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

1. 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 2014 bis zum 28. Februar 2015

Vorgelegt im März 2015

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

Inhalt

Vorwort 3

1. Rechtsänderungen 4
1.1 Die neue Anordnung über den kirchlichen Datenschutz 4
1.2 Bestellung durch den (Erz-)Bischof 4
1.3 Organisation der Amtswahrnehmung 5

2. Informations- und Kommunikationstechnik 8
2.1 Einbettung von Drittanbietern auf kirchlichen Webseiten 8
2.2 Veröffentlichung von Fotos nach § 23 KunstUrhG 9
2.3 Zentrale Datenverarbeitung für zehn Beratungsstellen 10

3. Datenschutz in kirchlichen Einrichtungen 12
3.1 Videoüberwachung 12
3.2 „Custos“ Pfarreiverwaltung 15
3.3 Milieuanreicherung Meldedaten 16
3.4 Datenschutz in Schulen 16
3.5 Kindertagesstätten-Verwaltungsprogramm „KIDkita“ 17
3.6 Einsatz von „Little Bird Elternportal“ in Sachsen-Anhalt 17
3.7 Einsatz von Ki-ON in Kindertagesstätten des kath. Gemeindeverbandes Bremen 18

4. Öffentlichkeitsarbeit / Unterrichtung der Dienststellen 20
4.1 Internetauftritt 20
4.2 Broschüren, Handreichungen 20
4.3 Hinweise zum künftigen Einsatz von VoIP 21

5. Zusammenarbeit 23
5.1 Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands 23
5.2 IT-Workshop 24
5.3 Zusammenarbeit mit den Datenschutzbeauftragten und –referenten im Bereich der evangelischen Kirche Deutschlands 25
5.4 Zusammenarbeit mit den Datenschutzbeauftragten der Länder 25
5.5 Projektpartnerschaft im Virtuellen Datenschutzbüro 26

Vorwort

Der nachfolgende Tätigkeitsbericht schließt an den Bericht für die Zeit vom 01.01.2010 bis 28.02.2014, vorgelegt im Juli 2014, an. Bereits hier wurde mitgeteilt, dass die (Erz-)Diözesen von Berlin, Hildesheim und Osnabrück jeweils zum 01. März 2014 die Anordnung über den kirchlichen Datenschutz neu verkündet haben, während dies im Erzbistum Hamburg und im Offizialat Vechta zum 01. April 2014 und im Bistum Magdeburg zum 01. Mai 2014 vorgenommen wurde. Es wurde ausgeführt, dass trotz dieser leicht unterschiedlichen Verkündungstermine davon auszugehen sei, dass die Tätigkeit des Unterzeichners ab dem 01.03.2014 auf der neu geschaffenen gesetzlichen Grundlage erfolgt. Infolge dessen ist nach § 18 Abs. 3 KDO nunmehr jährlich ein Tätigkeitsbericht zu erstellen, der dem Bischof vorgelegt und der Öffentlichkeit zugänglich gemacht wird. Nach der vorhergegangenen Regelung war dies nur innerhalb eines Zeitraums von drei Jahren erforderlich. Im Vorwort des letzten Berichts hatte ich bereits angekündigt, für die Zukunft jeweils einen Jahresbericht für die Zeit vom 01.03. – 28.02. des Folgejahres anzufertigen. Ich gehe davon aus, dass die (Erz-)Bistümer, die erst einen oder zwei Monate später die KDO verkündet haben, diesen Zeitraum ebenfalls akzeptieren werden. Einwendungen hiergegen sind jedenfalls nicht erhoben worden.

Es kann vom Umfang und dem damit verbundenen Arbeitsaufwand kein Bericht erstellt werden, der die gesamte Tätigkeit des Diözesandatenschutzbeauftragten geschlossen darstellt. Statt dessen kann und will der Bericht über die wichtigen Fragen seiner Tätigkeit Auskunft geben und zudem auf künftige Tätigkeitsschwerpunkte hinweisen. Daher werden die Berichte von Jahr zu Jahr ein unterschiedliches „Profil“ aufweisen, das abhängig sein wird von den jeweils bearbeiteten Schwerpunktthemen, die sich immer wieder in anderer Form stellen werden.

Im Gegensatz zum letzten Bericht war der Unterzeichner während des gesamten Berichtzeitraums gesund und konnte seine Aufgabe im vollen Umfang ohne Einschränkungen wahrnehmen. Eine Vertretung durch eine andere Person war insoweit nicht erforderlich und ist auch nicht erfolgt.

Hannover, den 27.02.2015

Lutz Grammann
Diözesandatenschutzbeauftragter

1. Rechtsänderungen

1.1 Die neue Anordnung über den kirchlichen Datenschutz

Die Vollversammlung des Verbandes der Diözesen Deutschlands hat in ihrer Sitzung am 18.11.2013 beschlossen, den Ortsbischöfen der deutschen Diözesen den Erlass einer neuen Anordnung über den kirchlichen Datenschutz (KDO) zu empfehlen. Die norddeutschen Bistümer sind dieser Empfehlung gefolgt und haben in wörtlicher Übereinstimmung mit der Vorlage, die dem Beschluss der Vollversammlung vorgelegen hat, eine neue Anordnung über den kirchlichen Datenschutz in Kraft gesetzt. Die (Erz-)Diözesen von Berlin, Hildesheim und Osnabrück haben sie jeweils mit Wirkung zum 01.03.2014 in ihren Amtsblättern verkündet, das Erzbistum Hamburg und das Offizialat Vechta zum 01.04. und im Bistum Magdeburg zum 01.05.2014. Der Grund für den Neuerlass der KDO war die notwendige Anpassung an die Rechtsprechung des Europäischen Gerichtshofes zur Unabhängigkeit der Datenschutzaufsicht.[1] Hierdurch wurden die Bestimmungen über die Bestellung des Diözesandatenschutzbeauftragten (§ 16 KDO), seine Rechtsstellung (§ 17 KDO), seine Aufgaben nach § 18 KDO und die Möglichkeit, Verstöße zu beanstanden nach § 19 KDO wesentlich geändert.

1.2 Bestellung durch den (Erz-)Bischof

Staatliche Datenschutzbeauftragte werden heute zunehmend durch einen Beschluss des jeweiligen Parlaments gewählt, wodurch ihre Unabhängigkeit auch gegenüber der jeweiligen Regierung und deren Ministerien nach außen hin dokumentiert wird. Im kirchlichen Bereich besteht diese Möglichkeit nicht. Es bleibt also dabei, dass der Diözesandatenschutzbeauftragte wie bisher auch vom jeweiligen Bischof bestellt wird. Ein Grund für eine größere Abhängigkeit, als sie bei staatlichen Datenschützern gegeben ist, ist hierin nicht zu sehen. Das verhindert § 16 Abs. 3 KDO, nachdem der Widerruf der Bestellung vor Ablauf der Amtszeit nur möglich ist, wenn Gründe vorliegen, die nach § 24 des Deutschen Richtergesetzes bei einem Richter auf Lebenszeit dessen Entlassung aus dem Dienst rechtfertigen würden oder der Betreffende ein Verhalten zeigt, das nach der Grundordnung des kirchlichen Dienstes im Rahmen kirchlicher Arbeitsverhältnisse eine Kündigung rechtfertigen würde. Somit können nicht sachliche Gründe mit Bezug zur Amtswahrnehmung zum Entzug des Amtes führen, sondern lediglich Gründe, die sich aus einem rechtswidrigen persönlichen Verhalten ergeben. Ein Datenschutzbeauftragter, der sein Amt ordnungsgemäß ausführt, hat daher durchaus die Möglichkeit, auch im Widerspruch zur bischöflichen Behörde zu verfahren, ohne seine Entlassung befürchten zu müssen.

§ 17 Abs. 1 KDO legt zudem fest, dass er in Ausübung seiner Tätigkeit nicht an Weisungen gebunden und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen ist. Damit wird klargestellt, dass eine

[1] Urteil des Gerichtshofes der Europäischen Union C-518/07 vom 09.03.2010, Link zur vollständigen Fassung des Urteils auf www.datenschutz-kirche.de/eugh

Rechts- oder Fachaufsicht nicht stattfindet und die allgemeine Dienstaufsicht ausdrücklich so zu regeln ist, dass hierdurch seine Unabhängigkeit nicht beeinträchtigt wird (§ 17 Abs. 1 S. 3 KDO).

Die Amtszeit des Datenschutzbeauftragten ist von bisher drei auf vier bis acht Jahre verlängert worden. Auch hierdurch wird eine größere Unabhängigkeit erreicht, da die Beauftragung nicht schon nach einer relativ kurzen Amtszeit beendet werden kann. Die längere Amtszeit ermöglicht es dem Amtsinhaber sehr viel besser, ein eigenes Profil in der Wahrnehmung seiner Aufgaben zu entwickeln und bei den zu kontrollierenden Dienststellen auch durchzusetzen. Aus diesem Grund wird zu erwarten sein, dass die Auswahl an geeigneten Bewerbern für dieses Amt steigen wird.

