1. Tätigkeitsbericht des Diözesandatenschutzbeauftragten der ostdeutschen Bistümer

gemäß § 18 Abs. 3 KDO

Berichtszeitraum 01.01.2016 bis 31.12.2016

Inhaltsverzeichnis

Abkürzungsverzeichnis

APuZ	Aus Politik und Zeitgeschichte
ArztR	Arzt Recht
BAD	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGH	Bundesgerichtshof
BGHZ	Entscheidung des Bundesgerichtshofes im Zivielsachen
BVerfGE	Bundesverfassungsgerichtsentscheidung
DKWW	Däubler, Klebe, Wedde, Weichert
DMW	Deutsche Medizinische Wochenschrift
DuD	Datenschutz und Datensicherheit
KDO	Kirchliche Datenschutzordnung
KuR	Kirche und Recht
LG	Landgericht
MdEP	Mitglied des Europaparlamentes
NJW	Neue Juristische Wochenschrift
NStZ	Neue Strafrecht Zeitschrift
OLG	Oberlandesgericht
StGB	Strafgesetzbuch
ZD	Zeitschrift für Datenschutz
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für Strafrechtswissenschaften

1. Einleitung

1.1. Warum Datenschutz

Der Begriff „Datenschutz“ wurde das erste Mal als Gesetzesbegriff im (weltweit) ersten Landesdatenschutzgesetz verwendet, das 1970 in Hessen verabschiedet worden ist. 1977 folgte das erste Bundesdatenschutzgesetz. Seinerzeit ging es noch in erster Linie um den Substanzerhalt der Daten und damit um den Schutz der Daten gegen Wegnahme, Zerstörung, Manipulation u.ä. Dieser Aspekt der Datensicherheit ist auch heute noch ein Teilgebiet des Datenschutzes.

Aber es bestand schon immer Einigkeit darüber, dass nicht nur die Daten als solche und schon gar nicht um ihrer selbst willen geschützt werden sollen, sondern das Persönlichkeitsrecht eines jeden Einzelnen.[1] Letzten Endes sollen also durch den Datenschutz nicht in erster Linie die Daten, sondern die Menschen geschützt werden. Geschützt werden soll die Privatsphäre und damit alle Lebensbereiche. Auch die Spuren, die jemand aufgrund von Verpflichtungen oder freiwillig über sich in der Lebensumwelt hinterlässt, indem er bspw. Eintragungen in Datenbanken vornimmt oder auf seiner eigenen Website Informationen über sich einstellt, unterfallen dieser geschützten Privatsphäre.[2]

Es geht darum, dass auch in einer digitalisierten Welt jeder selber entscheiden können muss, wer etwas über ihn weiß, was mit diesen Daten gemacht wird und welche möglichen Auswirkungen damit verbunden sind.[3] Der Schutz der Daten dient dazu, die Persönlichkeit des Einzelnen durch die informationelle Selbstbestimmung, wie es in dem grundlegenden Urteil des Bundesverfassungsgerichtes zur Volkszählung genannt wird, zu gewährleisten.

Dieses Recht leitet das Gericht direkt aus den Artikeln 2 Abs. 1 i.V.m. 1 Abs.1 des Grundgesetzes ab.[4] Aufgabe des Datenschutzes ist es also, die grundgesetzlich geschützte freie Entfaltung der Persönlichkeit zu gewährleisten, weil Selbstbestimmung eine elementare Funktionsbestimmung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist. „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert werden, wird versuchen, nicht

[1] § 1 BDSG, § 1 KDO
[2] Taeger, Datenschutzrecht S. 54
[3] Jan-Philipp Albrecht, MdEP, Die Datenschutzreform der Europäischen Union S. 7
[4] Urteil des Bundesverfassungsgerichtes BVerfGE 65,1 vom 15.12.1983

durch solche Verhaltensweisen aufzufallen. … Dies würde deshalb nicht nur die individuellen Entfaltungschancen des Einzelnen beinträchtigen, sondern eben auch das Gemeinwohl.“ [5]

Datenschutz war lange Zeit als ein Abwehrrecht gegen den Staat verstanden worden, da Daten vornehmlich über das öffentliche Melde- und Steuerwesen und die Polizei in den öffentlichen Verwaltungen akkumuliert wurden. In der totalitären Zeit des Nationalsozialismus wurde das Missbrauchspotential derartiger Datensammlungen deutlich, da seinerzeit die Melderegister dazu missbraucht wurden, die planmäßige Vernichtung der Juden und anderer gesellschaftlicher Gruppen zu unterstützen. Im demokratischen System aber können die Ansprüche auf Wahrung des Datenschutzes und der Persönlichkeit vom Bürger durch die Kontrolle der staatlichen Stellen und nicht zuletzt durch Wahlen beeinflusst werden.

Nunmehr ist durch das Internet eine Veränderung eingetreten, die zu einer Machtkonzentration bei einigen großen Wirtschaftsunternehmen geführt hat.[6] Eine Kontrollmöglichkeit für den Betroffenen ist dort ohne gesetzliche Regelung nicht möglich. Dazu beigetragen hat insbesondere eine sich wandelnde Einstellung der Gesellschaft im Umgang mit personenbezogenen Daten. Die freiwillige und umfangreiche Preisgabe von Daten speziell in sozialen Netzwerken steht dem Ideal des Datenschutzgesetzes, der Anonymität, entgegen.[7]

Datenschutz ist deshalb jetzt wichtiger denn je.

Die zunehmende Transparenz des Einzelnen durch die Abgleichung von Datensammlungen eröffnet Unternehmen die Möglichkeit, neben Direktmarketing jeden Bürger vornehmlich mit bestimmten, auf ihn zugeschnittenen Informationen zu versorgen und damit eine Engführung der Informationen zu erreichen. Die selektive Bereitstellung von Informationen bedeutet deshalb Manipulation, bedeutet Lenkung des Einzelnen, auf eine subtile Art mit Hilfe der von ihm selber zur Verfügung gestellten persönlichen Daten. Informationsfreiheit kann aber nur bestehen, wenn gewährleistet ist, dass dem Einzelnen Informationen ungefiltert zukommen.

Die Aufgabe des Datenschutzes besteht deshalb zunehmend darin, nicht nur rückwärtsgewandt personenbezogene Daten weiterhin geheim zu halten, sondern

[5] BVerfGE, 65,1, (43)
[6] Google beherrscht ca. 95% der Suchanfragen
[7] Lewinski Zur Geschichte von Privatsphäre und Datenschutz … S. 31

vorwärts gerichtet das Persönlichkeitsrecht eines jeden zu respektieren, indem ihm die Möglichkeit eingeräumt wird, sich frei und unbeeinflusst zu informieren. Einem so verstandenen Datenschutz kann der häufig gehörte Einwand „ich habe nichts zu verbergen“ nicht entgegengehalten werden, weil es eben nicht nur darum geht, etwas zu verbergen, sondern darum etwas zu erfahren, das andere verbergen wollen, indem sie Informationen nur gefiltert bereitstellen.

Aufgabe des Datenschutzes ist es in diesem Sinne für Transparenz zu sorgen. Die vermeintlich freiwillige Herausgabe von persönlichen Daten, ohne die ein Zugang zu den modernen Kommunikationswegen, wie z. B der sozialen Netze nicht möglich ist, ist zu hinterfragen. Die persönlichen Daten, die dort abgefragt werden, obwohl sie mit dem bereitgestellten Dienst nichts zu tun haben, sind das Entgelt für die scheinbar kostenlose Aufnahme in den Kreis der Nutzer, deren persönliche Daten durch Bereitstellung und Verkauf an Dritte zu Geld gemacht werden. Datenschutz muss vermeiden, dass in Zukunft nur noch solche Menschen ihre Autonomie bewahren können, die es sich leisten können für solche Dienste mit Geld statt mit Daten zu bezahlen[8]. Nur wenn der Nutzer ausdrücklich darauf hingewiesen wird, an wen seine Daten zu welchem Zweck weitergeleitet werden, kann von einer wirklich freiwilligen Hergabe dieser Daten gesprochen werden. Datenschutz hieß schon bislang ein Informationsgleichgewicht, eine Informationsbalance zu gewährleisten. Aufgabe des Datenschutzes kann es nicht sein, die Bürger dazu aufzufordern sich den modernen Kommunikationswegen zu verweigern. Es geht vielmehr darum, ein transparentes, rechtliches und sozioökonomisches Umfeld zu schaffen, indem das Teilen von Daten nicht zu Manipulation und Ausbeutung führt.[9]

1.2. Die Europäische Datenschutzgrundverordnung

Die EU-Datenschutzgrundverordnung (EU-DSGVO) wurde vom Europäischen Parlament am 14. April 2016 verabschiedet und am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht. Gem. Art. 99 Abs. 2 EU-DSGVO gilt diese ab dem 25.05.2018 in allen Mitgliedstaaten. Nach der EU-DSGVO verbleiben jedoch Regelungsspielräume und Gesetzgebungsaufträge für die einzelnen Nationalstaaten. Die Gesetzgeber von Bund und Ländern sind deshalb aufgefordert, bis zum Geltungsstichtag eine Reihe von Anpassungen und Änderungen des jeweiligen nationalen Rechts vorzunehmen. Die geltende Struktur

[8] Wewer ZRP 2016, 23
[9] Evgeny Morozov, in „Big Data“ APuZ 11-12/2015 S. 7

wird auch unter dem europäischen Recht beibehalten. Es ist deshalb davon auszugehen, dass der Datenschutz nun in allen Staaten der Europäischen Union ein gleiches Niveau erreicht.[10]
Gleichzeitig jedoch erfährt der Datenschutz durch Verschärfungen der Sicherheitspolitik infolge von Terroranschlägen und mit der fortschreitenden Digitalisierung von Wirtschaft und Gesellschaft zusätzliche Bewährungsproben.
Insbesondere das geplante Videoüberwachungsverbesserungsgesetz steht in der Kritik der Datenschützer.

1.2.1. Neue Regelungen durch die EU-Datenschutzgrundverordnung (EU-DSGVO) in Bezug auf die Kirchen

Die entscheidende Rechtsvorschrift der EU-Datenschutzgrundverordnung für die Kirchen ist in Art. 91 EU-DSGVO festgelegt und lautet:
Abs. 1 Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedsstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regelungen zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.
Abs. 2
Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, unterliegen der Aufsicht einer unabhängigen Aufsichtsbehörde, die spezifischer Art sein kann, sofern sie die in Kapitel VI niedergelegten Bedingungen erfüllt.

Damit wird den Kirchen und religiösen Vereinigungen oder Gemeinschaften unter bestimmten Voraussetzungen ein eigenständiger kirchlicher Datenschutz gewährleistet. Allerdings werden durch die EU-Datenschutzgrundverordnung (EU-DSGVO) für den ganzen Bereich der Europäischen Union einheitliche Standards formuliert, die auch für den kirchlichen Bereich gelten, bzw. damit „in Einklang“ zu bringen sind. Dabei ist Einklang nicht gleichbedeutend mit Konformität. Vielmehr darf das kirchliche Datenschutzrecht zu den Grundentscheidungen der Verordnung nicht in Widerspruch stehen.[11] Auch nach der EU-Datenschutzgrundverordnung kommt dem staatliche Datenschutzrecht gegenüber

[10] Presseerklärung der Bundesbeauftragten für Datenschutz und Informationsfreiheit Ausgabe 9/2016 vom 02.05.2016
[11] Ziegenhorn / Aswege KuR 2/2015 S. 209

dem kirchlichen Datenschutzrecht nur eine Auffangfunktion zu, die verhindert, dass es datenschutzfreie Räume gibt.[12]

2. Das Recht der Kirchen den Datenschutz selber zu regeln

Der Datenschutz rückt immer mehr in den Fokus der Öffentlichkeit. Dies betrifft besonders auch das Privileg der Kirchen, Datenschutzordnungen in eigener Regie zu erlassen und den Datenschutz außerhalb staatlicher Kontrollgremien zu gewährleisten. U.a. wurde diese Tatsache bei meinem Besuch einer Landesdatenschutzbeauftragten massiv hinterfragt und angekündigt, dass man, ggf. auch gerichtlich, prüfen werde, ob für Einrichtungen der Kirche außerhalb des verfassten Bereiches das Selbstbestimmungsprivileg Bestand haben kann.

