlt sich ein Hinweis auf die Veröffentlichungen unter der Rubrik >Recht< >Bistum Hildesheim< auf der Webseite des Diözesandatenschutzbeauftragten.

3. **Unterrichtung des Betroffenen, Auskunftsanspruch und Benachrichtigungspflicht**
   Die Ausführungsvorschriften zur Unterrichtung der Betroffenen (§ 12 Abs. 3 KDO, Ziffer V KDO-DVO), der Auskunftsanspruch des Betroffenen (§ 13 Abs. 1 KDO, Ziffer VI KDO-DVO) und die Benachrichtigungspflicht bei Erhebung von Daten ohne Kenntnis des Betroffenen (§ 13a KDO, Ziffer VII KDO-DVO) sind in der bisherigen Form beibehalten worden.

4. **Berichtigung, Löschung oder Sperrung von Daten**
   Auch für das Verfahren und die Notwendigkeit der Berichtigung, Löschung oder Sperrung von Daten (§ 14 KDO) ergeben sich keine Änderungen zu der bisherigen Rechtslage.

C. Die neuen Teile der KDO-DVO

Hineinnahme der früheren APC-Richtlinie der Nordbistümer (Anlage 2) und IT-Richtlinien

Die Bestimmung der Arbeitsplatzcomputer ist im Hinblick auf die frühere APC-Richtlinie erweitert worden. Als Arbeitsplatzcomputer, für die diese Vorschrift gilt, werden nunmehr neben den klassischen PCs und PC-Netzwerken nunmehr auch mobile Endgeräte, wie Tablets und Smartphones einbezogen.

Hierdurch hat sich die EDV-Landschaft insgesamt verändert: Von einzelplatzbezogener oder im Falle eines lokalen Netzwerkes unternehmensbezogener Verarbeitung, hat sie den Sprung zu einem weltweit erreichbaren Arbeitsplatz gemacht. Gleichzeitig ist auch keine technische Homogenität mehr vorhanden oder auch

nur erreichbar. Denn neben dem Betriebssystem für den Server, kommen durch die mobilen Systeme auch noch weitere OS hinzu (iOS, Android, Windows Phone, Blackberry). Und diese Systeme sind in ihrer Ausführung und Version kaum einheitlich zu handhaben. Allein bei Android reichen die Betriebssytemversionen von derzeit von 4.1 bis 6.0, ohne die Möglichkeit, sie alle auf ein bestimmtes Level zu vereinheitlichen. Noch nicht einmal die Ausstattung mit Sicherheits-Updates ist einheitlich zu gewährleisten, da deren Zurverfügungstellung vom jeweiligen Hardwareanbieter abhängig ist. Das Problem moderner Datenverarbeitung besteht heute darin, die weltweit erreichbaren Daten so abzuschotten, dass nur berechtigte Personen auf sie Zugriff nehmen können. Gleichzeitig müssen sie vor den Aktivitäten krimineller Hacker geschützt werden. Hierzu wird empfohlen, den Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu Rate zu ziehen, der zuletzt am 19.11.2015 unter dem Titel „Die Lage der IT-Sicherheit in Deutschland 2015“ erschienen ist. Das BSI stellt darin zur Bedeutung von Schadprogrammen (Seite 22 und 23) fest:

> *„Schadprogramme sind weiterhin eine der größten Bedrohungen sowohl für private Anwender als auch für Unternehmen und Behörden. Gegenüber 2014 haben sich die Schadprogramme weiterentwickelt und die klassischen Abwehrmaßnahmen werden zunehmend umgangen. Mobile und alternative Plattformen geraten zunehmend in den Fokus der Angreifer. Schadprogramme werden oft durch Mitwirkung des Nutzers installiert, wodurch technische Schutzmaßnahmen umgangen werden und Angreifer in abgesicherte Netze eindringen können. **Zum Schutz reichen klassische AV-Lösungen und Firewalls nicht mehr aus, vielmehr muss IT-Sicherheit als Gesamtkonzept verstanden und umgesetzt werden, wozu auch die Einbeziehung des Nutzers gehört.**“*

Leider sieht weder die Anlage 2 zu § 6 KDO noch die hierzu erlassenen IT-Richtlinien eine Verpflichtung zur Erstellung eines IT-Sicherheitskonzepts vor. Aber ohne diese Maßnahme ist eine Sicherung moderner Informationssysteme nach § 6 KDO nicht möglich.