Der Diözesandatenschutzbeauftragte soll zudem Jurist sein und die Befähigung zum Richteramt gem. § 5 Deutsches Richtergesetz vorweisen können. Damit hat die KDO eine klare Richtung angegeben, die das Amt des Datenschutzbeauftragten in erster Linie als juristische Tätigkeit sieht und die technischen Fragen, die sich in diesem Bereich ebenfalls stellen, nicht in den Vordergrund rückt.

Darüber hinaus muss er nunmehr auch sein Amt hauptamtlich verwalten, denn anderweitige Tätigkeiten, wie sie bisher bei vielen Datenschutzbeauftragten im kirchlichen Bereich ausgeführt wurden, dürfen die Unabhängigkeit und Unparteilichkeit nicht gefährden. Eine Tätigkeit in Ordinariaten oder Generalvikariaten sowie in Katholischen Büros dürfte mit der Anforderung nach § 16 Abs. 2 S. 4 KDO nicht zu vereinbaren sein.

Durch diese Grundsätze wird das Amt des Diözesandatenschutzbeauftragten in seiner Unabhängigkeit gegenüber dem Auftraggeber deutlich gestärkt.

1.3 Organisation der Amtswahrnehmung

Die Einschränkung der Unabhängigkeit des Datenschutzbeauftragten könnte auch durch Reduzierung der Finanzausstattung oder der Personalkosten erfolgen, die die Wahrnehmung seiner Aufgaben behindern würden. Auch hierzu hat die neue KDO nunmehr eindeutige Vorgaben geschaffen.

- Der Diözesandatenschutzbeauftragte verfügt über einen eigenen jährlichen Haushalt, der gesondert auszuweisen ist und veröffentlicht wird. Hierdurch wird eine Beeinträchtigung der Finanzierung einer angemessenen Personal- und Sachausstattung verhindert. Im Rahmen des ihm zur Verfügung stehenden Haushalts kann er eigenständig über die Sachausgaben entscheiden.

- Er hat Anspruch auf angemessene Personalausstattung, wobei er selbst das notwendige Personal auswählt, das von einer kirchlichen Stelle angestellt wird. Die Mitarbeiter unterstehen auch seiner Dienst- und Fachaufsicht und können nur mit seinem Einverständnis gekündigt, versetzt oder abgeordnet werden (§ 17 Abs. 4 KDO).

Eine praktische Regelung hierzu ist bisher nicht erfolgt. Dem Unterzeichner ist bisher noch kein Haushalt für das Jahr 2015 vorgelegt worden. Auch über die Art und Weise der Führung des Haushalts ist dem Unterzeichner bisher noch keine Entscheidung bekanntgegeben worden. Ein großes Problem sehe ich hierin nicht, da die norddeutschen Diözesen bisher sämtliche Sachkosten ohne Schwierigkeiten übernommen haben und im Jahre 2014 auch erhebliche Beträge zur Renovierung des Büros und für eine neue EDV-Ausstattung aufgewendet haben. Auch personell wurde durch die Einstellung eines Mitarbeiters für die Büroverwaltung, der halbtags tätig ist, eine Verbesserung der Aufgabenerfüllungen des Datenschutzbeauftragten zur Verfügung gestellt. Gleichzeitig wurde ihm die Möglichkeit eingeräumt, durch Inanspruchnahme eines externen Technikers, Herrn Dr. Todt von der Datenschutz Nord GmbH, auch die Bearbeitung technischer Fragen und Probleme, die sich im Datenschutz immer wieder stellen, angemessen zu bearbeiten. Insoweit sehe ich im Fehlen eines eigenständigen Etats nur eine Verzögerung, die sich aus der Notwendigkeit ergibt, hier erstmals praktikable Regelungen zu entwickeln. Ich gehe davon aus, dass dies im Jahre 2015 erfolgen wird.

Darüber hinaus muss meiner Ansicht nach eine verlässliche Vereinbarung über die anzustrebende Personalausstattung getroffen werden. Ich habe auf einer Konferenz mit IT-Leitern der Bistümer, den Datenschutzreferenten und den betrieblichen Datenschutzbeauftragten, eine Tischvorlage zur Diskussion vorgelegt. In ihr wird zwischen der passiven, reaktiven Tätigkeit des Datenschutzbeauftragten und einer aktiven Wahrnehmung des Amtes unterschieden und darauf hingewiesen, dass eine aktive Amtswahrnehmung deutlich mehr Maßnahmen im organisatorischen Bereich erfordert.

Um passive Wahrnehmung des Amtes handelt es sich immer dann, wenn der Anlass zur Tätigkeit von Außen gesetzt wird. Das ist beispielsweise dann der Fall, wenn sich jemand über die seiner Meinung nach unzulässige Datenverarbeitung durch eine kirchliche Dienststelle beschwert (§ 15 KDO), wenn er die bischöfliche Behörde oder sonstige kirchliche Dienststellen in Fragen des Datenschutzes berät (§ 18 Abs. 1 S. 3 KDO), wenn er Vorträge auf Anforderung von Verbänden hält oder auch einen Tätigkeitsbericht erstellt, zudem er nach § 18 Abs. 3 KDO verpflichtet ist. Hierfür ist der Personalbestand, wie er im Augenblick besteht, durchaus ausreichend. Eine aktive Wahrnehmung des Amtes, in dem eine Tätigkeit aufgrund eigener Entschlüsse vorgenommen wird, ist wesentlich aufwendiger. Schon das Anfertigen nach Außen hin wirkender Informationen, wie die einer Webseite, Arbeitshilfen oder Mustervorlagen, ist mit einem erheblichen Mehr an Arbeitsaufwand versehen. Aber auch die eigenständige Kontrolle von Dienststellen und Einrichtungen erfordert einen enormen Aufwand. Würde beispielsweise der Datenschutzbeauftragte bei sämtlichen Kindergärten eine Unterrichtung über die dort vorhandene EDV-Ausstattung, das Vorhandensein eines betrieblichen Datenschutzbeauftragten, anfordern, wäre dies bei der Vielzahl von Einrichtungen in sechs Bistümern schon ein enormer Aufwand bei der Erstellung der notwendigen Adressliste, was ohne einen Mitarbeiter, der allein für die

Erstellung einer entsprechenden Datenbank verantwortlich wäre, kaum geleistet werden könnte. Auch die Auswertung und Bearbeitung solcher Anfragen würde zeitlich eine enorme Arbeitszeit in Anspruch nehmen und wenn hieraus auch noch Prüfungstätigkeiten entwickelt werden sollen, ist das mit dem bisherigen Personalbestand nicht zu schaffen. Es muss in einer solchen Vereinbarung also die Frage geklärt werden, ob ein aktiver Datenschutz angestrebt wird und ob hierfür die notwendige Personalausstattung zur Verfügung gestellt werden kann. Meine Tischvorlage ist insoweit diesem Bericht im Anhang beigefügt.

An dieser Stelle mag ein kleiner Seitenblick erlaubt sein. Die Stabstelle Recht in einem der auftraggebenden Bistümer besteht aus der Leiterin, zwei Referentinnen und drei Mitarbeiterinnen für Sachbearbeitung und Sekretariat. Mit einer solchen Zahl wäre auch eine erheblich aktivere Wahrnehmung des Amtes des Datenschutzbeauftragten möglich.

Weitere Regelungen sind noch nicht konkret umgesetzt. So habe ich im Hinblick auf § 17 Abs. 6 KDO angefragt, ob ein juristischer Mitarbeiter der Datenschutz Nord GmbH für den Fall meiner Verhinderung als Vertreter bestellt werden kann, der unaufschiebbare Entscheidungen treffen könnte. Durch die Zusammenarbeit mit der Datenschutz Nord GmbH wäre er ohnehin über die aktuell wichtigen Fälle informiert. Ihm könnte zudem zeitweise ein Zugriff auf die Aktenverwaltung in der Cloud eingerichtet werden. Ich halte diese Maßnahme für die beste Lösung.

Neu geregelt wurde in der KDO auch, dass der Diözesandatenschutzbeauftragter oberste Dienstbehörde im Sinne von § 96 StPO und oberste Aufsichtsbehörde im Sinne von § 99 VwGO ist.

Die für das Amt des Diözesandatenschutzbeauftragten noch zu treffenden Ausführungsbestimmungen:

- Vereinbarung über die angestrebte Personal- und Sachausstattung
- Erstellung eines eigenen jährlichen Haushalts
- Vereinbarung darüber, von wem dieser Haushalt geführt wird. Soll hiermit ein Rendant beauftragt werden?
- Vereinbarung über die Bestellung eines Vertreters nach § 17 Abs. 6 KDO

2. Informations- und Kommunikationstechnik

2.1 Einbettung von Drittanbietern auf kirchlichen Webseiten

Immer wieder steht der Datenschutz vor der Frage, wie weit die Angebote von Drittanbietern wie Google, Facebook, Twitter u.a. in das eigene Webangebot mit einbezogen werden können. Aus Sicht des Datenschutzes besteht das Problem, dass hierbei auch der Programmcode des anderen Dienstanbieters in die eigene Webseite eingebunden und bei Aufruf ausgeführt wird. Hierbei werden dem Nutzer Cookies zur Verfügung gestellt, deren Nutzung nicht genau abschätzbar ist. Die Situation ist daher mit einer Einbindung von Social-Plugins zu vergleichen.