Gem. Art. 140 GG i.V.m. Art. 137 Abs. 3 Weimarer Reichsverfassung (WRV) gilt: Jede Religionsgemeinschaft ordnet und verwaltet ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes. Das kirchliche Selbstbestimmungsrecht, das durch diese Vorschriften zum Ausdruck kommt, begrenzt somit die Geltung staatlicher Regelungen.
Nach der ständigen Rechtsprechung des Bundesverfassungsgerichtes „sind nicht nur die organisierte Kirche und deren rechtlich selbständige Teile, sondern alle der Kirche in bestimmter Weise zugeordneten Einrichtungen ohne Rücksicht auf ihre Rechtsform Objekte, bei deren Ordnung und Verwaltung die Kirche grundsätzlich frei ist, wenn die Einrichtungen nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend berufen sind, ein Stück des Auftrages der Kirche wahrzunehmen und zu erfüllen. … [dabei] genügt, ... dass die in Frage stehende Einrichtung der Kirche so nahesteht, dass sie teilhat an der Verwirklichung eines Stücks Auftrags der Kirche im Geist christlicher Religiosität.[13]“
Damit sind vor allem Einrichtungen im sozialen Bereich (Caritas, Kindergärten, Schulen, Krankenhäuser u.a.), auch wenn sie als juristische Personen des privaten Rechts organisiert sind, in das Selbstbestimmungsrecht der Kirche einbezogen, wenn die Kirche sie in die Reichweite ihres Selbstbestimmungsrechtes einbezieht[14]. Art 140 GG i.V.m. Art 137 WRV garantieren der Kirche die Kompetenz, selber festzulegen, wie weit ihre Angelegenheiten reichen[15]. Eine Differenzierung danach, ob die jeweilige Einrichtung zum Kernbereich der Kirche

[12] Ebd. S. 205, 209
[13] BVerfGE 53, 366 (391, 392)
[14] Ziegenhorn / Aswege KuR 2/2015 S. 199
[15] BVerfGE 53, 391

gehört (bzw. verkündigungsnahe Tätigkeiten ausübt) oder nach der Organisationsform[16], widerspricht dem verfassungsrechtlich garantierten Selbstbestimmungsrecht der Kirche[17]. An diesem Ergebnis wird sich grundsätzlich auch durch die neue EU-Datenschutzgrundverordnung nichts ändern. Durch den Vorrang dieser Verordnung vor nationalen Rechtsnormen, wird die Selbstbestimmung der Kirchen zukünftig nicht mehr durch die Regelungen des Art. 140 GG i.V.m. Art. 137 WRV geregelt, sondern durch Unionsrecht (s.o.).

3. Datenschutz der EKD

Der Beauftragte für den Datenschutz der EKD (BfD EKD) nimmt die im EKD-Datenschutzgesetz normierte Datenschutzaufsicht für die EKD, für das Evangelische Werk für Diakonie und nach vertraglicher Übertragung für 16 Gliedkirchen, die Zusammenschlüsse und im Bereich von sechs diakonischen Landesverbänden wahr. Zur Wahrnehmung der gesetzlich normierten sowie der vertraglich übertragenen Aufgaben der Datenschutzaufsicht existiert seit Anfang 2014 – in der Rechtsform einer unselbständigen Einrichtung der EKD - die unabhängige und eigenständige Behörde „Der Beauftragte für den Datenschutz der EKD (BfD EKD)“. Diese Behörde wird von der Person des Beauftragten geleitet und hat ihren Hauptsitz in Hannover. Vier Gliedkirchen und mehrere diakonische Landesverbände nehmen die Datenschutzaufsicht weiterhin eigenständig wahr.

Zur regionalen Gliederung der vertraglich auf die EKD übertragenen Datenschutzaufsicht in den Gliedkirchen und diakonischen Landesverbänden wurden die vier Datenschutzregionen Nord, Ost, Süd und Mitte-West gebildet. In jeder Datenschutzregion wurde eine Außenstelle errichtet (Nord: Hannover; Ost: Berlin; Süd: Ulm; Mitte-West: Dortmund).

[16] Dammann in Simitis Bundesdatenschutzgesetz § 2 Rn. 108 ff.
[17] Preuß, Das Datenschutzrecht der Religionsgemeinschaften ZD 2015, 221

4. Datenschutz in der katholischen Kirche

Der Datenschutz in der katholischen Kirche ist im vergangenen Jahr neu strukturiert worden. Um dem Urteil des EuGH vom 09.03.2010 (Az. C-518/07) Rechnung zu tragen, ist die Aufsicht nunmehr auf selbständige und unabhängige Diözesandatenschutzbeauftragte übertragen worden, die zwar in der Regel eine Anstellung bei einem Belegenheitsbistum haben, diesem jedoch disziplinarisch und fachlich nicht unterstellt sind, sondern weisungsfrei arbeiten.

Diese Aufsicht ist auf fünf Bereiche aufgeteilt worden. Diese sind der Bereich der bayrischen (Erz-) Bistümer Augsburg, Bamberg, Eichstätt, München-Freising, Regensburg und Würzburg,
der Bereich der nordrhein-westfälischen (Erz-) Bistümer (Aachen, Essen, Köln, Münster [nordrhein-westfälischer Teil des Bistums] und Paderborn,
der Bereich der norddeutschen (Erz-) Bistümer Hamburg, Hildesheim, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O.,
der Bereich der ostdeutschen (Erz-) Bistümer Berlin, Dresden-Meißen, Görlitz, Erfurt und Magdeburg sowie
der Bereich der mittel- und südwestdeutschen (Erz-) Bistümer Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer, Trier. Der vorliegende Bericht ist der erste Tätigkeitsbericht des Diözesandatenschutzbeauftragten der ostdeutschen Bistümer.


HAMBURG
BERLIN
Osna-
brück
Hildesheim
Münster
PADERBORN
Magdeburg
Görlitz
Essen
KÖLN
Aachen
Fulda
Erfurt
Dresden-
Meißen
Limburg
Trier
Mainz
Würzburg
BAMBERG
Speyer
Eichstätt
Regensburg
Rottenburg-
Stuttgart
Passau
Augsburg
MÜNCHEN-
FREISING
FREI-
BURG

5. Diözesandatenschutz für die ostdeutschen Bistümer

5.1. Räumliche Situation

Zu Beginn des Jahres 2016 wurde das Büro des Diözesandatenschutzbeauftragten eingerichtet. Auf Wunsch der beteiligten (Erz-) Bistümer sollte der Diözesandatenschutzbeauftragte seinen Sitz nicht am Ort eines Bischofsitzes haben, um die Unabhängigkeit dieser Stelle zu unterstreichen. Deshalb wurde als Standort die Stadt Schönebeck gewählt.

5.2. Personelle Situation im Büro des Diözesandatenschutzbeauftragten

Bei Errichtung der Stelle wurde geplant dort drei Mitarbeiter (neben dem Diözesandatenschutzbeauftragten eine technische Fachkraft sowie eine Sekretariats-/Sachbearbeiter-Stelle) anzustellen. Die beiden Stellen neben dem Diözesandatenschutzbeauftragten sollten nach der ersten Planung als Teilzeitstellen mit einem Umfang von jeweils 20 Stunden/Woche ausgestaltet werden.
Diese personelle Ausstattung entspricht vor dem Hintergrund der zu betreuenden Einrichtungen und der Katholikenzahl, vor allem aber der Fläche, die sich über fünf Bundesländer erstreckt, nicht einer den staatlichen Landesdatenschutzstellen vergleichbaren Ausgestaltung. Auch im Vergleich mit den anderen Diözesandatenschutzbeauftragten ist diese personelle Ausstattung mittelfristig ungenügend. Weiterhin entspricht sie auch nicht der neuen Europäischen Datenschutzgrundverordnung, die seinerzeit noch nicht veröffentlicht worden war. Gleichwohl ist die Kirche, um ihren Autonomie-Status beim Datenschutz zu erhalten, verpflichtet, einen adäquaten Datenschutz zu gewährleisten.
Für das kommende Jahr sind deshalb Mittel im Haushalt einzustellen, die die Anstellung von zwei Vollzeitarbeitskräften neben dem Diözesandatenschutzbeauftragten erlauben.
Außerdem kann die katholische Kirche einen dem staatlichen Bereich adäquaten Datenschutz nur dadurch gewährleisten, dass sie die Verpflichtung betriebliche Datenschutzbeauftragte zu bestellen, wie es die KDO in § 20 verbindlich fordert, konsequent umsetzt. In diesem Zusammenhang ist auf die Eingabe der Konferenz der Diözesandatenschutzbeauftragten an den Verwaltungsrat des VDD hinzuweisen.

5.3. Aufbau des Datenschutzes in den beteiligten (Erz-) Bistümern

Dem Aufbau eines solchen Datenschutz- bzw. Datenschützernetzwerkes hat der Unterzeichner, gerade auch wegen der aufgrund des neuen EU-Rechts zu erwartenden Veränderungen, die oberste Priorität eingeräumt. Leider wird dies von den beteiligten Bistümern nicht in jedem Fall im erforderlichen Maße mitgetragen. Obwohl die Regelung in der KDO insofern eindeutig ist, ging die Bestellung von betrieblichen Datenschützern bislang nur schleppend voran.

Die neue EU-DSGVO sieht bei der Verpflichtung zur Schaffung von betrieblichen Datenschutzbeauftragten keine Mindestzahl der mit der Verarbeitung von personenbezogenen Daten beschäftigten Mitarbeiter mehr vor. Bislang war dies sowohl im BDSG als auch in der KDO anders geregelt. Nach diesen Vorschriften waren betriebliche Datenschutzbeauftrage erst zu bestellen, wenn mit der Verarbeitung personenbezogener Daten mehr als neun bzw. 10 Personen beschäftigt waren. D. h. nach der neuen EU-DSGVO an die unsere KDO anzupassen ist, wird in Zukunft in jeder Einrichtung, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten befasst ist, ein betrieblicher Datenschutzbeauftragter zu bestellen sein. In diesem Zusammenhang ist darauf hinzuweisen, dass die in § 20 Abs. 2 KDO als „Soll-Vorschrift“ formulierte Forderung eine „Muss-Vorschrift“ ist. („Sollen“ im verwaltungsrechtlichen Sinne heißt „müssen“, wenn nicht gravierende, außergewöhnliche Umstände eine Abweichung rechtfertigen. S. a. Beschluss der Konferenz der Diözesandatenschutzbeauftragten „Betrieblicher Datenschutzbeauftragter nach § 20 KDO, Pkt.1. Ermessensausübung)

Um die Anforderungen der KDO in § 20 Abs. 2 und Abs. 3 näher zu konkretisieren, hat die Konferenz der Diözesandatenschutzbeauftragten auf ihrer Sitzung am 19.10.2016 den in der Anlage 2 beigefügten Beschluss verabschiedet. Damit soll nicht zuletzt ein einheitlicher Standard in den Diözesen erreicht werden.
Im Berichtszeitraum sind im Wirkungsbereich des Diözesandatenschutzbeauftragten zwei Fälle im Bereich der Caritas bekannt geworden, in denen die Vergabe von Projekten, auf die sich die Caritaseinrichtungen beworben hatten, von der Vorlage eines Datenschutzkonzeptes abhängig gemacht worden sind. Das Vorliegen solcher Datenschutzkonzepte in den Einrichtungen ist bestenfalls eine Ausnahme. Ein solches Konzept ist in der Regel auch nicht innerhalb weniger Tage zu erstellen.