Eine gravierende Lücke besteht auch bei der Einbeziehung privater Datenverarbeitungssysteme, wenn ihnen die Möglichkeit eingeräumt wird auf Daten vom dienstlichen Server Zugriff zu nehmen (Bring Your Own Device). Ziffer 5.1 der Anlage 2 zu § 6 und Ziffer 4.3 der IT-Richtlinie werden der bestehenden Problematik nicht gerecht. Nicht gesehen wird die Anfälligkeit gegen Angriffe durch die Speicherung von Mobilfunkdaten in den Clouds der Hersteller, die Nutzung öffentlicher Hotspots, die meist unverschlüsselt übertragen und die Ortbarkeit der Geräte durch GPS-Systeme. Ebenso wenig werden die Gefahren durch eingesetzte Apps, die häufig Schadcode enthalten oder ungerechtfertigt auf gespeicherte, sensitive Daten Zugriff nehmen können (Beispiel: „Stagefright“ auf Android-Systemen) einer Lösung zugeführt. Richtig ist hierbei lediglich die statuierte grundsätzliche Unzulässigkeit in Ziffer 5.1 der Anlage 2. Sie lässt sich jedoch in vielen Fällen nicht durchhalten. Dann **muss** der Einsatz eines Mobile Device Managements (MDM) erfolgen, das den Bereich der privaten Nutzung von der dienstlichen Nutzung **vollständig** trennt. Auch hierzu ein weiteres Zitat aus dem Lagebericht des BSI:

> *„Mobile Device Management (MDM)-Systeme haben sich in den vergangenen Monaten weiterentwickelt. In Kooperation mit den Herstellern der mobilen Betriebssysteme werden mittlerweile Lösungen angeboten, die es ermöglichen, Regelwerke zu definieren, mit denen geschäftlich genutzte Mobilgeräte zentral verwaltet und eingeschränkt werden können. Dabei kann auch vorgegeben*

werden, welche Apps installiert werden dürfen. Auch Szenarien mit kombinierter privater und geschäftlicher Nutzung werden von MDM-Systemen adressiert.“

Die Anbindung mobiler Endgeräte an das eigene Computernetzwerk darf daher und unabhängig davon, ob es sich um dienstliche oder private Geräte handelt, nur unter verantwortlichem Einsatz eines MDM-Programms erfolgen. Diese Lösung wird jedoch in der KDO-DVO nicht vorgegeben. Sollte dabei eine Trennung zwischen dem dienstlichen und privatem Bereich nicht möglich sein ist Ziff. 3.4, 3. Unterpunkt anzuwenden. Der Einsatz privater Programme auf diesen Geräten ist dann unzulässig.

Zudem wird heute immer mehr die Benutzung von fremden Speicherplätzen, sogenannter „Clouds“ angestrebt. Der Vorteil liegt darin, dass Datenverarbeitung nicht mehr allein am Arbeitsplatz im Büro erfolgen kann, sondern praktisch überall durchführbar ist und mobile Endgeräte dafür sorgen, dass die gespeicherten Daten auch unterwegs abgerufen werden können. Zudem erleichtern die Clouds die fachliche Zusammenarbeit mehrerer Mitarbeiter. Nach Ziffer 4.2 der Anlage 2 handelt es sich hierbei um eine Auftragsdatenverarbeitung. Dabei muss sichergestellt sein, dass sich der Auftragnehmer zur Einhaltung der KDO verpflichtet und der Speicherort der Daten ausschließlich in Deutschland liegt. Die Benutzung öffentlicher Cloud-Angebote der Hersteller oder Mobilfunkanbieter ist daher folgerichtig ausgeschlossen. Bisher hat nur Microsoft die Absicht, die Speicherung von Daten innerhalb von „365 Office“ ab Mitte 2016 in Deutschland und Österreich zu ermöglichen. Der KDO werden sie sich trotzdem nicht unterwerden und die Aufsicht des Diözesandatenschutzbeauftragten nicht akzeptieren. Andere Systeme, wie die von Apple, T-Mobile, Google und vielen weiteren Anbietern brauchen nach 4.2 der Anlage 2 gar nicht in Betracht gezogen zu werden.