Der Techniker, der mit mir zusammenarbeitenden Datenschutz Nord GmbH, hat auf meine Anfrage folgendes ausgeführt:

> *„Die Problematik bei der Einbettung externer Dienste besteht darin, dass der Websitebetreiber nicht kontrollieren kann, welche Datenverarbeitungen des anderen Diensteanbieters (etwa YouTube) ausgelöst werden. Wird z.B. der YouTube Embedded Player genutzt, führt dies dazu, dass YouTube bei Aufruf der Website verschiedene Cookies setzt, deren Funktion unbekannt ist. Es ist zudem nicht auszuschließen, dass weitere Funktionen durch den eingebetteten Code ausgeführt oder nachgeladen werden. Hier besteht insbesondere die Gefahr, dass die Einbettung des externen Dienstes zu einer unzulässigen Datenverarbeitung – etwa einer unzulässigen Profilbildung - führt.*
>
> *Sofern belastbare Informationen darüber vorliegen, welche Funktionen und Datenverarbeitungen mit der Einbettung eines Dienstes einhergehen, muss sowohl der eingebettete Dienst als auch die mit der Einbettung einhergehende Datenverarbeitung in der Datenschutzerklärung aufgenommen werden. Es muss zudem sichergestellt werden, dass die Datenverarbeitung an sich datenschutzrechtlich zulässig ist und bleibt.*
>
> *Sofern die mit der Einbettung einhergehende Datenverarbeitung nicht belastbar festgestellt werden kann – was der Regelfall sein dürfte –, ist die Einbettung datenschutzrechtlich als überaus kritisch zu bewerten. Denn ein Websitebetreiber, der auf Seiten, die in seinem Verantwortungsbereich liegen, durch die Einbettung eine Datenverarbeitung in Gang setzt, die er nicht überblicken kann, ist nicht in der Lage:*
>
> *a) den Besucher seiner Website die für die Datenschutzerklärung erforderlichen Informationen zu stellen,*
> *b) auszuschließen, dass bereits der Aufruf seiner Website unzulässige Datenverarbeitungen – etwa unzulässige Profilbildungen – auslöst.*

> *Es ist daher empfehlenswert, in diesen Fällen auf die Nutzung der eingebetteten Dienste zu verzichten oder eine Lösung zu entwickeln, die der für Social-Plugins genutzten Zwei-Klick-Lösung entspricht. Insgesamt sind eine Anpassung der Datenschutzerklärung und die Darstellung der konkret mit dem Aufruf der Website verbundenen Datenverarbeitungen erforderlich."*

Im Hinblick auf diese Ausführungen wurde die verwendete Datenschutzerklärung überprüft und an einigen Stellen geändert. Hierin findet sich an vielen Stellen, wie beispielsweise bei Google Analytics bis hin zu Knight Lab, der Hinweis: „Welche Daten ein solches Plugin erfasst, kann von uns nicht beeinflusst werden". Weiterhin wird festgestellt: „Ebenso haben wir keinen Einfluss darauf, wie die Daten von (…) verwendet werden". Diese Angaben sind zutreffend und auch eine ausreichende Belehrung des Nutzers der Internetseite, so dass sich aus datenschutzrechtlicher Sicht keine Beanstandungen ergeben. Trotzdem muss es erlaubt sein die Frage zu stellen, ob wir uns wirklich bedingungslos den wirtschaftlichen Forderungen der Plugin-Anbieter zur Ausspähung der Nutzer unterwerfen wollen. Insoweit muss für jede Webseite eingehend die Frage gestellt werden, ob die Angebote der Drittanbieter wirklich erforderlich und für bestimmte Bereiche notwendig sind. Wenn dies nicht ordnungsgemäß begründet werden kann, sollte man auf sie verzichten.

In dem von mir zu beurteilenden Fall wurden eine Reihe überzeugender Gründe genannt, so dass sowohl die Einbindung wie auch die Hinweise in der Datenschutzerklärung unbeanstandet akzeptiert wurden.

2.2 Veröffentlichung von Fotos nach § 23 KunstUrhG

Nach § 23 des Kunsturheberrechtsgesetzes (KunstUrhG) dürfen Bildnisse ohne die erforderliche Einwilligung der abgebildeten Personen veröffentlicht werden, wenn es sich dabei um Bildnisse der Zeitgeschichte handelt.

Hierbei wurde früher zwischen absoluten und relativen Personen der Zeitgeschichte unterschieden. Absolute Personen der Zeitgeschichte standen durch ihr gesamtes Wirken dauerhaft im Blickpunkt der Öffentlichkeit, wie zum Beispiel eine Bundeskanzlerin oder berühmte Wissenschaftler. Um relative Personen der Zeitgeschichte handelte es sich dann, wenn die Person entweder nur für eine begrenzte Zeit oder in einem besonderen Zusammenhang den Blickpunkt der Öffentlichkeit bildete. Hierzu gehörten beispielsweise Schauspieler, Sänger, Sportler, Showgrößen aber auch Retter von verunglückten Bergleuten, die für eine kurze Zeit die Bewunderung der Öffentlichkeit erweckten. Für kirchliche Publikationen kam daher dieser Ausnahmetatbestand nur selten in Betracht.

Inzwischen hat der Bundesgerichtshof in Anlehnung an die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte[2] seine Rechtsprechung geändert und

[2] EGMR, Große Kammer, Urteil vom 07.02.2012, 40660/08 und 60641/08

die oben wiedergegebene Unterscheidung aufgegeben. Seither wird die Frage gestellt, ob ein historischer Bezug zur Zeitgeschichte vorliegt. Dabei ist eine Abwägung vorzunehmen zwischen der Meinungs- und Pressefreiheit und dem Persönlichkeitsrecht der betroffenen Person und es wird in den Bezug zur geschichtlichen Bedeutung keineswegs nur ein herausragendes Zeitgeschehen einbezogen. So hat der Bundesgerichtshof im Jahre 2014 entschieden:

> *„Der für die Frage, ob es sich um ein Bild aus dem Bereich der Zeitgeschichte handelt (§ 23 Abs. 1 Nr. 1 KunstUrhG) maßgebende Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinen gesellschaftlichen Interessen. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören (wie hier ein Mieterfest einer Wohnungsgenossenschaft).“*[3]

Damit werden sich auch Fragen, wie zum Beispiel die Veröffentlichung einer Schrift über die Geschichte eines Kindergartens und die Zustimmung der abgebildeten Personen zur Veröffentlichung von Lichtbildern in dieser Form anders stellen und anders zu beantworten sein, als bisher. Dabei wird jedoch für Printpublikationen in jedem Fall die Interessenabwägung zwischen geschichtlichem Interesse und Persönlichkeitsschutz sorgfältig vorzunehmen sein. Bei Internetveröffentlichungen sind die besonderen Gefahren der Internetpublikation mit der Möglichkeit des Missbrauchs nach § 23 Abs. 2 KunstUrhG besonders eingehend in Betracht zu ziehen, da hierdurch das berechtigte Interesse der abgebildeten Personen in besonderer Weise verletzt werden kann.

2.3 Zentrale Datenverarbeitung für zehn Beratungsstellen

Die Einrichtung einer zentralen Serverlösung für zehn Beratungsstellen im Bistum Osnabrück war schon mehrfach Gegenstand der Darstellung in den Tätigkeitsberichten. So wurde im Bericht 2004 – 2009 über die Planung einer zentralen Datenverarbeitung für zehn psychologische Beratungsstellen berichtet.[4] Der Bericht 2010 – 2014 machte deutlich, dass nunmehr eine Verschlüsselung der verarbeiteten Daten auch intern auf dem Zentralserver erfolgt, um die Verschwiegenheitspflicht der Berater nach § 203 StGB zu wahren.[5] Notwendig erschien jedoch noch eine Prüfung des Systems, die klären sollte, ob die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten getroffen worden sind. Nachdem nunmehr der Diözesandatenschutzbeauftragte die Möglichkeit hat, Mitarbeiter der Datenschutz Nord GmbH als externe Techniker zu seinen Prüfungen hinzuzuziehen, konnte 2014 eine Prüfung vor Ort stattfinden. Im letzten Tätigkeitsbericht wurde bereits darauf hingewiesen, dass dem Unterzeichner ausreichende Unterlagen zur eingesetzten Software SoPart EBuCO und auch eine ausführliche Verfahrensbeschreibung zur Verfügung gestellt worden sind. Nach Einarbeitung des Technikers, Herrn Cyl, in diese Unterlagen fand am 06.08.2014 der Prüfungstermin

[3] BGH, Urteil vom 08.04.2014, VI ZR 197/13
[4] siehe Tätigkeitsbericht 2004 – 2009, Kap. 3.6.2, Seite 28
[5] siehe Tätigkeitsbericht 2010 – 2014, Kap. 3.6.3, Seite 35

statt. Die gemeinsamen Feststellungen, die während dieses Termins getroffen wurden, und zudem eine telefonische Klärung offener Fragen mit dem Vertreter der Firma Trading Point und Herrn Sander vom Caritasverband, führten dann zur Erstellung eines Ergebnisberichts von Herrn Cyl, der mir am 27.08.2014 zugesandt wurde.