Hier ist es erforderlich, dass die betrieblichen Datenschutzbeauftragten vor Ort dafür sorgen, dass solche Unterlagen erstellt und bereitgehalten werden. Der Diözesandatenschutzbeauftragte steht dabei als Berater unterstützend zur Verfügung. Damit wird aber auch klar, dass dort, wo kein Datenschutzbeauftragter in der Einrichtung vorhanden ist, wichtige Datenschutzvorschriften nicht eingehalten werden. Dies kann z. B. im Falle eines nicht vorhandenen Datenschutzkonzeptes zu finanziellen Einbußen führen und auch dazu, dass kirchliche Einrichtungen aufgrund eines mangelhaften Datenschutzes von Ausschreibungen ausgenommen werden!

Zu den Aufgaben des Diözesandatenschutzbeauftragten gehört auch die Zusammenarbeit mit staatlichen Beauftragten für Datenschutz (§ 18 Abs. 5 KDO). Dort, wo Gespräche mit den Landesbeauftragten für Datenschutz erfolgt sind, wurde auch sofort die personelle Ausstattung des Büros des Diözesandatenschutzbeauftragten kritisch hinterfragt. Wie oben bereits dargestellt, konnten derartige Bedenken mit dem Hinweis auf eine flächendeckende Bestellung von betrieblichen Datenschutzbeauftragten und den intensiven Austausch mit diesen zum Teil eingeschränkt werden. Aber auch hier wird nochmal deutlich, dass die Kirchen mit ihrem Sonderstatus einer durchaus kritischen Beobachtung unterstehen. Auch wenn sich die Kirchen für ihren Sonderstatus auf das Grundgesetz und die Weimarer Reichsverfassung berufen können, ist dieser keineswegs „in Stein gehauen“. Wir gefährden diesen Sonderstatus, wenn wir nicht mehr darstellen können, dass wir einen dem staatlichen bzw. jetzt dem europäischen Datenschutz adäquaten Datenschutz gewährleisten. Selbst eine öffentliche Diskussion darüber würde unseren Einrichtungen in einem umkämpften Markt schaden.

Das Erzbistum Berlin und das Bistum Magdeburg wurden bis zum Ende des Jahres 2015 im Rahmen des norddeutschen Datenschutzverbundes vom Diözesandatenschutzbeauftragten Grammann mit Sitz in Hannover betreut. Herr Grammann war im norddeutschen Verbund für ein Gebiet von der holländischen bis zur polnischen Grenze zuständig. Aufgrund dieser flächenmäßigen Ausdehnung seines Zuständigkeitsbereiches konnte eine Betreuung bzw. eine Beratung einzelner Einrichtungen der angeschlossenen Bistümer nicht gewährseistet werden. Herr Grammann konzentrierte sich deshalb darauf, Ausführungen sowie Musterformulare zu datenschutzrechtlichen Einzelfragen zu erstellen. Er hat dabei ein umfangreiches und fundiertes Werk geschaffen und, vor

dem Hintergrund der großen Fläche und der zahlreichen Einrichtungen für die er zuständig war, das ihm Mögliche getan. Gleichwohl sah sich Herr Grammann häufig der Kritik ausgesetzt, weil seine Amtsführung als zu passiv angesehen wurde und er in den Bistümern nur selten in Erscheinung trat.
Die Bistümer Dresden-Meißen, Erfurt und Görlitz haben bis zum Ende des Jahres 2015 Mitarbeiter, die in der Hierarchie der jeweiligen Einrichtung standen, als Diözesandatenschutzbeauftragte beschäftigt. Dies ist unzulässig und entsprach seit dem Urteil des Europäischen Gerichtshofes vom 09.03.2010 (EuGH C 518/07) nicht mehr dem geltenden Recht. Das Gericht legte fest, dass der Datenschutzbeauftragte unabhängig und weisungsfrei arbeiten muss.

Mit der Einrichtung des gemeinsamen Diözesandatenschutzbeauftragten für die ostdeutschen Bistümer sollte eine rechtskonforme Einrichtung geschaffen werden, die die Anforderungen der KDO umsetzt. Zu diesen Anforderungen gehört die Überwachung der Einhaltung der Regelungen über den Datenschutz, Empfehlungen zu Verbesserungen des Datenschutzes, Beratung kirchlicher Dienststellen und ggf. Erstellung von Gutachten und Berichten (§ 18 Abs. 1 KDO). Bei dieser Betrachtung wird deutlich, dass der Diözesandatenschutzbeauftragte sich nicht darauf beschränken kann, in seinem Büro auf Aufträge oder Anfragen zu warten, sondern aktiv auf die Einrichtungen zugehen muss. Dafür bedarf es aber eines Ansprechpartners vor Ort, der sich mit den datenschutzrechtlichen Belangen der Einrichtung auskennt. Der betriebliche Datenschutzbeauftragte ist deshalb als Partner für den Diözesandatenschutzbeauftragen wichtig, da letzterer ohne ihn seine Aufgaben nicht sachgemäß erfüllen kann bzw. gar nicht um die Probleme in den Einrichtungen weiß. Nur eine regelmäßige Zusammenarbeit beider kann einen konsequenten Datenschutz gewährleisten und eine effektive Arbeit des Diözesandatenschutzbeauftragten ermöglichen.
Der Arbeitsaufwand für den betrieblichen Datenschutzbeauftragten wird dabei nach diesseitiger Einschätzung und Rücksprache mit betrieblichen Datenschutzbeauftragten zwei Stunden pro Woche selten überschreiten.
Die Beauftragung eines externen Unternehmens als betrieblicher Datenschutzbeauftragter ist nach der KDO möglich. (Diese Rechtsansicht wurde bislang nicht von allen Diözesandatenschutzbeauftragten der deutschen Bistümer geteilt.) Als empfehlenswert wird sie dennoch nicht betrachtet. Zum einen sind dadurch deutlich höheren Kosten zu erwarten, zum anderen aber geht vor allem die Verbindung zwischen dem betrieblichen Datenschutzbeauftragten und dem Diözesandatenschutzbeauftragten verloren. Außerdem wird kaum eine

kontinuierliche Beziehung zwischen dem betrieblichen Datenschutzbeauftragten und der zu betreuenden Einrichtung entstehen, sondern immer nur eine partielle auf das jeweilige Problem ausgerichtete Zusammenarbeit. Wenn man jedoch der Rechtsansicht folgt, dass mit der Aufgabe des betrieblichen Datenschutzbeauftragten auch ein Unternehmen beauftragt werden kann, ist eine entsprechende Entscheidung der Einrichtungsleitung hinzunehmen. Insoweit hat der Diözesandatenschutzbeauftragte diesbezüglich kein Einspruchsrecht.

6. Aufgaben und Tätigkeiten des Diözesandatenschutzbeauftragten

Zu den Kernaufgaben des Diözesandatenschutzbeauftragten gehören gem. § 18 Abs. 1 KDO

- Überwachung der Einhaltung von Datenschutzvorschriften in den Einrichtungen der beauftragenden Bistümer
- Beratung zu datenschutzrechtlichen Themen
- Erstellung von Gutachten auf Antrag

Eine einmal erteilte zeitlich nicht beschränkte Einwilligung bedeutet im Grundsatz nicht, dass sie unwiderruflich erteilt worden wäre.

6.1. Allgemein

Bei der Prüfung jedes Einzelfalls ist zunächst zu ermitteln, ob die Erhebung, Verarbeitung oder Nutzung zweckmäßig, erforderlich und verhältnismäßig ist.

6.1.1. Zweckbindung

Die datenschutzrechtlichen Normen gehen vom Grundsatz der Datensparsamkeit aus (§ 2a KDO, § 3a BDSG). In diesem Zusammenhang ist bei jeder Erhebung, Verarbeitung oder Nutzung zunächst der Zweck festzulegen, für den sie erfolgt. Für die informationelle Selbstbestimmung ist zentral, dass personenbezogene Daten nur für den definierten Zweck genutzt werden dürfen[18]. Damit ist das Sammeln nicht anonymisierter Daten auf Vorrat zu unbestimmten Zwecke unzulässig[19]. Auch unzulässig ist die Weitergabe innerhalb verschiedener Organisationseinheiten einer Verwaltungseinheit, bzw. eines Trägers[20], weil es

[18] Weichert in DKWW Kommentar zum BDSG, Einleitung Rn. 17
[19] Fachet, Datenschutz in der Kirche 2.2.2.c)
[20] Ebd. 2.2.2.h)

einen Grundsatz der „Einheit der Verwaltung“ oder „Einheit der verarbeitenden Stelle“, innerhalb der erlangte Daten frei verfügbar sind, nicht gibt[21].

6.1.2. Erforderlichkeit

Für den verfolgten Zweck muss die Erhebung, Nutzung oder Verarbeitung von personenbezogenen Daten erforderlich sein.
Der Begriff der Erforderlichkeit durchzieht die KDO wie auch das BDSG. Bei seiner Auslegung ist zu beachten, dass die KDO wie auch das BDSG vom Grundsatz geprägt sind, dass Erhebung, Verarbeitung und Nutzung von Daten grundsätzlich verboten sind[22].
An den Begriff der Erforderlichkeit sind deshalb strenge Anforderungen zu stellen. Es ist nicht ausreichend, dass die Daten zur Aufgabenerfüllung geeignet oder zweckmäßig sind. Notwendig ist vielmehr, dass es der empfangenden Stelle ohne die Erhebung, Verarbeitung oder Nutzung der Daten unmöglich ist, ihre Aufgaben zu erfüllen[23]. Das gilt selbst dann, wenn die Aufgabe sonst nur unter großen Schwierigkeiten erfüllt werden kann.[24]

6.1.3. Verhältnismäßigkeit

Auch wenn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zweckmäßig und erforderlich ist, ist dennoch zu prüfen, ob diese Maßnahme auch verhältnismäßig ist. D. h. es ist im Einzelfall zu untersuchen, ob schutzwürdige Interessen des Einzelnen, insbesondere sein Recht auf informationelle Selbstbestimmung das Interesse der verarbeitenden Stelle nicht überwiegen und somit die Erhebung, Verarbeitung oder Nutzung unzulässig machen.

6.1.4. Die Einwilligung gem. § 3 Abs. 2 KDO

Im deutschen Datenschutzrecht gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt. Das heißt, Datenerhebungen, -nutzungen und –verarbeitungen sind rechtswidrig, wenn nicht ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat[25].

[21] Weichert in DKWW Kommentar zum BDSG Einleitung Rn. 178
[22] Dammann in Simitis § 13 Rn. 25
[23] Eßer in Auernhammer Kommentar zum BDSG § 15 Rn. 13, Wedde in DKWW Kommentar zum BDSG § 15 Rn. 5
[24] Dammann in Simitis Kommentar zum BDSG § 15 Rn. 11
[25] § 4 Abs. 1 BDSG

Soweit eine Verwendung der personenbezogenen Daten nicht bereits durch eine gesetzliche Vorschrift gem. § 3 Abs. 1 Nr. 1 KDO erlaubt ist, kann die Legitimation dazu durch die Einwilligung gem. § 3 Abs. 2 KDO erfolgen. Die Einwilligung ist die vorher erklärte Zustimmung gem. § 183 BGB. Die Erhebung und Verwendung personenbezogener Daten, die gesetzlich ausdrücklich verboten ist, kann dabei aber durch eine Einwilligung nicht legitimiert werden (§134 BGB)[26].

Bei der Einwilligung kommt es auf die Geschäftsfähigkeit nicht an, sondern ausschließlich darauf, ob der Betroffene die Konsequenzen seines Handelns übersehen konnte.[27] Damit kann eine wirksame Einwilligungserklärung grundsätzlich auch von Minderjährigen abgegeben werden, wenn und soweit eine Einsichtsfähigkeit besteht[28].

Eine Stellvertretung scheidet aufgrund des höchstpersönlichen Charakters der Einwilligung aus.