In der letzten Zeit ist zunehmend versucht worden, eigene „Private Clouds“ durch die Diözesen einzurichten, um auch hier sichere Systeme zu schaffen. Aus datenschutzrechtlicher Sicht, sind solche Systeme anzustreben. Dabei muss allerdings gewährleistet sein, dass jede Stelle als Cloud-Nutzer weiterhin selbstständig über die von ihr eingesetzten Programme und die gespeicherte Daten entscheiden kann. Der Zugriff unberechtigter Personen ist sowohl durch eine verschlüsselte Übertragung, wie auch durch eine verschlüsselte Speicherung herbeizuführen.

Weitere Lösungen sind die Benutzung des Open-Source Programms „ownCloud“, dass auf eigenen Servern installiert werden kann oder auch zur Benutzung auf kirchlichen Rechenzentren, wie KIGST bereitgestellt wird, sowie die Benutzung von „iDGARD“, das durch Anwendung der „Sealed Cloud Technologie“ sicherstellt, dass auch der Anbieter keinen Zugang zu den gespeicherten Daten hat und das Verfahren damit auch die Verschwiegenheitspflicht des Auftraggebers nach § 203 StGB umfassend berücksichtigt.

Verpflichtende Mindestanforderungen – Ziffer 3.4 der Anlage 2

a) Erstellung eines Verzeichnisses nach § 3a Abs. 4 KDO.
b) Verpflichtungserklärungen aller Mitarbeiter, die mit der automatischen Datenverarbeitung beteiligt sind.
c) Die ausschließliche Verwendung autorisierter Programme.

Zusätzliche Anforderungen – Ziffern 4.0 bis 4.4 der Anlage 2

a) Vornahme der Einteilung nach Datenschutzklassen.
b) Daten, die nicht elektronisch verarbeitet werden dürfen.
c) Einhaltung der Maßnahmen für die jeweilige Datenschutzklasse nach Ziff. 2.1 bis 2.3 IT-Richtlinien.
d) Maßnahmen zur Datensicherung nach Ziff. 3 bis 3.2 der IT-Richtlinien.

Besondere Gefahrenlagen – Ziffer 5.1 und 5.2 der Anlage 2

a) Nutzung privater Datenverarbeitungssysteme. Generelle Ausnahme: § 7 SchulDO. Hierzu auch Ziffer 4.3 IT-Richtlinien.
b) Fremdzugriffe, insbesondere Fernwartung und die Durchführung von Wartungsarbeiten innerhalb oder außerhalb der Dienststelle. Zu beachten ist hier Ziffer 5.2 der Anlage 2 und Ziffer 4.1.
c) Fremdzugriffe durch automatisierte Abrufvereinbarungen - § 7 KDO, Ziffer 5.2 Anlage 2 KDO-DVO.
d) Auftragsdatenverarbeitung innerhalb einer Cloud – Ziffer 4.2 IT-Richtlinien.
e) Verschrottung und Vernichtung von Datenträgern – Ziff. 4.6 IT-Richtlinien. Hier ist die DIN 66399 einzuhalten. Für die Bestellung eines Drittunternehmens sollte der vom Diözesandatenschutzbeauftragten empfohlene Mustervertrag zugrunde gelegt werden.
f) Verwaltung von BIOS- und Administrationspasswörtern – Ziffer 4.7 IT-Richtlinien.