Der Bericht kommt überwiegend zu dem Ergebnis, dass die getroffenen Maßnahmen grundsätzlich angemessen sind, aber Verbesserungspotential aufweisen.[6] In dem Bericht wurde das Ergebnis zu den Punkten

5.1 Räumliche Sicherheit und Zutrittskontrolle,
5.2 Zugangskontrolle und Client-Sicherheit,
5.3 Rechteverwaltung und Mandantenfähigkeit,
5.4 Datenspeicherung und Zugriffskontrolle, sowie
5.5 Datenübermittlung und Weitergabekontrolle,

einzeln erörtert und mit einer Bewertung und Empfehlung dargelegt.

Mit Mail-Brief vom 04.09.2014 wurden die Mitarbeiter des Bistums Osnabrück gebeten, insbesondere die Empfehlungen des Berichts zu den gemeinsam genutzten Windows-Benutzerkonten und dem umgehenden Ersatz von Windows-XP-Rechnern sowie die Hinweise zur Verschlüsselung der Access-Datenbanken noch einmal eingehend in den Blick zu nehmen und hier möglicherweise die vorgeschlagenen Änderungen durchzuführen.

Kurz vor Abschluss des Jahresberichts hat das Bistum Osnabrück mit Schreiben vom 24.02.2015 mitgeteilt, dass der Austausch von Rechnern mit Windows XP durch neue Geräte mit dem Betriebssystem Windows 7 stattgefunden hat und abgeschlossen ist. Außerdem werde die Verwendung von Access-Datenbanken durch die Einrichtung eines SQL-Servers für SoPart EBuCO ersetzt. Dabei finde auch ein Wechsel vom Rechenzentrum des Diözesan-Caritasverbandes zur ITEBO GmbH statt. Ein erster Testlauf sei für Ende Februar, Anfang März dieses Jahres geplant. Aufgrund dieser Mitteilung, die auch von Herrn Cyl zustimmend zur Kenntnis genommen worden ist, ist das Bistum Osnabrück auf einem sehr guten Weg, eine sichere Datenverarbeitung für mehrere Beratungsstellen zu gewährleisten.

[6] siehe Ergebnisbericht zur Überprüfung der Informationssicherheit von SoPart EBuCO vom 27.08.2014, Zif. 1 Summary

3. Datenschutz in kirchlichen Einrichtungen

3.1 Videoüberwachung

Die Durchführung von Videoüberwachung innerhalb von Kirchen war ein wesentliches Schwerpunktthema während des zurückliegenden Jahres.

Aufgrund von Pressemeldungen hat der Diözesandatenschutzbeauftragte erfahren, dass in einer Kirchengemeinde in Hannover im Innenraum der Kirche eine Videoüberwachungsanlage installiert worden ist. Eine andere Kirchengemeinde, ebenfalls in Hannover, hat die vorhandene Anlage erneuert und wesentlich ausgeweitet. Dies gab Veranlassung, das Thema Videoüberwachung innerhalb eines Kirchengebäudes grundlegend neu zu bearbeiten.

Das Bundesverfassungsgericht hat in einem Urteil aus dem Jahre 2007[7] im Zusammenhang mit der Videoüberwachung öffentlicher Bereiche eine Diskussion entfacht. Zuvor war allgemein angenommen worden, dass eine optisch-elektronische Beobachtung für den Bürger in der Regel unschädlich sei. Solange er sich in einem Bereich bewege, der von einer Vielzahl anderer Menschen zur gleichen Zeit genutzt werde, könne er keine Intimsphäre in Anspruch nehmen und daher auch keine Maßnahmen zum Schutz seines informationellen Selbstbestimmungsrechts erwarten. Dieser Sichtweise hat das Bundesverfassungsgericht deutlich widersprochen. Es hat festgestellt, dass eine Videoüberwachung von einem öffentlichen Raum ein intensiver Eingriff von erheblichem Gewicht für die Rechte der Betroffenen darstellt. Es hat hierfür die folgenden Gründe angeführt:

1. Die Beobachtung bereite hoheitliche Maßnahmen vor, wie beispielsweise die Einleitung von Straf- und Bußgeldverfahren.
2. Sie beabsichtige die Lenkung des Verhaltens der Betroffenen.
3. Durch Aufzeichnung der Bilder sei eine nachträgliche Auswertung in vielfältiger Weise sowie eine Bearbeitung und Verknüpfung mit anderen Informationen möglich.
4. Zudem würden überwiegend Personen erfasst, die selbst keinen Anlass dafür geschaffen haben, sie zu beobachten.

Darüber hinaus führt eine Videoüberwachung innerhalb des Kirchenraumes nicht nur zu einer Beeinträchtigung des Persönlichkeitsrechts der Betroffenen sondern auch ihres Rechts auf ungestörte Religionsausübung, auf das sie nach Art. 4 Abs. 2 GG Anspruch haben. Die überwiegende Zahl der Menschen, die eine Kirche besuchen, tun dies, um ihren Glauben zu praktizieren. Dies geschieht häufig durch eine Begegnung mit Christus, der in Gestalt seines eucharistischen Leibes anwesend ist. Das geltende Kirchenrecht schafft hierzu einige grundlegende Bedingungen.

[7] Urteil des Bundesverfassungsgerichts - 1 BvR 2368/06 - vom 23.02.2007, Link zur vollständigen Fassung des Urteils auf www.datenschutz-kirche.de/bverfg

Die heilige Eucharistie darf nach Can. 934 CIC nur in einer Kirche aufbewahrt werden und Can. 935 CIC legt fest, dass es niemandem erlaubt ist, die Eucharistie bei sich aufzubewahren. Jeder Christ hat das Recht, innerhalb der Kirche vor dem heiligsten Sakrament beten zu können, was durch Can. 937 CIC ausdrücklich festgelegt wird. Insoweit hat die Kirche ein Monopol, das dazu führt, dass die Gläubigen nur hier Christi Gegenwart unmittelbar erleben, ihn verehren und anbeten können. Insoweit dürfte die Kirche im Wege der mittelbaren Drittwirkung auch zur Beachtung dieser Verfassungsbestimmung aufgefordert sein. Parallel hierzu bestimmt das Kirchenrecht in Can. 220 CIC: „Niemandem ist es erlaubt, das Recht irgendeiner Person auf Schutz der eigenen Intimsphäre zu verletzen."

Eine Überwachung des gesamten Kirchenraumes würde also die ungestörte Religionsausübung in gravierender Weise beeinträchtigen. In dem Moment, wo sich ein Gläubiger vielleicht flehend und weinend im Gebet an den anwesenden Christus wendet, muss er unbeobachtet bleiben. Der von den Verantwortlichen immer wieder genannte Grund, dann sei man eben gezwungen, die Kirche außerhalb der offiziellen Gottesdienstzeiten zu schließen, steht zudem noch im eindeutigen Widerspruch zu Can. 937 CIC und ist datenschutzrechtlich daher nicht zu berücksichtigen. Das entsprechende Kirchenrecht lautet in deutscher Übersetzung:

> Can. 937 CIC: Wenn kein schwerwiegender Grund dem entgegensteht, ist eine Kirche, in der die heiligste Eucharistie aufbewahrt wird, täglich wenigstens einige Stunden für die Gläubigen offenzuhalten, damit sie vor dem heiligsten Sakrament dem Gebet obliegen können.

Wenn man der Rechtsprechung des Bundesverfassungsgerichts folgt, setzt ein solch intensiver Eingriff von erheblichem Gewicht voraus, dass auch der Anlass so gewichtig ist, dass er die schutzwürdigen Interessen der betroffenen Personen überwiegt. In allgemeinen Veranstaltungen innerhalb der Kirche ist dies in der Regel nicht der Fall. Immer dann, wenn eine Nutzung der Kirche für Gottesdienste, Andachten oder auch für kulturelle Zwecke wie Konzerte, Vorträge oder ähnliches erfolgt, besteht keine Veranlassung anzunehmen, dass sich die Teilnehmer anders verhalten, als es dem Anlass entspricht.

Eine gesonderte Frage besteht darin, ob eine Videoüberwachung in der Zeit stattfinden kann, in der die Kirche unbeaufsichtigt ist. Eine Gesamterfassung des Kirchenraumes scheitert bereits daran, dass sie die kirchen- und verfassungsrechtlichen Maßgaben vollständig missachtet.

Für eine Teilüberwachung einzelner Bereiche müssen gravierende Gründe benannt und nachgewiesen sein, die eine Einschränkung des allgemeinen Persönlichkeitsrechts erfordern.

Kein ausreichender Grund besteht zum Beispiel dann, wenn es

1. nur um Bagatelldelikte, wie den Diebstahl von ein paar Münzen aus eingebauten Opferstöcken handelt, oder
2. wenn es um den Schutz des Eigentums der Kirchenbesucher geht, für den die Pfarrgemeinde keine Verantwortung trägt.