Im Gegensatz zur Genehmigung hat die Einwilligung vor der Verwendung zu erfolgen. Eine spätere Legitimation ist nicht möglich,[29] schließt aber ggf. die Geltendmachung von Schadenersatzansprüchen aus.

Gem. § 3 Abs. 2 S. 3 KDO hat die Einwilligung grundsätzlich schriftlich zu erfolgen. Gem. § 126 BGB ist dafür die eigenhändige Unterschrift erforderlich. Zwar entsprechen Fax und E-Mail der Textform des § 126b BGB, diese ist der Schriftform jedoch nicht gleichgestellt und in § 4a Abs. 1 S. 3 nicht erwähnt, so dass diese Form nicht ausreichend ist.[30]

Die Einwilligung muss erkennen lassen, welche Daten zu welchem Zweck von wem verwendet werden sollen. Pauschale Einwilligungen, die dies nicht erkennen lassen, sind unzulässig.[31] Der Betroffene kann in einem Fall pauschaler Zustimmung zur Verwendung persönlicher Daten nicht den Zweck der Verwendung erkennen. Damit fehlt ihm die Beurteilungsgrundlage für eine Einwilligung.[32]

Die Einwilligung muss freiwillig erfolgen.

Dies ist bereits dann nicht mehr gegeben, wenn für den Fall der Verweigerung der Einwilligung dem Einwilligenden erhebliche Nachteile in Aussicht gestellt wurden.

[26] Taeger, (Taeger / Gabel BDSG) § 4a Rn 18
[27] Däubler, § 4a Rn. 5
[28] Simitis § 4a Rn 20
[29] OLG Köln, NJW 1993, 793, Taeger § 4a Rn. 32
[30] Däubler, Gläserne Belegschaften § 4 Rn. 145
[31] Taeger, §4a Rn. 30, Däubler, § 4a Rn. 18
[32] So auch der Hamburger Datenschutzbeauftragte im 18. TB

Widerruf der Einwilligung.
Eine einmal erteilte Einwilligung kann unter denselben Bedingungen, wie sie erteilt wurde, auch widerrufen werden. Es ist mithin eine höchstpersönliche schriftliche oder in elektronischer Form abzugebende Erklärung erforderlich.[33] Einigkeit besteht auch darin, dass der Widerruf der Einwilligungserklärung nur mit Wirkung für die Zukunft ausgesprochen werden kann.[34] Ab dem Zeitpunkt des Widerrufszuganges ist die weitere Verwendung der Daten für die erhebende Stelle unzulässig. Diese wird durch den Widerruf verpflichtet, die Daten gem. § 14 Abs. 2 KDO zu löschen.
Unstreitig ist auch, dass eine Einwilligung befristet erteilt werden kann. Dies ergibt sich bereits aus der Freiwilligkeit einer Einwilligung und der Möglichkeit von des Widerrufs.

6.2. Details

6.2.1. Veröffentlichung von Amtsbezeichnungen

Bei der Frage, ob eine Veröffentlichung der Daten von Mitarbeitern und Mitarbeiterinnen im Internet zulässig ist, wenn eine diesbezügliche Einwilligung der/des Betroffenen nicht vorliegt, kommt es darauf an, ob die Veröffentlichung der Daten zur ordnungsgemäßen Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist. Dies ist insbesondere bei Mitarbeitern/innen zu bejahen, die ein Leitungsamt ausüben oder ein Amt mit Außenwirkung. Solche Amtsträger, zu denen auch die Mitarbeiter einer Kirchenverwaltung gehören, können sich dann und soweit nicht auf das Recht der informationellen Selbstbestimmung berufen, soweit sie als für die Kirche handelnde Personen im Rahmen einer nach außen gerichteten Aufgabe tätig werden.
Angaben, die im Zusammenhang mit einer nach außen gerichteten Tätigkeit als Amtsträger stehen, sind Name, Vorname, Funktion sowie dienstliche Erreichbarkeit und Dienstort. Diese Daten können ohne Einwilligung des/der Betroffenen oder eine Rechtsgrundlage an Dritte übermittelt werden.
Dies gilt im Umkehrschluss nicht für solche Mitarbeiter, die lediglich innere Dienste versehen, wie Pförtner, Buchhalter u.ä.

[33] Simitis § 4a Rn. 96, Däubler § 4a Rn. 36
[34] Gola DuD 2001, 279; Weichert DuD 2002, 139

Darüberhinausgehende Mitteilungen wie Angaben zu privater Wohnung und Erreichbarkeit sowie zu Ausbildungswegen, Ausbildungsabschlüssen und Stationen der beruflichen Tätigkeit, dürfen ohne Einwilligung des Amtsinhabers nicht veröffentlicht werden.

So darf zum Beispiel die Sendung bzw. Beauftragung einer/s Gemeindereferentin/en in eine bestimmte Pfarrei mit den o. g. zulässigen Angaben ohne Zustimmung der Mitarbeiterin des Mitarbeiters im Amtsblatt veröffentlicht werden.

Auch die Angabe, dass ein/e Gemeindereferent/in vom Dienst entpflichtet worden ist darf im Amtsblatt veröffentlicht werden. Der Grund der Entpflichtung jedoch darf in der Regel nicht mitgeteilt werden, da damit weitere persönliche Daten bekanntgegeben werden. Z. B.: „…wird entpflichtet, weil sie in die Altersrente geht“ oder „… wird entpflichtet, weil sie sich der Erziehung ihrer Kinder widmen möchte“ o.ä. Für die Bekanntgabe derartiger persönlicher Daten bedarf es einer Einwilligung des/der Betroffenen.

6.2.2. Fotografien

Immer wieder ist das Thema „Fotos in der Kinder-Einrichtung“ Gegenstand von Anfragen. Dabei geht es sowohl um datenschutzrechtliche Fragen, z. B. ob Fotoverbote in der Einrichtung ausgesprochen werden dürfen, wie mit Fotos zu verfahren ist, die auf Veranstaltungen der Einrichtung angefertigt wurden, wo die Fotos veröffentlicht werden dürfen, aber auch um die Fragen der Urheberrechte an den Fotos. Problematisch in diesem Kontext ist die Anfertigung und ggf. die Verbreitung von Fotos, die Eltern ohne Einwilligung des Kita-Personals und der abgebildeten Kinder aufnehmen.

Die Rechtsgrundlage für Veröffentlichung von Fotos, unabhängig davon ob sie digital oder analog erstellt werden, bildet das Kunsturhebergesetz (KunstUrhG).

> § 22 KunstUrhG
> Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

Aufgrund des dort geregelten „Rechtes am eigenen Bild“ dürfen Fotos grundsätzlich nur mit Einwilligung des Abgebildeten veröffentlicht werden. Für Kindereinrichtungen wurden dazu Mustertexte erstellt. (Anlage2)

Diese Vorschrift gilt gleichermaßen für alle Beteiligten. Es ist also egal, ob Eltern von Kindern, Personal der Einrichtung oder sonstige Dritte die Aufnahmen erstellen.

Die Herausgabe von Fotos an Dritte ist zu unterlassen. Das betrifft auch den Aushang im Schaukasten der Einrichtung oder Kirchengemeinde. Sollte es eine Einwilligung der Berechtigten zur Anfertigung und Weitergabe von Fotos geben, ist gesondert eine Zustimmung zur Weitergabe von Fotos in digitaler Form einzuholen.

Fotos dürfen ausschließlich an die Eltern des Kindes herausgegeben werden, welches auf dem Foto abgebildet ist. Sind neben dem Kind auch andere Kinder auf dem Foto abgebildet, scheidet eine Herausgabe aus.

Über das Verbot der Anfertigung von Fotos auf denen neben dem eigenen Kind andere Kinder oder Personen der Einrichtung zu sehen sind, sollten Eltern besonders belehrt werden. Die Eltern sollten dies durch Unterschrift bestätigen (Anhang 3a). Auch wenn die Eltern diese Regelung nicht unterschreiben sollten, kann die Einrichtung natürlich ein Fotoverbot aussprechen und dieses durch Aushänge ggf. durch entsprechende Piktogramme bekannt machen. Das Thema sollte auf einem Elternabend besprochen und im Protokoll festgehalten werden. Dem Protokoll ist dann die Teilnehmerliste anzuheften. Damit ist die Mitteilung dieses Verbotes belegbar.

Vielfach werden Fotos oder Videos im Rahmen von Entwicklungsberichten durch die Erzieher/innen angefertigt. Auch in diesem Bereich gilt das Gesagte (Anhang 3b). Die Anfertigung von Fotos oder Videos stellt einen erheblichen Eingriff in das Persönlichkeitsrecht des Kindes dar. Regelmäßig wird es hierfür an einer Erforderlichkeit (s.o. 6.1.2.) fehlen, da die Erzieher-/innen aufgrund ihrer Ausbildung in der Lage sein müssen ihre Wahrnehmungen schriftlich zu fixieren.

Hinzuweisen ist weiter auf den Fall, dass ein professioneller Fotograf in die Einrichtung kommt und Fotos von den Kindern anfertigt, um den Eltern diese hinterher zum Kauf anzubieten. Auch hierfür ist dann eine gesonderte Einwilligung (vorher!) einzuholen. Dabei ist darauf zu achten, dass von den Kindern, die eine solche gesonderte Einwilligung nicht vorlegen auch keine Aufnahmen, erstellt werden.

§ 22 KunstUrhG und die hier benannten Grundsätze gelten aber auch für alle anderen Anlässe, bei denen Fotos oder Videoaufnahmen angefertigt werden. So dürfen Bilder von Gemeindefesten, Firmungen, Beerdigungen und anderen kirchlichen Veranstaltungen ebenfalls nicht ohne Zustimmung aller auf dem Foto Abgebildeten veröffentlicht werden.
Eine Ausnahme gilt nach § 23 KunstUrhG für den Fall, dass Bilder von einem Aufzug oder einer Versammlung, an denen die dargestellten Personen teilgenommen haben, gemacht werden. Das ist z. B. dann der Fall, wenn das Gemeindefest als Ganzes fotografiert wurde, ohne dass dabei einzelne Personen besonders hervortreten.

6.2.3. Veröffentlichung von Jubiläumsdaten

Im Pfarrblatt einer Pfarrei werden regelmäßig unter der Überschrift „Allen Geburtstagskindern dieser Woche gratulieren wir herzlich und wünschen Gottes Segen!“ Jubilare ab einem bestimmten Alter mit Vor- und Zunamen sowie dem Alter benannt, die in der entsprechenden Zeit Geburtstag feiern. Das Pfarrblatt wird in einer Printvariante verteilt und ist im Internet einsehbar.
Aufgrund einer Beschwerde, die beim Diözesandatenschutzbeauftragten eingegangen ist, war dazu Stellung zu nehmen:
Bei Vor- und Zunamen sowie dem Alter handelt es sich um personenbezogene Daten. Weiterhin ist auch die Konfession, der eine Person angehört, ein personenbezogenes Datum.
Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist gem. § 3 der kirchlichen Datenschutzordnung nur zulässig, soweit
1. die kirchliche Datenschutzordnung (KDO) oder eine andere kirchliche oder eine staatliche Rechtsvorschrift dies erlaubt oder anordnet oder
2. der/die Betroffene eingewilligt hat.

Mit dem Abdrucken bzw. Veröffentlichen im Internet liegt eine Verarbeitung im Sinne des § 3 KDO vor.
Eine Einwilligung ist nach der Legaldefinition des § 183 BGB eine vorherige Zustimmung. Sofern eine solche vorliegt, ist eine Veröffentlichung im Pfarrblatt grundsätzlich kein Problem. Jedoch ist hierbei zu beachten, dass die Einwilligung freiwillig und grundsätzlich schriftlich zu erfolgen hat und der Einwilligende über den Umfang der Einwilligung Kenntnis besitzt. Insbesondere der letzte Punkt ist dann zu beachten, wenn eine Einwilligung zur Veröffentlichung in einem

Printmedium erteilt wird, dieses aber auch ins Internet gestellt wird. Hier ist eine ausdrückliche Einwilligung auch für die Veröffentlichung im Internet erforderlich.