Hannover, den 01. Dezember 2015

Der Diözesandatenschutzbeauftragte der norddt. Bistümer
Engelbosteler Damm 72 – 30167 Hannover – 0511/81 93 15
Mail: info@datenschutz-kirche.de – www.datenschutz-kirche.de

Fragenkatalog
zur strukturierten Erhebung über die IT-Ausstattung in Schulen

A. Grundangaben:

Name der Schule _____

Leiter der Schule _____

Betrieblicher Datenschutzbeauftragter _____

IT-Beauftragter _____

Größe der Schule:
Zahl der Schüler(innen) _____ Zahl der Klassen _____ Zahl der Lehrer _____

B. Angaben zur Ausstattung:

☐ Schüler- und Elterndaten werden elektronisch verarbeitet.
☐ Schüler- und Elterndaten werden in Papierform verarbeitet.

Die Nutzung des Schulverwaltungsrechners erfolgt durch folgenden Personengruppen:
☐ Leitung ☐ Sekretariat ☐ Lehrerkräfte ☐ Referendare ☐ sonstige (bitte benennen)

_____

☐ Hierfür wurde eine Rechteverwaltung installiert.

Private Rechner werden derzeit bei ____ Lehrkräften eingesetzt.
☐ Das Genehmigungsverfahren nach § 7 SchulDO wurde jeweils durchgeführt.

☐ Es werden EDV-Systeme zur Nutzung durch die Schüler bereitgehalten.
☐ Zahl der hierfür nutzbaren Rechner: _____
☐ Es wurde ein spezieller Computerarbeitsraum eingerichtet.
☐ Die Nutzung der Rechner durch Schüler(innen) erfolgt nur für Unterrichtszwecke.
☐ Schüler können die Rechner auch zu bestimmten Zeiten unbeaufsichtigt nutzen.
☐ Den Schülern ist auch eine private Nutzung der Rechner gestattet.
☐ Es besteht eine verbindliche EDV-Nutzungsordnung (bitte beifügen).

☐ Es besteht eine Videoüberwachungsanlage, für folgende Bereiche:
☐ Pausenhof ☐ Treppenhaus ☐ Spielplätze/Sportanlagen ☐ andere Bereiche
☐ Es erfolgt eine Aufzeichnung der Bilder.
☐ Die Löschung der Aufnahmen erfolgt automatisiert nach _____ Tagen.
☐ Die Vorabkontrolle wurde von unserem betr. DSB durchgeführt.

C. Umsetzung der rechtlichen Vorgaben

☐ Ein Datenschutzkonzept ist vorhanden.
☐ Es besteht ein IT-Sicherheitskonzept.
☐ Die Mitarbeiter werden durch Vorträge und Schulungen sensibilisiert.

Im letzten Schuljahr gab es _____ Anfragen zum Thema Datenschutz/IT-Sicherheit.

Im letzten Schuljahr gab es _____ Beschwerden zum Thema Datenschutz.

Die Beschwerden wurden von ☐ Mitarbeitern ☐ Schülern ☐ Eltern ☐ Dritten erhoben.

☐ Es gibt bei uns ein standardisiertes Verfahren zur Bearbeitung von Beschwerden.

☐ Die Verfahren automatisierter Datenverarbeitung sind nach § 3a KDO an den Diözesandatenschutzbeauftragten gemeldet worden.
☐ Die Meldung ist nach § 3a Abs. 3 KDO ist nicht erforderlich, weil
  ☐ ein betrieblicher Datenschutzbeauftragter bestellt wurde
  ☐ ausschließlich Daten für eigene Zwecke erhoben, verarbeitet und genutzt werden und zudem nicht mehr als 10 Personen ständig mit der Datenverarbeitung beschäftigt sind.
  ☐ Die Einwilligung der Betroffenen in die Datenverarbeitung liegt vor.

_____ _____
Datum Unterschrift