Wer zum Beispiel eine Speisegaststätte betritt, wird dort meistens durch einen schriftlichen Hinweis darüber belehrt, dass der Wirt keine Haftung für mitgebrachte Sachen, insbesondere die Garderobe des Gastes, übernimmt. Der Wirt ist nicht bereit und auch nicht im Stande, dem Besucher insoweit das „allgemeine Lebensrisiko“ abzunehmen. Auch für Pfarrgemeinden besteht keine Veranlassung, dies zu tun und sich dabei noch eventuellen Haftungsansprüchen auszusetzen. Darüber hinaus würde eine komplett videoüberwachte Gaststätte wohl auch niemand mehr betreten wollen.

Beachtenswerte Gründe sind sicherlich

1. die Gefahr massiver Beschädigungen bis hin zur Brandstiftung an einem Marienaltar, wie sie in einem der behandelten Fälle vorgekommen ist;
2. Gefahren für Kunstwerke, die aus bautechnischen Gründen nicht anders gesichert werden können.

In diesen Fällen ist die Videobeobachtung und -aufzeichnung auf den gefährdeten Raum zu beschränken und die Kirchenbesucher darauf hinzuweisen, dass die Altäre oder Kunstwerke speziell durch Videoüberwachung gesichert werden.

Auch die konkrete Anbringung von Videoüberwachungskameras gibt immer wieder Anlass zur Kritik. So hat eine Kirche zwei Videokameras an den Seitenwänden des Vorraums installiert, um Diebstähle aus Opferstöcken zu erschweren. Die Videokameras konnten das Geschehen jedoch nur von hinten beobachten, so dass durch die Aufzeichnung weder die Tat als solche zu sehen war noch Bilder zur Identifizierung des Täters beigebracht werden konnten. Auch die Videoüberwachung im Eingangsbereich der Kirche war so fehlerhaft angebracht, dass ein einfacher Blick zur anderen Seite ausreichte, um sich der Identifikation zu entziehen.

Der Diözesandatenschutzbeauftragte hat in einem Fall die Entfernung der gesamten Videoinstallation angeordnet.

Im zweiten zu beurteilenden Fall wurde die Gesamtbeobachtung des Kirchenraums abgeschafft und die Videokameras lediglich gezielt auf die beiden zu schützenden Altäre gerichtet. Diese Änderung wurde als ordnungsgemäß anerkannt.

**Datenschutzrechtliche Voraussetzungen
für die Videoüberwachung eines Kirchenraums:**

Unzulässig ist in jedem Fall

- die Videoüberwachung während der Messen oder anderer offizieller Veranstaltungen;
- die Erfassung des gesamten Kirchenraumes.

Zulässig kann eine Videoüberwachung sein, wenn

- einzelne Bereiche, die Altäre oder Kunstwerke enthalten, vor Beeinträchtigung geschützt werden sollen, und
- die Überwachung nur während der unkontrollierten Öffnungszeiten erfolgt;
- durch eine Installationsplanung sichergestellt wird, dass die mit ihr verbundenen Ziele auch tatsächlich erreicht werden können, und
- eine Vorabkontrolle nach § 3 Abs. 5 KDO stattgefunden hat, und
- die automatisierte Verarbeitung vor ihrer Inbetriebnahme dem Diözesandatenschutzbeauftragten nach § 3a KDO gemeldet worden ist.

3.2 „Custos“ Pfarreiverwaltung

Eine Firma Haneke aus Siegburg bietet eine Software für Pfarrgemeinden an. Dabei wurde ich angefragt, ob ich dieses Programm zertifizieren könnte, damit es den entsprechenden Gemeinden als datenschutzgerechte Software angeboten werden könnte. Allerdings sieht unsere Anordnung über den kirchlichen Datenschutz keine solche Zertifizierungsmöglichkeit vor. Ich hatte daher zu prüfen, ob eine Zertifizierung im Sinne des von Schleswig-Holstein praktizierten Datenschutzgütesiegels möglich ist. Das ist dann der Fall, wenn Schleswig-Holsteinische Einrichtungen als Nutzer dieses Programms in Betracht kommen. Selbstverständlich will die Firma Haneke ihr Programm auch Schleswig-Holsteinischen Gemeinden anbieten. Zum anderen besteht auch die Möglichkeit, eine Prüfung anhand des kirchlichen Rechts in Verbindung mit dem für kirchliche Einrichtungen geltenden staatlichen Recht durchzuführen. Als prüfende Stelle käme die Datenschutz Nord GmbH in Frage, die vom ULD Schleswig-Holstein als Zertifizierungsstelle für solche Verfahren anerkannt ist.

Es wäre eine wichtige und für den Datenschutz sehr nützliche Sache, wenn auch Programme, die speziell für den kirchlichen Bereich entwickelt worden sind, zertifiziert werden könnten. Eine solche Verfahrensweise wäre eine wesentliche Erleichterung für die abnehmenden Stellen, aber auch für die Datenschutzaufsicht, die in solchen Fällen schneller zu einer Genehmigung des Programms kommen könnte. Eine künftige Änderung der KDO sollte diesen Punkt aufnehmen.

Die Angelegenheit wird derzeit weiter verfolgt.

3.3 Milieuanreicherung Meldedaten

Bereits im Jahre 2010 hatte der Diözesandatenschutzbeauftragte ein Verfahren zur Milieuanreicherung von Meldedaten, die zum Zwecke kirchlicher Werbeanschreiben genutzt werden sollten, genehmigt. Auftragnehmer war seinerzeit die Firma Microm Consumer Marketing mit Sitz in Neuss, Auftraggeber das Bistum Hildesheim.

Nunmehr sollte das gleiche Verfahren für das Erzbistum Hamburg durchgeführt werden. Nach Anpassung der Verträge sowie der Datenschutzerklärung nebst Beschreibung der technisch-organisatorischen Sicherungsmaßnahmen von Seiten der Microm GmbH an die seinerzeit schon genehmigten Bestimmungen im Verfahren mit dem Bistum Hildesheim, konnte auch erneut eine Genehmigung erteilt werden.

3.4 Datenschutz in Schulen

Der Datenschutz in Schulen hat im Berichtszeitraum zunächst keine wichtige Rolle gespielt. Der Unterzeichner hat jedoch gegen Ende des Berichtsjahres ein Gespräch mit den Schulleitern im Bistum Hildesheim geführt. Zwar stand insgesamt nur eine Stunde hierzu zur Verfügung, diese Zeit hat jedoch einiges in Bewegung gebracht mit der Folge, dass der Schuldatenschutz im kommenden Jahr sicherlich ein Schwerpunktthema bilden wird.

Erster Punkt war die Bestellung eines betrieblichen Datenschutzbeauftragten für die allgemeinbildenden Schulen. Nach § 2a unserer Schuldatenschutzanordnung besteht hier lediglich eine „Kann“-Bestimmung, so dass Schulen, die insoweit keinen Betriebsbeauftragten bestellt haben, nicht rechtswidrig handeln. Auf der anderen Seite besteht ein Widerspruch zum geltenden Niedersächsischen Landesrecht, wonach kommunale Schulen Behörden sind und in jedem Fall einen behördlichen Datenschutzbeauftragten zu ernennen haben.[8] Der Diözesandatenschutzbeauftragte hat auf diesen Widerspruch hingewiesen und die Bistümer gebeten zu prüfen, ob hier nicht eine Änderung der Schuldatenschutzordnung erfolgen sollte. Gleichzeitig wurden auch die Schulleiter zu dieser Frage sensibilisiert.

Fehlt ein Schuldatenschutzbeauftragter, so sind die Datenverarbeitungsverfahren nach § 3a KDO dem Diözesandatenschutzbeauftragten zu melden. Solche Meldungen liegen bisher nicht vor. Lediglich die alten Meldungen nach § 17 Abs. 3 KDO-alt aus den Jahren 1992 und 1993 liegen vollständig vor, dabei ist nicht anzunehmen, dass die damaligen Verfahren noch mit den heutigen technischen Verfahren identisch sind. Insoweit ist für das nächste Berichtsjahr geplant, eine Erhebung der Verfahren zur Bearbeitung personenbezogener Daten durchzuführen.

Weiterhin angesprochen wurde das Thema Videoüberwachung und ebenfalls darauf hingewiesen, dass auch solche Verfahren meldepflichtig sind und zudem einer Vorabkontrolle nach § 3 Abs. 5 KDO unterliegen. Im kommenden Jahr wird auch hier

[8] § 8a Abs. 1 NDSG: „Jede öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet, hat eine Beauftragte oder einen Beauftragten für den Datenschutz zu bestellen.“

von Seiten der Diözesanaufsichtsbehörde eine allgemeine Erhebung über Videoüberwachung an Schulen durchgeführt werden.