Wenn keine Einwilligung vorliegt, ist zu prüfen, ob die Veröffentlichung durch eine kirchliche oder staatliche Rechtsvorschrift erlaubt oder angeordnet ist.
Das Bundesmeldegesetz (BMS), dort § 50, ist hier nicht einschlägig, da die Pfarreien keine Meldebehörden i. S. des BMS sind.
Eine andere rechtliche Grundlage könnte in der Regelung des § 10 Abs. 2 Nr. 10 KDO zu sehen sein. Dies setzte voraus, dass die Veröffentlichung der Jubiläen im Auftrag der Kirche bzw. der Glaubwürdigkeit ihres Dienstes erforderlich ist. Es mag für den einzelnen Jubilar wichtig sein zu erfahren, dass man seines Ehrentages gedenkt bzw. dass man ihn in die Gemeinschaft einbezieht. Dies kann aber auch auf anderem, die Persönlichkeitsrechte nicht beeinträchtigendem Wege erreicht werden. Beispielsweise durch Zusendung einer Glückwunschkarte. Die Preisgabe personenbezogener Daten ist nicht Aufgabe der Kirche und die Unterlassung dessen beeinträchtigt die Glaubwürdigkeit ihres Dienstes nicht. Somit scheidet auch diese Vorschrift als Rechtsgrundlage einer Veröffentlichung aus.
Dem jeweiligen Bischof steht es frei, eine entsprechende Rechtsvorschrift zu erlassen, in der die Veröffentlichung von Jubiläumsdaten geregelt ist. Eine solche rechtliche Grundlage für die Veröffentlichung der benannten personenbezogenen Daten bestand seinerzeit nicht. Die Veröffentlichung der genannten personenbezogenen Daten war deshalb unzulässig
Zwischenzeitlich haben die beteiligten Bistümer in ihren Amtsblättern eine Jubiläumsordnung veröffentlicht. Der Text der Jubiläumsordnung ist inzwischen auch von der Diözesandatenschutzkonferenz auf ihrer Sitzung am 19.10.2016 beschlossen worden und soll allen Bistümern zur in Kraft Setzung vorgelegt werden (Anhang 1).

6.2.4. Weitergabe von Meldedaten

Ein Petent beschwerte sich beim Diözesandatenschutzbeauftragten darüber, dass offensichtlich die über ihn beim Bistum gespeicherten Meldedaten an einen im Eigentum mehrerer Bistümer stehenden Verlag weitergeleitet worden sind, um diesem Werbemaßnahmen bei Katholiken zu ermöglichen. Dabei wurden die übermittelten Daten genutzt, um den Petenten auf ein in diesem Verlag periodisch erscheinendes Printerzeugnis hinzuweisen und ihm ein Abonnement nahe zu legen.

Es geht hier um die Übermittlung von personenbezogenen Daten gem. § 11 Abs. 1 KDO an eine kirchliche Stelle gem. § 1 Abs. 2 Nr. 3 KDO. Eine solche ist zunächst zulässig, wenn sie gem. § 11 Abs.: 1 Nr. 1 „… zur Erfüllung der in der Zuständigkeit … der empfangenden Stelle liegenden Aufgaben erforderlich ist“ An den Begriff „erforderlich“ sind strenge Anforderungen zu stellen[35](s.o. 6.1.2.).

Die zu erfüllende Aufgabe des Verlages besteht darin, eine Publikation herauszugeben, die den Verkündigungsauftrag der Kirche unterstützt. Neben dem Abdruck und der Auslegung der sonntäglichen Schriftstellen (Evangelium, Lesungen) und der Behandlung aktueller Themen aus kirchlicher Sicht wird dabei besonderer Wert auf die Darstellung von Ereignissen und Veranstaltungen in den jeweiligen Bistümern gelegt. Damit erfüllt dieses Druckerzeugnis den Auftrag und ist konkurrenzlos.

Um diesen Auftrag zu erfüllen, bedarf es jedoch nicht der Übermittlung von Meldedaten. Denn dies hieße, dass die kirchliche Stelle, hier also der Verlag, ohne die Übermittlung der Meldedaten, die in seine Zuständigkeit fallenden Aufgaben nicht erfüllen könnte, was offenkundig nicht der Fall ist.

An dieser Betrachtung ändert sich auch nichts, wenn man davon ausgeht, dass der Verlag zur Herstellung des Printerzeugnisses auf einen festen Leserstamm in Form von Abonnenten vertrauen können muss. Für die Gewinnung von Abonnenten ist die Übermittlung von Meldedaten aber nicht erforderlich, da solche auch auf anderem Wege mit anderen Werbemaßnahmen gewonnen werden können.

Gem. § 11 Abs. 1 Nr. 2 KDO müssten kumulativ die Voraussetzungen vorliegen, die eine Nutzung nach § 10 zulassen würden.

Danach müsste der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes die Übermittlung der Meldedaten erforderlich machen (§ 10 Abs. 2 Nr. 10 KDO).

Bereits der Vergleich mit den anderen in § 10 Abs. 2 KDO geregelten Erlaubnistatbeständen zeigt, dass Gründe von einigem Gewicht vorliegen müssen um eine Datenspeicherung, -veränderung oder –nutzung zu rechtfertigen. Wenn z. B. in Nr. 6 von der Abwehr einer Gefahr für die öffentliche Sicherheit, in Nr. 7 von der Verfolgung von Straftaten oder in Nr. 8 von der Abwehr einer schwerwiegenden Beeinträchtigung der Rechte von Personen die Rede ist, kann das Erforderlichkeitskriterium in Nr. 10 nicht auf bloße Nützlichkeit reduziert werden[36]. Es ist eben nicht ausreichend, dass die Daten zur Aufgabenerfüllung geeignet oder zweckmäßig sind. Notwendig ist vielmehr, dass es der

[35] Dammann in Simitis Kommentar zum BDSG § 13 Rn. 26

[36] So auch Fachet, Datenschutz in der katholischen Kirche, Praxiskommentar zur KDO Seite 103

empfangenden Stelle ohne die Übermittlung der Daten unmöglich ist, ihre Aufgaben zu erfüllen[37]. Das gilt selbst dann, wenn die Aufgabe sonst nur unter großen Schwierigkeiten erfüllt werden kann.[38]
Der Auftrag der Kirche besteht u. a. in der Verkündigung. Dieser Auftrag wird durch das Publikationsorgan unterstützt, das damit als kirchliches Organ auch den Verkündigungsauftrag wahrnimmt. Darauf kommt es aber nicht an. Zu fragen ist vielmehr, ob der Auftrag der Kirche nur durch direkte Werbemaßnahmen, die aufgrund der Weitergabe von Meldedaten ermöglicht worden ist, erfüllt werden kann, indem auf diese Weise auf die Existenz des Printerzeugnisses hingewiesen wird. Das ist nicht der Fall. Dies kann vielmehr auch auf anderem Wege, z.B. in der Kirche „von der Kanzel'", im Pfarrbrief, durch Verteilen von Freiexemplaren vor der Kirche u.a. geschehen. Eine Erforderlichkeit im Sinne des § 10 Abs. 2 Nr. 10 KDO liegt deshalb nicht vor.
Eine Weitergabe von Meldedaten an Dritte zum Zweck der Werbung für ein kirchliches Printerzeugnis ist deshalb unzulässig.

6.2.5. Schweigepflicht

Eine Caritasmitarbeiterin nahm bei dem Besuch eines zu betreuenden Klienten wahr, dass dieser an der Wand mehrere Säbel/Schwerter angebracht hatte. Auf ihre Frage, was er damit wolle, nahm er eine dieser Waffen von der Wand und hielt sie der Caritasmitarbeiterin mit den Worten vor „Ich habe auch schon mal jemanden umgebracht".

Der Diözesandatenschutzbeauftragte wurde von der Teamleiterin dieser Mitarbeiterin angerufen und gefragt, ob sie der Polizei den gestandenen „Mord" melden müsse.

Nach § 203 StGB ist das Offenbaren, also jedwedes Mitteilen, eines zum Zeitpunkt der Tat noch bestehenden Geheimnisses gegenüber einer nicht zum Wissen berufenen Person, die das Geheimnis noch nicht sicher kennt, strafbar.[39]

Das Offenbaren, also die Mitteilung, muss die geheime Tatsache und die Person des Berechtigten umfassen. Es muss also zumindest aus dem Zusammenhang eine Identifikation der Person des Berechtigten für mindestens einen Dritten

[37] Eßer in Auernhammer Kommentar zum BDSG § 15 Rn. 13, Wedde in DKWW Kommentar zum BDSG § 15 Rn. 5
[38] Dammann in Simitis Kommentar zum BDSG § 15 Rn. 11
[39] Langkeit, NStZ 1994, S. 6

möglich sein. Anonymisierte bzw. pseudonymisierte Mitteilungen reichen demgegenüber nicht aus, um sich strafbar zu machen.[40]

Das schützenswerte Interesse des Betroffenen ist weit auszulegen. So sind auch der Name des Betroffenen und die Tatsache, dass er Patient/Klient der Einrichtung ist bereits darunter zu fassen.[41] Ebenso die bloße Vereinbarung eines Termins[42] oder Gedanken, Meinungen, Empfindungen, familiäre finanzielle und berufliche Verhältnisse.

Nach der herrschenden Meinung ist der strafrechtliche Schutz auch für solche Informationen anerkannt, die der Arzt bei Gelegenheit seiner Berufsausübung erlangt hat.[43]

Die Gewissheit um die Diskretion des um Rat befragten Arztes ermöglicht eben, „Hoffnungen, Erwartungen, Sorgen und Ängste zu besprechen, sich etwas Bedrückendes von der Seele zu reden und einen Vertrauten bei der Entscheidung um Rat zu fragen, der für das weitere Leben von Bedeutung, vielleicht sogar lebensentscheidend ist.“[44]

Der Arzt hat auch über solche Rechtsbrüche Stillschweigen zu bewahren, die während eines stationären Klinikaufenthaltes begangenen wurden[45]. Die demgegenüber vertretene Mindermeinung, nur solche Geheimnisse seien schützenswert, die der Patient notgedrungen dem Arzt mitgeteilt hat, da nur sie der tragende Grund des Berufsgeheimnisses seien[46], ist abzulehnen. Dass durch diese Vorschrift zu schützende Rechtsgut ist nicht allein die Privatsphäre des Patienten, sondern darüber hinaus auch die staatliche Gesundheitsfürsorge.[47] Nur wenn der Patient damit rechnen kann, dass alles was er dem Arzt im Rahmen seiner Berufsausübung erzählt geheim bleibt, kann ein Vertrauensverhältnis zwischen Arzt und Patient entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt und der Aufrechterhaltung einer effektiven Gesundheitsvorsorge dient.[48]

---

[40] Fischer, Kommentar zum Strafgesetzbuch § 203, Rn. 30

[41] Rieger, DMW 1982, S. 352

[42] OLG Karlsruhe Urteil vom 23.06.2006, AK 14 U 45/04

[43] Muschalik ArztR 1984, 235, 236

[44] Vilmar DÄ 1982, 25 [57], zitiert in Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes und seiner berufsmäßigen Gehilfen nach § 203 StGB im Hinblick auf Verhütung und Aufklärung von Straftaten.

[45] LG Karlsruhe, Strafverteidiger 1983, 144

[46] Ostendorf ZStW 90 (1978) 11 [54]

[47] Eichelbrönner, Die Grenzen der Schweigepflicht des Arztes und seiner berufsmäßigen Gehilfen nach § 203 StGB im Hinblick auf Verhütung und Aufklärung von Straftaten

[48] BVerfGE 32, 373 ff.; BVerfGE 2BvR 988/75, NJW 1975, S. 1489, 1491

Keines der objektiven Tatbestandsmerkmale des § 203 Abs. 1 StGB wird dadurch ausgeschlossen, dass der Empfänger der Mitteilung seinerseits schweigepflichtig ist.

Auch innerhalb des Kreises der „Schweigepflichtigen“ droht dem Berechtigten das Recht auf informationelle Selbstbestimmung zu entgleiten, da er bei einer größeren Zahl von „Schweigepflichtigen“ nicht mehr sicher sein kann, wer sein Geheimnis kennt und wer nicht.

Ausgenommen von dem Verbot der Weitergabe sind Personen, die typischer Weise in den Behandlungsablauf integriert sind und mit deren Einschaltung der Patient von vornherein rechnet.

Wenn sich der Betroffene jedoch vor seiner Offenbarung gegenüber dem Therapeuten dessen Schweigepflicht versichert, drängt sich dadurch auf, dass er damit jedwede Weitergabe des Offenbarten untersagen wollte. In diesem Fall ist davon auszugehen, dass er sich nur dem konkreten, angesprochenen Therapeuten mitteilen wollte. Eine Weitergabe der Mitteilung hat in einem solchen Fall auch gegenüber dem Kreis zu unterbleiben, der ansonsten unterrichtet werden dürfte.

Auch eine Offenbarung des Geheimnisses gegenüber den Dienstvorgesetzten muss unterbleiben, wenn diese nicht typischer Weise in den Behandlungsablauf integriert sind und deshalb nicht erkennbar für den Betroffenen zum Behandlungsteam gehören.

In folgenden Fällen ist eine Weitergabe der Mitteilung erlaubt:

Wenn

- das ausdrückliche Einverständnis des Betroffenen vorliegt
- eine konkludente (stillschweigende oder mutmaßliche) Einwilligung vorliegt Beispiel: Es liegt der Verdacht auf eine Gewalttat vor und der Patient kann sich nicht äußern. Hier darf die Polizei eingeschaltet werden.
- eine gesetzliche Auskunftspflicht besteht, z. B. gegenüber den Sozialleistungsträgern oder gemäß Infektionsschutzgesetz.

  Ansonsten ist dies dann der Fall, wenn eine der in § 138 StGB genannte Straftat bevorsteht (u.a. Geld- und Wertpapierfälschung, Mord, Totschlag, Raub, Menschenhandel, Brandstiftung) und die Ausführung oder der Erfolg einer solchen Straftat noch verhindert werden kann. Wenn die Straftat bereits erfolgt ist, liegt ein solcher Rechtfertigungsgrund für die Preisgabe des Geheimnisses nicht vor, da in diesem Fall nur noch das Interesse des Staates an der Rechtsverfolgung als schützenswertes Rechtsgut besteht, welches hinter dem Recht auf Wahrung der Persönlichkeit und des Geheimnisschutzes zurücksteht.

- ein rechtfertigender Notstand gemäß § 34 StGB vorliegt.
  Ein solcher rechtfertigende Notstand liegt nur dann vor, wenn eine Güterabwägung ergibt, dass das zu schützende Rechtsgut das durch die Schweigepflicht gewährte Persönlichkeitsrecht überwiegt. Hier sind die Fälle der Kindesmisshandlung einzuordnen.

Eine besondere Aussagepflicht besteht auch nicht gegenüber der Polizei oder der Staatsanwaltschaft.

Auch gegenüber Familienangehörigen von Patienten besteht die Geheimhaltungspflicht.

Auch Minderjährige genießen den Schutz vor Verletzung von Privatgeheimnissen. Deshalb dürfen Mitteilungen von diesem Personenkreis nicht ohne deren Zustimmung an Dritte, z. B. die Eltern, weitergegeben werden. Dies gilt ab einem Alter, ab dem die Minderjährigen in der Lage sind, die Bedeutung einer Einverständniserklärung zu verstehen. Dies wird in der Regel ab einem Alter von 15 Jahren anzunehmen sein.

Die Schweigepflicht besteht grundsätzlich auch über den Tod des Betroffenen hinaus fort. Auch Erben oder Angehörige haben nach dem Tod nicht das Recht, den Therapeuten wirksam von seiner Schweigepflicht zu entbinden. Eine Ausnahme gilt dann, wenn der Therapeut zu der Erkenntnis kommt, dass die Preisgabe des Geheimnisses nach dem Tod des Betroffenen in seinem mutmaßlichen Interesse liegt.

Im vorliegenden Fall durfte keine Mitteilung an die Polizei erfolgen.

6.2.6. Zulässigkeit von Videoaufnahmen

Ein Petent wandte sich an den Diözesandatenschutzbeauftragten. Seine Frau ist dement und befindet sich in einer Pflegeeinrichtung der Caritas. In dieser Einrichtung waren insgesamt 15 Videokameras, sowohl im Inneren wie im Äußeren des Gebäudes, verbaut. Der Petent fühlte sich durch diese Kameras bei seinen Besuchen in seinem Persönlichkeitsrecht beeinträchtigt. Er wollte sich ungezwungen im Gebäude und auf dem Gelände der Einrichtung gemeinsam mit seiner Frau bewegen können, ohne befürchten zu müssen, dabei beobachtet zu werden.

In einem ersten Termin wurde die Einrichtung besucht und mit der Leitung besprochen, welchem Zweck die Anbringung so umfangreicher Überwachungsanlagen dient. Dafür wurden vor allem Sicherheitsgründe benannt, da in der Einrichtung mehrfach Diebstähle vorgekommen seien.

Die kirchliche Datenschutzordnung (§ 5a KDO) verwendet ebenso wie das Bundesdatenschutzgesetz (§ 6b BDSG) den Begriff der „optisch-elektronischen Einrichtung“. Damit wird deutlich, dass alle Geräte die zu einer Bildaufzeichnung oder Überwachung eingesetzt werden können unter diese Vorschrift fallen und nicht nur klassische Videogeräte[49]. Dabei ist es egal, ob diese Geräte mobil oder fest installiert sind[50] und ob sie digital oder analog arbeiten[51].

Durch den verwendeten Begriff „Beobachtung“ wird ferner deutlich, dass es auf eine Aufzeichnung der Bilder nicht ankommt und somit auch Monitor-Systeme unter die Vorschrift fallen. Das sind solche Systeme, bei denen die Bilder direkt auf einen Bildschirm übertragen werden, der von einer Überwachungsperson beobachtet wird[52].

Kameraattrappen fallen zwar nicht unter den Anwendungsbereich der Vorschrift, da sie nicht mit einem optisch-elektronischen Verfahren arbeiten und für Beobachtungen nicht geeignet sind[53], jedoch können gegen sie zivilrechtliche Abwehr- und Unterlassungsansprüche geltend gemacht werden[54].

Die in § 5a KDO geregelte Zulässigkeit von Videoüberwachungen erlaubt in bestimmten Grenzen nur die Videoüberwachung öffentlich zugänglicher Räume (§ 5a Abs. 1 KDO).

Öffentlich zugänglich sind solche Räume, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten oder benutzt werden können[55].

Dazu gehören Kirchen, Eingangsbereiche von Krankenhäusern und Alten- sowie Pflegeheimen, Cafés[56], öffentlich zugängliche Außenanlagen, aber auch Pfarrsäle, Jugendtreffs, Sozialstationen und das Pfarrbüro, soweit es den allgemein zugänglichen Teil betrifft.

Dabei spielt es keine Rolle, ob für den Zugang weitere Voraussetzungen, wie z. B. der Erwerb einer Eintrittskarte oder eine vorherige Anmeldung erforderlich sind.

Demgegenüber sind nichtöffentliche Räume solche, die nur von einem bestimmten oder genau abgegrenzten Personenkreis betreten werden dürfen[57]. Dazu zählen z.B. auch Treppenaufgänge und Aufzüge, die in einem Gebäude belegen sind, welches Wohnzwecken dient, da lediglich Bewohner und deren Besucher Zugang

[49] Scholz in Simitis Kommentar zum Bundesdatenschutzgesetz § 6b Rn. 38
[50] Scholz in Simitis § 6b Rn. 37, Wedde in DKWW § 6b Rn. 17
[51] Scholz ebd,. Rn. 40
[52] Wedde in DKWW § 6b Rn. 13
[53] Wolf/Brink DuD 2011, 447
[54] Gola/Schumerus Kommentar zum BDSG § 6b, Rn. 13;
[55] Bergmann/Möhrle/Herb, Kommentar zum BDSG § 6b Rn. 22
[56] XII. Tätigkeitsbericht des Landesdatenschutzbeauftragten Sachsen-Anhalt, 15.2.4
[5757] Scholz in Simitis Kommentar zum BDSG § 6b Rn. 48

haben sollen und über eine entsprechende Erlaubnis verfügen. Anders sind solche Bereiche einzustufen, wenn in dem Gebäude auch Gewerberäume, Kanzleien, Arztpraxen oder andere für eine unbestimmte Personengruppe zugängliche Räume vorhanden sind. Dann gelten diese Räume als öffentliche Räume, jedenfalls zu den Geschäfts- bzw. Öffnungszeiten[58].

Gem. § 5 a Abs. 1 Nr. 1 KDO ist eine Videobeobachtung zulässig, wenn sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder nach § 5 Abs. 1 Nr. 2 KDO zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist.

In der Regel wird es nicht zur Aufgabenerfüllung kirchlicher Dienststellen oder einer kirchlichen Einrichtung gehören, Videoaufnahmen von Bewohnern und Besuchern zu erstellen.

Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer das Gebäude betreten und sich darin aufhalten darf[59]. Dies mag es rechtfertigen, eine Videoanlage im Monitoring-System zu installieren, wenn die übrigen Voraussetzungen gegeben wären. Solche Anlagen sind z. B. in Eingangsbereichen oder Tiefgaragenzufahrten denkbar, wenn diese sonst nicht einsehbar sind und eine Öffnung von zentraler Stelle erfolgt. Auch in Intensiv- oder Pflegebereichen können Videoüberwachungen im Monitoring System unter bestimmten Umständen gerechtfertigt sein. Erforderlich ist aber stets die direkte Überwachung mit sofortiger Eingriffsmöglichkeit.

§ 5 Abs. 1 Nr. 2:

Die Wahrnehmung berechtigter Interessen setzt das Bestehen einer konkreten Gefährdungslage voraus. Hierfür sind konkrete Vorfälle darzulegen, die eine Anbringung der Videoüberwachung gerade an dieser Stelle erforderlich machen. Eine bloße Behauptung oder Vermutung, dass Rechtsverletzungen gerade an dieser Stelle zu erwarten sind, reicht nicht aus[60].

Weiterhin müsste eine konkrete Zweckbestimmung vorliegen, d. h. das konkrete Ziel der Überwachung müsste benannt sein. Allgemeine Erklärungen wie „Gefahr von Diebstählen oder Sachbeschädigungen“ werden dem nicht gerecht[61].

In der Regel lassen sich durch eine Videoüberwachung im Aufzeichnungssystem Straftaten nicht verhindern. In diesen Fällen soll die Überwachung lediglich der Verfolgung des Straftäters dienen und vermittelt bestenfalls ein subjektives Sicherheitsempfinden. Objektiv führen Videoaufzeichnungen häufig nicht dazu,

[58] VG Oldenburg, ZD 2013, 296

[59] Scholz in Simitis Kommentar zum BDSG § 6b Rn. 73

[60] BGH NJW 1995, 1950 (1957); Scholz in Simitis Kommentar zum BDSG § 6b Rn. 80

[61] So auch BfDI 23. Tätigkeitsbericht Pkt. 12.1. (dort zum Thema Beschäftigtendatenschutz)

Straftaten zu vermeiden[62]. Dadurch, dass Täter häufig ihr Gesicht bedecken sind auch für die Strafverfolgung die Aufnahmen nur bedingt geeignet. Schließlich müsste der Täter direkt bei Begehung der Straftat gefilmt werden. Allein der Nachweis, dass eine bestimmte Person sich zu einer Zeit an einem Ort aufgehalten hat, an dem auch eine Straftat begangen worden ist, wird regelmäßig nicht ausreichen, um zu einer Verurteilung zu führen.