Der zuletzt angesprochene Punkt betraf die Einbeziehung des Datenschutzes in den Schulunterricht. Schüler nutzen heute in großem Maße Internetangebote wie Soziale Medien, Chatsysteme und Kommunikationsprogramme, die alle auch erhebliche Risiken mit sich bringen. Es ist Aufgabe der Schule, Kinder zu veranlassen, mit diesen Themen für sich selbst aber auch für andere mit großer Verantwortung umzugehen. Erfreulicherweise wurde dem Unterzeichner gesagt, dass hier bereits eine Fülle von Veranstaltungen, auch unter Beteiligung externer Fachleute, durchgeführt worden sind. Für das kommende Berichtsjahr ist geplant, hier die Schulen um eine Auflistung ihrer Bemühungen bei der Unterrichtung von Kindern über die Gefahren des Internets zu bitten. Es ist dann geplant, im nächsten Bericht eine Übersicht über den Stand der Unterweisung auf kirchlichen Schulen darzulegen.

Von den Schulleitern wurde noch angeregt, eine Arbeitshilfe zum Verhalten im Internet zu veröffentlichen. Es wurde bekannt gegeben, dass bereits Vorbereitungen für eine solche neue Arbeitshilfe stattfinden würden und damit zu rechnen ist, dass sie im Laufe des nächsten Berichtsjahres erscheinen wird.

3.5 Kindertagesstätten-Verwaltungsprogramm „KIDkita“

Der Diözesancaritasverband Hildesheim hatte mir Mitte 2014 den Entwurf eines Rahmenvertrages sowie Musterregelungen für die Datensicherheit und den Datenschutz im Rahmen der Auftragsdatenverarbeitung der Firma COMRAMO IT Holding AG Hannover vorgelegt und um datenschutzrechtliche Prüfung gebeten. Gleichzeitig wurde ein Testzugang für die Cloud und das entsprechende Programm zur Verfügung gestellt. Da hier technische Fragen zur Sicherheit der Cloud-Datenverarbeitung, der Übertragung der Daten von den Einzelplatzrechnern zum Server sowie Maßnahmen zur Zugangskontrolle und Zutrittskontrolle wesentlich im Vordergrund standen, wurde von Anfang an der mir zur Verfügung stehende externe Techniker der Firma Datenschutz Nord GmbH, Herr Dr. Sascha Todt, in das Verfahren mit eingeschaltet. Nach erster Durchsicht der Unterlagen ergaben sich eine Reihe von klärungsbedürftigen Fragen, die vom Anbieter in einem umfangreichen Mailschreiben beantwortet worden sind. Von Herrn Dr. Todt wurde sodann im August 2014 eine Kurzstellungnahme zum Kindertagesstätten-Verwaltungsprogramm KIDkita-ASP erstellt.

3.6 Einsatz von „Little Bird Elternportal“ in Sachsen-Anhalt

Das Land Sachsen-Anhalt hat die Möglichkeit geschaffen, durch eine Software mit dem Namen „Little Bird Elternportal“ ein elektronisches Anmelde- und Platzvergabesystem für Kindertageseinrichtungen zu benutzen. Die Frage, die sich hierzu stellte, war die, ob kirchliche Kindergärten verpflichtet sind, sich an diesem Programm zu beteiligen oder ob dieses auch freiwillig möglich ist. Darüber hinaus entstand die Frage, ob die Verarbeitung personenbezogener Informationen der Kinder und ihrer Eltern nur mit

Einwilligung der Betroffenen möglich ist. Nach einer Vorprüfung ergab sich, dass weder im Sozialgesetzbuch noch in speziellen Kindertagesstättenregelungen ein Verfahren dieser Art gesetzlich angeordnet worden ist.

Zur Klärung der Angelegenheit wurde sowohl die evangelische Kirche wie auch der Landesbeauftragte für den Datenschutz Sachsen-Anhalt kontaktiert. Mit Schreiben vom 08.09.2014 hat der LfD Sachsen-Anhalt mitgeteilt, die Software im Jahre 2011 im Auftrag der Landeshauptstadt Magdeburg geprüft und dabei keine datenschutzrechtlichen Bedenken festgestellt zu haben. Rechtsgrundlage für die Datenerhebung und –verarbeitung im Rahmen einer ordnungsgemäßen Platzvergabe seien die Vorschriften aus §§ 62 Abs. 1, 64 Abs. 1 SGB VIII. Der Anspruch auf Kinderbetreuung richte sich dabei nach § 3 Abs. 4, 1 KiFöG, wobei die Landkreise und kreisfreien Städte als Träger der örtlichen Jugendhilfe anzusehen seien.

Über das Elternportal können Eltern eine Reservierung in einer KiTa vornehmen, wobei es sich um einen zusätzlichen Service handelt, der weiterhin auch die Möglichkeit einschließt, sich direkt in der Einrichtung anzumelden. Die Trägersoftware steht auch den Mitarbeitern der Träger und den Einrichtungen sowie den zuständigen Mitarbeitern des Jugendamtes zur Verfügung. Dabei sei durch die Schaffung von Zugriffsrechten auf Rollenbasis, verbunden mit einem Passwort, das nach erstmaliger Anmeldung am System geändert werden kann, gewährleistet, dass nur bestimmte Informationen abgerufen werden können. Mitarbeiter des Jugendamtes hätten mit der ihnen zugewiesenen Rolle keinen Zugriff auf personenbezogene Daten, sondern lediglich auf statistische Auswertungen.

Von Seiten der evangelischen Kirche wurde mitgeteilt, dass eine Freigabe des Kindergartenverwaltungsprogramms und Elternportals „Little Bird“ durch den Regionaldatenschutzbeauftragten der evangelischen Landeskirchen und Diakonien in Baden-Württemberg und Bayern erfolgt ist. Hierbei handelt es sich um die gleiche Software, die dort in gleicher Weise eingesetzt wird.

Nach Prüfung aller Informationen bestand keine Veranlassung, den Einsatz des Programms zu beanstanden. Es kann bei Kindertageseinrichtungen in Trägerschaft des Caritasverbandes für das Bistum Magdeburg eingesetzt werden.

3.7 Einsatz von Ki-ON in Kindertagesstätten des katholischen Gemeindeverbandes Bremen

Das Kindertagesstätten-Verwaltungssystem Ki-ON unterstützt Kindertagesstätten bei der Verarbeitung personenbezogener Daten der Kinder, ihrer Sorgeberechtigten und der Mitarbeiterinnen und Mitarbeiter der Einrichtung. Die Sicherheit des Systems wurde von der Datenschutz Nord GmbH geprüft und im Rahmen eines „Datenschutzkonzept [Ki-On] Entwurf für freie Träger“ im Auftrag der Senatorin für Soziales, Kinder, Jugend und Frauen der Freien und Hansestadt Bremen festgestellt. Der mir zur Beurteilung vorgelegte Vertrag zur Auftragsdatenverarbeitung nebst Anlagen mit dem Anbieter, der Firma Redlink Mediendienste GmbH, gab dieses

Datenschutzkonzept jedoch in keiner Weise wieder. Es fehlte an klaren Regelungen und eindeutigen Verpflichtungen, sowie an einer verbindlichen Verfahrensbeschreibung im Sinne der Anlage zu § 6 KDO. Die ursprünglichen Unterlagen entsprachen nicht den Anforderungen an eine Auftragsdatenverarbeitung nach § 8 KDO. Beide Seiten waren jedoch erfreulicherweise bereit, die zu treffende Vereinbarung entsprechend den Vorgaben über die Bestimmungen zur Auftragsdatenverarbeitung anzupassen. Zunächst wurde schriftlich mit dem katholischen Gemeindeverband in Bremen und der Firma Redlink eine rechtswirksame Vereinbarung vorbereitet und dann am 17.12.2014 in Bremen ein abschließendes Gespräch zwischen allen Beteiligten hierzu durchgeführt, das die vorher bestehenden Probleme beseitigt hat.

An der Bearbeitung der Sache, bei der vor allem technische Sicherheitsfragen im Vordergrund stand, war Herr Dr. Todt als externer Mitarbeiter für die technischen Fragen entscheidend mit beteiligt.

4. Öffentlichkeitsarbeit / Unterrichtung der Dienststellen

4.1 Internetauftritt

Im Tätigkeitsbericht für die Zeit vom 01.01.2010 bis 28.02.2014 wurde bereits angekündigt, die Seite „Veröffentlichungen“ mit dem Ziel eines schnelleren Auffindens benötigter Informationen umzugestalten. Dieses Vorhaben wurde im zurückliegenden Zeitraum verwirklicht. Anstelle des bisherigen Buttons „Veröffentlichungen“ ist nunmehr der Button „Themen“ getreten. Dort ist die angekündigte dreispaltig tabellarische Form verwirklicht worden. In der linken Spalte sind eine Fülle von Themen benannt, über die sich Mitarbeiter in den norddeutschen Diözesen informieren können. Im mittleren Bereich wird hierzu eine kurze Erläuterung und Einführung gegeben, während im rechten Feld Hilfsmittel benannt werden, die auf unserer Webseite oder auch durch Links zu anderen wichtigen Internetseiten aufrufbar sind.

Diese tabellarische Darstellung ist auch in weiteren Bereichen verwirklicht worden, so für die Darstellung wichtiger Gerichtsentscheidungen unter dem Button „Recht – Gerichtsentscheidungen“ und bei der Darstellung „Wir über uns“ und „Häufig gestellte Fragen“, so dass auch hier die Informationen schneller auffindbar sind.

Die Vorträge des Diözesandatenschutzbeauftragten wurden separat unter dem Button „Vorträge“ eingestellt und liegen nunmehr in einem PDF-Format vor.