Bei einer nur abstrakten Gefährdung fehlt das berechtigte Interesse[63].

Die Videoüberwachung müsste darüber hinaus erforderlich sein, um den benannten Zweck zu erreichen. An das Erforderlichkeitsmerkmal müssen stets hohe Anforderungen gestellt werden. So ist eine Erforderlichkeit nur dann gegeben, wenn das vorgegebene Ziel mit der Überwachung auch tatsächlich erreicht werden kann und es dafür kein gleich wirksames, aber im Hinblick auf die informationelle Selbstbestimmung weniger einschneidendes Mittel gibt[64]. Ungeeignet in diesem Sinne sind Überwachungsanlagen, die der Aufklärung und Beweissicherung bei bereits begangenen Straftaten dienen sollen, aber von vornherein nicht geeignet sind, hinreichend sichere Rückschlüsse auf den Täter liefern zu können[65].

Oftmals sind gespeicherte Bildaufnahmen, die ein Fehlverhalten belegen sollen, trotz hochwertiger Kameratechnik wenig aussagekräftig. Verursacher sind häufig nicht eindeutig zu identifizieren, so dass nur eine Anzeige gegen Unbekannt aufgegeben werden kann. Darüber hinaus gerät eine Vielzahl unbeteiligter Personen in den Überwachungsbereich, deren schutzwürdige Interessen überwiegen.

Stehen mildere Mittel zur Verfügung um den benannten Zweck zu erreichen, sind diese in jedem Fall einer Videoüberwachung vorzuziehen.

Für Videoaufnahmen im nicht öffentlich zugänglichen Bereich bietet § 5a KDO keine Rechtsgrundlage.

Bei Bildaufnahmen von Personen handelt es sich um personenbezogene Daten im Sinne von § 2 Abs. 1 KDO. Nach § 3 Abs. 1 KDO ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit eine kirchliche oder staatliche Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

[62] Datenschutznachrichten Heft 3 2010, Seite 121. Zu den Ergebnissen einer Videoüberwachung in Hamburg bei der festgestellt worden ist, dass die Zahl der Straftaten trotz intensiver Videoüberwachung gestiegen ist.

[63] Fn. 13

[64] BGH NJW 2005, 313; Wedde in DKKW Kommentar zum BDSG § 6b Rn. 40

[65] Scholz in Simitis Kommentar zum BDSG § 6b Rn. 87

Eine entsprechende Rechtsvorschrift für die Anfertigung von Videoaufnahmen im nicht öffentlichen Bereich besteht nicht.
Eine Einwilligung aller betroffenen Personen, die von den Videoaufzeichnungen betroffen sind, existiert ebenfalls nicht. Die Einholung einer solchen Einwilligung bei allen Betroffenen dürfte sich in der Praxis als unmöglich erweisen, da nicht nur diejenigen zustimmen müssten, die sich in dem konkreten Bereich regelmäßig aufhalten, sondern auch deren Besucher.
Sofern Videoüberwachungen auch Mitarbeiter erfassen können, ist die Einrichtung mitbestimmungspflichtig gem. § 36 Abs. 1 Nr. 9 Mitarbeitervertretungsordnung (MAVO).
Im Falle einer Videoüberwachung greift § 3 Abs. 5 Nr.2 KDO, d.h. eine Vorabkontrolle ist durchzuführen, wenn die Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist.
Solche besonderen Risiken liegen bei einer Videoüberwachung regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden. Ebenso kann die verwendete Technik (etwa bei schwenkbaren Kameras mit hoher Auflösung der gewonnenen Bilder) zu einem solchen besonderen Risiko führen. Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte. Soweit ein solcher nicht bestellt ist, der Diözesandatenschutzbeauftragte, § 3 Abs. 6 KDO.
Nach Darlegung der Rechtslage in einem weiteren Gespräch mit der Heimleitung und dem IT-Verantwortlichen erklärte sich die Heimleitung damit einverstanden alle Videokameras zu entfernen. Auf ein förmliches Beanstandungsverfahren konnte deshalb verzichtet werden.

7. Vor-Ort-Kontrollen

Außerdem wurden von mir erste Einrichtungsbesuche vorgenommen, um festzustellen, ob die nach der KDO (§ 6 und Anlage zu § 6 KDO) erforderlichen technisch organisatorischen Maßnahmen eingehalten werden. In allen Einrichtungen, in denen personenbezogene Daten verarbeitet, gespeichert oder genutzt werden, müssen folgende Punkte überdacht werden:

7.1. Allgemein

- Alle Mitarbeiter, die mit der Erhebung, Nutzung und Verarbeitung personenbezogener Daten zu tun haben, sind gem. § 4 KDO schriftlich auf das Datengeheimnis zu verpflichten.
- Eine schriftliche Regelung zur privaten Nutzung von Telekommunikationsgeräten.
- Eine schriftliche Regelung zur privaten Nutzung von Internet und E-Mail

7.2. Zutrittskontrolle

- Unbefugte dürfen die Räume der Einrichtung nicht unbemerkt betreten können.
- Besucher werden im Eingangsbereich empfangen. Der Mitarbeiter, der besucht werden soll, wird von dem Mitarbeiter in der Pforte angerufen und holt den Besucher ab. Besucher dürfen sich in den Räumlichkeiten nur gemeinsam mit Mitarbeitern aufhalten.
- Mitarbeiter nutzen für den Zugang zum Haus und zu den Büros einen Schlüssel des Schließsystems.
- Die Schlüssel werden nach Verantwortungsbereich vergeben
- Sicherung der Räumlichkeiten in der Nachtzeit.
- Zugang zu den Räumlichkeiten in der Nachtzeit.
- Verteilung der Post so, dass nur der jeweilige Berechtigte auf seine Post zugreifen kann.
- Sicherung der IT-Systemräume.
- Sicherung der Räumlichkeiten der Meldestelle.
- Der Personalbereich ist so zu gestalten, dass Personen, die nicht zu diesem Bereich gehören, keine Möglichkeit haben Einblick auf Bildschirme oder in andere Unterlagen zu nehmen, die personenbezogene Daten enthalten.
- Regelungen die besagen, dass die Büros beim Verlassen abzuschließen sind, um einen fremden Zutritt auszuschließen.

7.3. Zugangskontrolle

- Wird eine Firewall verwendet?
- Ist eine Anti-Viren-Software im Einsatz?
- Bestehen Regelungen zur Authentifikation?

- Bestehen Regelungen, die Rechner beim Verlassen des Arbeitsplatzes zu sichern?
- Bestehen Regelungen Datenträger oder externe Endgeräte wie Smartphones, Tablets, Laptops u.ä. zu verschlüsseln?
- Bestehen Regelungen zur externen Nutzung hauseigener Geräte oder zur dienstlichen Nutzung privater Geräte?

7.4. Zugriffskontrolle

- Der Datenbestand wird jeweils nur den Mitarbeitern zugänglich gemacht, die damit arbeiten müssen.
- Werden Zugriffe, Anwendungen, insbesondere Eingabe, Änderung und Löschung von Daten, protokolliert?
- Wird beim Einsatz von Aktenvernichtern DIN 66399 eingehalten?
- Werden Datenträger, die nicht mehr gebraucht werden, physisch zerstört oder siebenfach überschrieben?
- Werden bei der Aktenvernichtung durch externe Dritte die Grundsätze der Auftragsdatenverwaltung beachtet?
-

7.5. Auftragskontrolle

- Werden die Auftragnehmer gem. § 8 Abs. 2 KDO schriftlich verpflichtet?
- Werden Vertragsstrafen für den Fall von Verstößen in den Verträgen vereinbart?
- Werden regelmäßige Kontrollen beim Auftragnehmer durchgeführt?

7.6. Weiterhin erforderlich sind

- Erstellung der Verfahrensverzeichnisse (Art. 30 EU-DSGVO
- Erstellung eines Datenschutzkonzepts für die Einrichtung
- funktionierende Backup-Lösungen,
- Aufbau sicherer E-Mail-Systeme - auch mit den kirchlichen Verbänden wie den Caritasverbänden,
- Einbeziehung der Ehrenamtlichen in ein sicheres E-Mail-System,
- Umsetzung der in der Anlage zu § 6 KDO vorgesehenen Kontrollsysteme (Zugangskontrolle, Zugriffskontrolle usw., Art. 32 der EU-DSGVO).

Bei den Besuchen konnte u.a. festgestellt werden, dass die in der KDO § 4 Satz 2 festgeschriebene Forderung nach einer schriftlichen Verpflichtung jedes mit der Verarbeitung personenbezogener Daten beschäftigten Mitarbeiters auf das Datengeheimnis selten erfüllt wird.
Darüber hinaus konnte festgestellt werden, dass den Verantwortlichen nicht in jedem Fall die in den Amtsblättern veröffentlichten Regelungen zum Datenschutz vertraut waren.
Ebenso sind regelmäßige Belehrungen der Mitarbeiter zum Datenschutz offensichtlich die Ausnahme.
Wohl nicht zuletzt aufgrund dieser mangelhaften Bekanntmachung datenschutzrechtlicher Vorschriften konnten in den Einrichtungen zum Teil erhebliche Datenschutzfehler festgestellt werden. (Gehaltsbestätigungen von Mitarbeitern liegen ausgedruckt auf zentralen Druckern und sind damit Dritten unkontrolliert zugänglich, Mitarbeitergehälter werden individualisiert der Finanzabteilung zur Verfügung gestellt, Büros sind trotz Abwesenheit für Dritte zugänglich, die Verwendung privater IT-Endgeräte und Speichermedien ist nicht geregelt bzw. die Regelungen sind nicht bekannt oder werden missachtet u.a.)

8. Datenschutz bei Internetauftritt und E-Mail-Nutzung

8.1. Datenschutzerklärung

Gemäß § 13 Abs. 1 Telemediengesetz muss ein Dienstanbieter den Nutzer des Telemediums (z.B. den Besucher der Homepage) zu Beginn des Nutzungsvorganges über Art, Umfang, Ort und Zwecke der Erhebung und Verwendung seiner personenbezogenen Daten in allgemein verständlicher Form unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.
Eine Online-Datenschutzerklärung sollte insbesondere zu folgenden Aspekten - soweit relevant - Aussagen aufweisen:

- Art der gespeicherten personenbezogenen Daten, deren Verwendungszweck und Aufbewahrungsdauer
- Behandlung von E-Mail-Adressen
- Sammlung personenbezogener Daten ohne Wissen der Betroffenen

- Einbindung eines externen Dienstleisters bei der Realisierung oder beim Betrieb einer Web-Site
- Inhaltliche Korrektheit personenbezogener Daten (Maßnahmen zur
- Offenlegung und Weitergabe personenbezogener Daten (z.B. nur bei Zustimmung oder aufgrund gesetzlicher Verpflichtung)
- Angebotene Vorkehrungen zur Wahrung der Sicherheit und Vertraulichkeit von online erhobenen personenbezogenen Daten (z.B. Angebot kryptografischer Verfahren und Protokolle)
- Betrieb eines Forums mit Pseudonymen
- Kontaktperson für weiterführende Fragen[66]

Analyse-Tools wie Google Analytics oder Piwik dürfen eingesetzt werden, wenn die ermittelten IP-Adressen anonymisiert werden. Hinzu kommt, dass nach Auffassung der Aufsichtsbehörden für den Datenschutz der Einsatz von Google Analytics oder Piwik einen Fall der Auftragsdatenverarbeitung darstellen, der nach den Vorschriften des BDSG und der KDO einen schriftlichen Vertrag zwischen dem Seitenbetreiber und dem des Analyse-Tools zwingend vorsieht.