Ein Versuch, betriebliche Datenschutzbeauftragte in den kirchlichen Dienststellen schneller über aktuell wichtige Themen zu informieren ist mit der Schaffung von zunächst zwei Newslettern unternommen worden. Seit Dezember 2014 gibt es einen Newsletter für betriebliche Datenschutzbeauftragte und IT-Verantwortliche in kirchlichen Dienststellen, sowie einen Newsletter für betriebliche Datenschutzbeauftragte in katholischen Krankenhäusern. Auf der Webseite selbst können diese Newsletter direkt bestellt und auch wieder abbestellt werden, wobei lediglich die Eingabe der E-Mail-Adresse, an die der Newsletter geschickt werden soll, und der Name der Einrichtung zwingend anzugeben sind.

4.2 Broschüren, Handreichungen

Im zurückliegenden Zeitraum wurden zwei wichtige neue Muster veröffentlicht:

1. Das Muster für die Durchführung einer Vorabkontrolle nach § 3 Abs. 5 KDO und
2. Ein Mustervertrag zur Vernichtung von Datenträgern nach der neuen DIN 66399

Zu Zif. 1 sieht die neue KDO nunmehr erstmalig die Durchführung einer Vorabkontrolle bei automatisierten Datenverarbeitungsverfahren in bestimmten, festgelegten Fällen vor. Sie ist immer dann durchzuführen, wenn besondere Arten von personenbezogenen Daten nach § 2 Abs. 10 KDO verarbeitet werden oder die Verarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens.

Verantwortlich für die Durchführung der Vorabkontrolle ist der betriebliche Datenschutzbeauftragte und nur dann, wenn ein solcher nicht bestellt worden ist, der Diözesandatenschutzbeauftragte. Um die Möglichkeit einer ordnungsgemäßen Durchführung der Vorabkontrolle zu schaffen, wurde eine Reihe von Prüfungspunkten formuliert, die in jedem Fall angemessen zu berücksichtigen sind. Sie umfassen die Beschreibung des geplanten Verfahrens, die Überprüfung der rechtlichen Zulässigkeit der geplanten Datenverarbeitung, die Überprüfung der Wahrung der Rechte der Betroffenen, den technischen Schutz des Systems einschließlich der Sicherung der Auftragsdatenverarbeitung und ermöglichen so eine abschließende Bewertung des Gesamtverfahrens aus datenschutzrechtlicher Sicht.

Hiermit wird ein wesentliches Hilfsmittel für die Arbeit der betrieblichen Datenschutzbeauftragten zur Verfügung gestellt.

Der Mustervertrag zu Zif. 2 wurde erforderlich, nachdem bereits im Oktober 2012 die DIN 66399 die alte DIN 32757 abgelöst hat. Anstelle der Vernichtung von Akten in Papierform wird nunmehr auf eine Norm zurückgegriffen, die sich auf die Vernichtung aller Datenträger, also auch CDs, Festplatten oder Speichersticks und viele andere mehr, anwendbar ist. Ich bin in einigen Fällen von Dienststellen, die mit sensiblen Daten oder solchen, die der strafbewährten Verschwiegenheitspflicht unterliegen, umzugehen haben, angesprochen worden, ob nicht für diese Fälle auch ein Mustervertrag vorliegt, der mit Aktenvernichtungsunternehmen abgeschlossen werden kann und der neuen DIN-Norm entspricht. Aus dieser Anforderung heraus wurde in relativ kurzer Zeit ein „Mustervertrag zur Vernichtung von Datenträgern mit sensiblen personenbezogenen Daten nach DIN 66399“ erstellt und veröffentlicht. Da hierbei auch technische Fragen zu berücksichtigen waren, wurde ergänzend die Beratung durch den externen technischen Mitarbeiter, Herrn Dr. Todt, in Anspruch genommen.

4.3 Hinweise zum künftigen Einsatz von VoIP

Die Deutsche Telekom hat angekündigt, bis zum Jahre 2018 alle ihre ISDN-Anschlüsse auf IP-Technologie umzustellen. Ein Telefongespräch über ein analoges Netz oder ISDN wird es dann im Bereich des wichtigsten deutschen Anbieters nicht mehr geben sondern nur noch über „Voice over Internet Protocol“ telefoniert werden können.

Aus Sicht des Diözesandatenschutzbeauftragten ergab sich daher die drängende Frage, ob solche Dienststellen und Einrichtungen, die nach Außen ein hohes Maß an Vertraulichkeit in Anspruch nehmen, wie zum Beispiel Beratungsstellen, auch dann noch im Stande sind, vertrauliche Gespräche mit Hilfesuchenden anzubieten. Aus diesem Grunde hatte ich meinen externen Technikbeauftragten, Herrn Dr. Todt, gebeten, in einem Kurzbericht die Punkte darzustellen, auf die kirchliche Anbieter bei Umstellung ihres Anschlusses achten sollten. Hieraus ist ein sechsseitiger „Kurzbericht: Sicherheit bei der Voice over IP-Telefonie (VoIP)“ hervorgegangen, der für alle Dienststellen auf unserer Webseite zur Einsichtnahme und zum Download zur

Verfügung steht. Dabei werden vor allem folgende Punkte bei der Umstellung des Netzes zu beachten sein:

1. Verfügbarkeit des Telefonie-Anschlusses durch Verfügbarkeit des Datennetzes
2. Maßnahmen gegen das unbefugte Mithören von Gesprächen, vor allem im Bereich des Anschlussinhabers selbst
3. Schaffung einer ordnungsgemäßen IP-Verwaltung unter Einbeziehung der VoIP-Komponenten und der Anbindung von „Best Practices“ zu ihrer Absicherung

5. Zusammenarbeit

5.1 Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands

Im Berichtszeitraum hat der Diözesandatenschutzbeauftragte an den Konferenzen vom 24.03.2014 in Bonn und 08./09.09.2014 in Berlin teilgenommen.

Bei der Konferenz in Bonn wurde über die Novellierung der KDO sowie Änderungen über die Einrichtung von Datenschutzbehörden diskutiert. Weitere Themen waren die Leitlinien zum sexuellen Missbrauch, die Kommunikation mithilfe von Sozialen Netzwerken sowie die Datensicherheit in Rechenzentren. Darüber hinaus wurde ein Gespräch mit Herrn Diethelm Gerhold, Direktor bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, geführt. Weiterhin wurde aus der Ständigen Arbeitsgruppe für Datenschutz–, Meldewesen- und Internetrecht und aus der Tätigkeit des Katholischen Büros Berlin berichtet.

Bei dem zweitägigen Treffen in Berlin berichtete die Ständige Arbeitsgruppe Datenschutz-, Melde- und Internetrecht über einen erneuten Anlauf zur Schaffung einer allgemein geltenden Fundraisingordnung für alle Bistümer und erläuterte den Sachstand zur Schaffung einer neuen Arbeitshilfe zur KDO.

Der neue EKD-Datenschutzbeauftragte, Herr Jacob, war als Gast anwesend und erläuterte die neuen Strukturen, bei denen 12 von 20 Landeskirchen die datenschutzrechtliche Zuständigkeit auf die EKD übertragen haben und 2015 noch vier weitere hinzukommen werden. Der Sitz dieser zentralen EKD-Datenschutzaufsicht ist in Hannover. Darüber hinaus gibt es vier weitere Regionen in Berlin (Ostbereich), Ulm (Südbereich), Dortmund (Westbereich) und Hannover (Nordbereich). Er erläuterte, dass die Außenstellen mit zunächst jeweils drei Personen besetzt werden sollen, wobei es sich um Juristen, Sachbearbeiter und Assistenten handelt.

Gleichzeitig wurde auch über die datenschutzrechtliche Entwicklung in den einzelnen Diözesen der katholischen Kirche berichtet. Derzeit ist ein Datenschutzzentrum in NRW für die fünf nordrheinwestfälischen Diözesen mit Sitz in Dortmund geplant. Für die Region Ost ist eine Behörde mit Sitz in Leipzig oder Halle vorgesehen, die von einem Volljuristen geleitet werden und weiteres IT-Personal beschäftigen wird. Diese Behörde wird auch für Berlin und Magdeburg zuständig sein, so dass sich der Zuständigkeitsbereich des Diözesandatenschutzbeauftragten entsprechend verringern würde.

Für die Region Süd ist nach Angaben von Herrn Dr. Fachet eine kirchliche Datenschutzbehörde für die Diözesen Freiburg und Stuttgart vorgesehen, für die vier Stellen geschaffen werden sollen. Sitz dieser Datenschutzbehörde soll Stuttgart sein.

Noch in den Anfängen steckt die Schaffung einer Datenschutzbehörde für die Region West, umfassend die Diözesen Trier, Speyer, Mainz, Limburg und Fulda.

Darüber hinaus wurden noch eine Fülle weiterer Themen wie Videoüberwachung in der Kirche, Soziale Netzwerke in Schulen, Zeiterfassungssysteme, den E-Post-Brief und die Datenerfassung bei der U3-Anmeldung zur Kinderbetreuung erörtert.

Wie immer bei Konferenzen in Berlin konnten wir den Berliner Datenschutzbeauftragten, Herrn Dr. Alexander Dix, und die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg, Frau Dagmar Hartge, begrüßen, die uns jeweils interessante Probleme aus ihrem Tätigkeitsbereich berichteten.

Die nächste Konferenz wird am 21./22.04.2015 im Priesterseminar in Fulda stattfinden.

5.2 IT-Workshop

Im Berichtsjahr haben zwei IT-Workshops am 24.07.2014 und 28.01.2015 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.

Beim 5. IT-Workshop im Juli 2014 hat auch Herr Wolfgang Fischer vom Kirchenamt der EKD, Koordinierungsstelle IT/Meldewesen, als Gast an der Konferenz teilgenommen. Es wurde vereinbart, ihn immer wieder einzuladen, wenn gemeinsame Themen aus dem Bereich der Technik, die von beiden Kirchen bearbeitet werden, erörtert werden. Auf der Konferenz standen vor allem die Einbindung mobiler Endgeräte in kirchliche Datenverarbeitungssysteme mit einem Vortrag von Herrn Dr. Todt und die Anforderungen an Mobile Device Management Systeme und Voraussetzungen für „Bring Your Own Device“ (BYOD) auf der Tagesordnung. Zudem stellte Herr Leppelt von der Qabel GmbH ein neu entwickeltes Konzept vor, mit dem die Vertraulichkeit und Authentizität bei der Datenübermittlung im Internet sichergestellt werden soll.

Auf dem 6. IT-Workshop in Hannover beinhaltete die Vorstellung der Cloud ID-Gard, die mit dem Verfahren „Trusted Cloud Data Protection“ (TCDP) zur Schaffung einer „Sealed-Cloud“ eingesetzt wird. Herr Dr. Rieken als Geschäftsführer des Anbieters Uniscon GmbH aus München stellte uns das Verfahren im Einzelnen vor. Dabei ergaben sich interessante Möglichkeiten des Einsatzes der Cloud-Verwaltung auch für die Speicherung von Daten, die der Verschwiegenheitspflicht nach § 213 StGB unterliegen. Dabei soll gewährleistet werden, dass kein Zugriff von dritter Seite, also weder für Dritte noch für Mitarbeiter des Rechenzentrums, möglich ist.

Ein weiteres wichtiges Thema war die geplante Umstellung des Telekom-Netzes auf IP-Telefonie. Herr Dr. Todt zeigte in einem Vortrag die hinzukommenden Gefährdungen und die notwendigen Maßnahmen, die zu ihrer Vermeidung getroffen werden müssen.[9]

Als nächsten Termin für den kommenden IT-Workshop wurde der 15.07.2015 in Hannover festgelegt.

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

Durch die wesentlichen Änderungen an der Datenschutzaufsicht innerhalb der evangelischen Kirche wird die Konferenz der Datenschutzbeauftragten in den Gliedkirchen der evangelischen Kirche in Deutschland künftig nicht mehr stattfinden. Die letzte Konferenz dieser Art hat daher am 08./09.05.2014 wie gewohnt in Berlin stattgefunden. Selbstverständlich war der Unterzeichner als Gast auf dieser Konferenz anwesend. Für die Zukunft sind wohl nur noch Zusammenkünfte des Datenschutzbeauftragten der EKD mit den jeweiligen Leitern und Mitarbeitern der Außenstellen geplant.

Eine sehr gute Zusammenarbeit hat sich mit der Koordinierungsstelle IT/Meldewesen des Kirchenamts der EKD in Hannover ergeben. Der Leiter, Herr Wolfgang Fischer, hat mich in umfangreicher Form über die Unterlagen zur mobilen Datenverarbeitung und zum Einsatz von MDM-Systemen informiert, die für die katholische Kirche ebenso von Bedeutung sind. Auch hat er an einem unserer IT-Workshops teilgenommen, so dass auch für die Zukunft eine vertrauensvolle und sinnvolle Zusammenarbeit möglich ist.

Der Unterzeichner hat auch am 05.06.2014 als Gast an der Referentenkonferenz für Datenschutz, Meldewesen und Kirchenmitgliedschaftsrecht im Kirchenamt der EKD teilgenommen. Hierbei stand die Umsetzung der Novellierung des Datenschutzgesetzes der EKD, die Bestellung von Betriebs- und örtlich Beauftragten für den Datenschutz und das neue OSCI-XMeld-Verfahren im kirchlichen Meldewesen zur Diskussion. Die kommende Sitzung der Referentenkonferenz soll am 10.06.2015 erneut im Kirchenamt der EKD in Hannover stattfinden, zu der sich der Unterzeichner bereits angemeldet hat.

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

[9] siehe auch Zif. 4.3, Seite 21

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 beiden 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 mich weitergeleitet. Dabei wird der Betroffene über die 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 Berichtszeitraums 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 2014 auf 41.760,00 EUR belaufen und werden im Jahre 2015 voraussichtlich 41.412,00 EUR betragen.

In der Sache selbst ist eine völlige Umgestaltung, also ein Relaunch, der Webseite geplant, die künftig am Datenschutz interessierte Bürger als Zielgruppe der Nutzung der Webseite sieht. Bürger, die sich mit Datenschutz beschäftigen, ihre eigene Computer- oder mobile Nutzung gegen fremde Eingriffe absichern wollen, oder insoweit schon selbst geschädigt worden sind, sollen mit entsprechenden Angeboten konfrontiert werden. Hierbei werden nicht nur Unterlagen des Virtuellen Datenschutzbüros zur Verfügung gestellt sondern es werden auch andere öffentliche Webseiten, wie beispielsweise www.bsi-fuer-buerger.de, www.klicksafe.de, www.bfdi.bund.de, www.youngdata.de und www.irights.info verlinkt. Auch die Projektpartner werden die Möglichkeit haben, sich in einem Themenbereich vorzustellen und auf ihre Angebote zu verweisen. Der Unterzeichner hat an den entsprechenden Tagungen zur Projektentwicklung teilgenommen.

Die bisher letzte Sitzung der Projektpartner hat am 24.02.2015 stattgefunden, wie beim letzten Mal wiederum im Niels-Stensen-Haus in Hannover, in einem der dort zur Verfügung stehenden Vortragsräume.

Die Tätigkeit, einschließlich der anstehenden Neuorganisation der Webseite wird weiter fortgesetzt.

Tischvorlage zu TOP 3
Neuordnung der Datenschutzaufsicht in den norddeutschen Bistümern

IT-Workshop am 28.01.2015 in Hannover

Passive Amtsführung Tätigkeit des DSB erfolgt auf Grund von Anforderungen durch Dritte	**Aktive Amtsführung** Tätigkeit des DSB auf Grund eigener Initiativen
Aufgaben: • Beantwortung von Anfragen der Dienststellen - § 18 I S. 3 • Beratungen von Dienststellen zur Datenschutzorganisation - § 18 I S. 3 • Bearbeitung von Beschwerden - § 15 • Prüfungen auf Grund von Beschwerden oder bestimmten Vorfällen • Vorträge und Schulungen auf Einladung der Veranstalter • Erstellung von Gutachten und Berichten - § 18 I S. 4 • Tätigkeitsbericht - § 18 III • Zusammenarbeit mit anderen kirchlichen oder staatlichen Datenschutzbeauftragten - § 18 IV, V	**Aufgaben:** • Infomaterial veröffentlichen (Webseite, Arbeitshilfen, Muster, Newsletter) • Anforderungen zur Vorlage von Meldungen nach § 3a I • Empfehlungen zur Verbesserung des Datenschutzes - § 18 I Satz 2 • Durchführung von Prüfungen nach allgemeinen Kriterien • Anbietung eigener Veranstaltungen • Aktive Mitarbeit in Gremien und Ausschüssen • Zusammenarbeit mit anderen kirchlichen oder staatlichen Datenschutzbeauftragten - § 18 IV, V
Organisatorische Anforderungen: • Ordnungsgemäßes Büro (Erreichbarkeit postalisch, telegraphisch und elektronisch) • Sachbearbeitung (Texterstellung, Aktenverwaltung, Literatur, Internetzugang) • Begrenzte Reisetätigkeit	**Organisatorische Anforderungen:** • Ordnungsgemäßes Büro (Erreichbarkeit postalisch, telegraphisch und elektronisch) • Sachbearbeitung (Texterstellung, Aktenverwaltung) • Erweiterte Reisetätigkeit • Datenverarbeitung (z.B. Verzeichnis aller Dienststellen und Einrichtungen im Bereich der Zuständigkeit, einschließlich Caritas) • Anschluss an den elektronischen Schematismus

Personelle Anforderungen:	Personelle Anforderungen:
• 1 x Diözesandatenschutzbeauftragter • ½ x Büroleiter(in) / Sekretär(in) • ½ x IT-Mitarbeiter oder Möglichkeit zur Verpflichtung im Bedarfsfall	• 1 x Diözesandatenschutzbeauftragter • 1 x Büroleiter(in) / Sekretär(in) • 1 x IT-Mitarbeiter • 1 x weiterer Sachbearbeiter (mindestens)