8.2. Impressumspflicht

Wer einen Internetauftritt unterhält, ist grundsätzlich dazu verpflichtet, seine Identität bekannt zu machen und bestimmte Daten offen zu legen. Geregelt ist das in § 5 Telemediengesetz (TMG) unter der Überschrift „Allgemeine Informationspflichten“.
Von natürlichen Personen müssen Vor- und Zuname, und die vollständige Postanschrift (Straße, Hausnummer, Postleitzahl, Ort) angegeben werden. Nicht ausreichend ist die Angabe eines Postfachs oder nur einer E-Mail-Adresse.
Personengesellschaften und juristische Personen müssen die Firmenbezeichnung im handelsrechtlichen Sinn einschließlich des Rechtsformzusatzes und den Namen des Vertretungsberechtigten neben dem vollständigen Namen und der Anschrift angeben. Als Anschrift ist dabei der Sitz der Gesellschaft zu nennen. Vertretungsberechtigt sind Personen, die rechtlich verbindlich für die Gesellschaft handeln können.
Wichtig ist, dass das Impressum Angaben enthält, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen. Dies muss nach

[66] mit weiteren Beispielen datenschutz-bayern de.

der Rechtsprechung des Europäischen Gerichtshofes (EuGH) nicht zwingend eine Telefonnummer sein, eine elektronische Anfragemaske reicht insoweit aus.
Die Informationen müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein.

Leichte Auffindbarkeit

Die Informationen nach § 5 TMG müssen an gut wahrnehmbarer Stelle, ohne langes Suchen und jederzeit in der Sprache der Webseite auffindbar sein. Weiterhin müssen sie ohne spezielle Hilfsprogramme oder Einstellungen des Rechners (kein JavaScript-Popup) lesbar sein. Leicht erkennbar sind die Informationen, wenn die Möglichkeit einer einfachen und effektiven optischen Wahrnehmung besteht. Als Bezeichnungen haben sich „Impressum“ und „Kontakt“ eingebürgert.

Unmittelbare Erreichbarkeit

ist gegeben bei einer Zugangsmöglichkeit ohne wesentliche Zwischenschritte.
Der Aufwand für den Nutzer, der sich durch vier Bildschirmseiten scrollen muss um den einschlägigen Link „Impressum“ zu erreichen, dessen Platzierung am unteren Bildschirmrand zunächst nur vermutet werden kann, ist nach obergerichtlicher Rechtsprechung zu groß. Dabei kommt es nicht darauf an, ob der informierte und verständige Nutzer mit dem Scrollen als gängiger leicht zu bedienender Technik an sich vertraut ist.
Viermal klicken ist ebenfalls ein Verstoß gegen die Impressumspflicht.
Nach Auffassung des OLG Hamburg müssen die Informationen auch bei einer Bildschirmauflösung von 800 x 600 Pixel für den Nutzer ohne vorhergehendes scrollen erreichbar sein. Diese Ansicht wird aber in der Literatur überwiegend als überzogen abgelehnt.
Angaben in den AGB reichen jedoch nicht aus.

Ständig verfügbar

Solange die Seite online ist, muss auch der Link zum Impressum funktionieren. Ein Fehler wäre es das Impressum nur auf der Startseite zu verlinken. Das Impressum sollte von jeder einzelnen Unterseite aus direkt besucht werden können.

8.3. Weiterleitung von E-Mails

Eine Petentin richtet eine E-Mail an ihren Pfarrer. In der E-Mail ging es um Äußerungen der Petentin die eine vom Pfarrer betreute Auslandsreise betreffen. Die Äußerungen in der Mail fallen nicht unter das Beicht- oder Seelsorgegeheimnis.

Die Petentin hat in ihrer Mail nicht ausdrücklich darauf hingewiesen, dass der Inhalt der Mail vertraulich behandelt werden soll, ist aber gleichwohl davon ausgegangen, weil sie den Pfarrer ausdrücklich als solchen, also als eine Amtsperson, angesprochen hat.

Der Pfarrer hielt die Mail für „unmöglich“ und übermittelte sie an eine größere Zahl von Adressaten weiter.

Die Petentin fühlt sich durch die Weiterleitung in ihrem Persönlichkeitsrecht verletzt und fragt an, ob das Handeln des Pfarrers rechtmäßig gewesen sei.

Zunächst sind Geschäfts- und Privatbriefe weder gegen (weitere) Veröffentlichungen noch gar absolut gegen Kenntnisnahme geschützt, sofern der Wille des Verfassers oder Berechtigten zur Geheimhaltung nicht deutlich erkennbar ist.[67]. Dies gilt insbesondere bei E-Mails, bei denen wegen der problemlos möglichen Weiterverbreitung an einen größeren Empfängerkreis immer mit einer Weitergabe gerechnet werden muss[68].

Allerdings muss ein entsprechender Schutz wie bei Briefen gelten, wenn die Vertraulichkeit des Inhalts, bzw. ein die weitere Verbreitung entgegenstehender Wille in der Mail zutage tritt[69].

Eindeutige Hinweise für ein Verbot der Weitergabe können Hinweise wie „vertraulich“ „persönlich“ u. ä. sein, aber auch Anweisungen in sogenannten Disclaimern (Vorgefertigte Texte, die auf dem Brief, in der Regel am Ende, angebracht sind. Z. B. „Der Inhalt dieser Mail ist ausschließlich für den Empfänger bestimmt. Sollten Sie diese Mail erhalten haben ohne der richtige Empfänger zu sein, senden Sie bitte die Mail an den Absender zurück und löschen Sie sie in ihrem Posteingang.“)

Für Schweigeverpflichtete gem. § 203 StGB gilt ein Verbot der Weitergabe bereits aufgrund der strafgesetzlichen Vorschrift auch ohne ausdrücklichen Hinweis des Verfassers.

---

[67] OLG Stuttgart vom 10.11.2010 4 U 96/10 mit weiteren Hinweisen auf BVerfG NJW 1991, 2339; BGHZ 31, 308 [313]; Erman/Ehmann, BGB, 12. Aufl. 2008, Anh. § 12 Rn. 118

[68] Landgericht Saarbrücken vom 16.12.2011, AZ 4 O 287/11

[69] Landgericht Köln vom 02.10.2008, AZ 28 O 558/06

Amtspersonen, die vom Verfasser ausdrücklich als solche angesprochen werden (Sehr geehrter Pfarrer xy …), dürfen den Brief oder die Mail ebenfalls nicht weitergeben, da der Aussteller durch die Amtsbezeichnung deutlich macht, dass er Vertraulichkeit für seine Ausführungen beansprucht.

8.4. Weiterleitung von E-Mails bei Abwesenheit

Im Falle der Abwesenheit ist eine generelle Weiterleitung an Dritte (Arbeitskollegen, Vorgesetzte o.a.) abzulehnen. Eine solche allgemeine Weiterleitung führte dazu, dass auch persönliche oder vertrauliche, jedenfalls ausschließlich für den Empfänger bestimmte Mails, zur Kenntnisnahme von Dritten gelangen könnten.
Die Einrichtung einer Abwesenheitsmeldung (bin in der Zeit vom … bis … nicht per E-Mail erreichbar), ggf. mit einem Hinweis auf eine Vertretung in wichtigen Fällen, ist der richtige Weg.
Für Schweigepflichtige Personen im Sinne des § 203 StGB kann die automatische Einrichtung einer Weiterleitung strafbar sein!

8.5. E-Mail-Verteilerlisten (An, CC, BCC)

Bei E-Mail-Adressen handelt es sich um personenbezogene Daten i. S. der KDO
Die Weitergabe von E-Mail-Adressen ohne Zustimmung des Inhabers der Adresse ist ein Verstoß gegen die KDO.
Wenn mit einer Mail eine Vielzahl von Personen angesprochen werden soll, schreiben manche Nutzer die E-Mail-Adressen in das Anschriftenfeld (An) oder nutzen, wenn neben dem Empfänger weitere Personen mit einer Kopie bedacht werden sollen, das Feld „CC“. In diese Felder eingetragene E-Mail-Adressen sind für alle Empfänger sichtbar. Damit sind die Adressen weitergegeben. Dies ist rechtswidrig und wurde bereits von einem Landesdatenschutzbeauftragten mit einem Bußgeld geahndet.
Wenn eine größere Personenzahl angeschrieben werden soll, ist anzuraten in das Adressfeld den (eigenen) Absender einzutragen und alle Adressaten in das Feld „BCC“ (Blindkopie). Neben seiner eigenen E-Mail-Adresse sieht dann jeder Empfänger nur die Adresse des Absenders.

9. Gesetz gegen unerlaubten Wettbewerb (UWG)

Unerlaubte Telefonwerbung ist verboten.

Gem. § 7 Abs. 2 Nr. 2 UWG stellt ein Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung eine unzumutbare Belästigung dar.

Für Telefonwerbung gelten die Regelungen der staatlichen Rechtsnormen, insbesondere des UWG. Danach ist diese Art der Werbung nur bei vorheriger, ausdrücklicher schriftlicher Einwilligung in die entsprechende Datenerhebung und Nutzung zu Werbezwecken zulässig[70]. Da Sonderregelungen für kirchliche oder caritative Einrichtungen in diesem Gesetz nicht vorgesehen sind, gelten diese gesetzlichen Regelungen auch für den kirchlichen Bereich. Dies ist vom OLG Köln auch für den Bereich caritativer Einrichtungen bestätigt worden[71]. Die Konferenz der Diözesandatenschutzbeauftragten hat sich dieser Rechtsauffassung ausdrücklich angeschlossen und festgestellt, dass das Gesetz auch kirchliche Gesellschaften und Körperschaften bindet und telefonische Werbung ohne eine zuvor erteilte Zustimmung des Betroffenen zu unterlassen ist.

10. Ausblick

Trotz des erheblichen zeitlichen Aufwandes, den die Besuche von Einrichtungen zur Beratung oder Prüfung in Anspruch nehmen, ist es wichtig durch diese Besuche einen engen Kontakt zu den Einrichtungen, den betrieblichen Datenschutzbeauftragten und den dort beschäftigten Mitarbeitern herzustellen. Bei den Beratungen geht es stets darum, Sensibilität für den Datenschutz herzustellen und deutlich zu machen, dass Datenschutz die Persönlichkeitsrechte von Mitarbeitern und Klienten schützt.

Mitarbeiter insbesondere in den Caritaseinrichtungen werden durch einen funktionierenden Datenschutz davor bewahrt, auf Schadensersatz verklagt oder nach strafrechtlichen Vorschriften belangt zu werden. Wenn dies vermittelt werden kann, führt das regelmäßig dazu, dass die Verantwortlichen und Mitarbeiter einer Einrichtung bereit und daran interessiert sind, entsprechende Datenschutzregelungen gemeinsam mit dem Diözesandatenschutzbeauftragten zu erarbeiten.

[70] Landesbeauftragter für Datenschutz Baden-Württemberg, Datenschutz und Werbung S. 7
[71] Oberlandesgerichts Köln 6 U 69/12

Es ist mir ein Anliegen, durch Beratungen und Besuche der Einrichtungen, durch Veröffentlichungen u.ä. ein vertrauensvolles Verhältnis zwischen Mitarbeitern der Bistümer und Caritasverbände und dem Diözesandatenschutzbeauftragten herzustellen, damit die Mitarbeiter bereit sind, sich in Zweifelsfragen sofort an mich zu wenden, um selber Sicherheit zu gewinnen und Sicherheitslücken oder -probleme gar nicht erst entstehen zu lassen.

Mein Anspruch ist dabei, jede Anfrage unverzüglich zu bestätigen, eventuell bestehenden Klärungsbedarf telefonisch zu erörtern und kurzfristig eine schriftliche Antwort zu erteilen. Sollte dies nicht ausreichen, wird ein zeitnaher Ortstermin vereinbart.

Für das kommende Jahr sind regelmäßige Zusammenkünfte der betrieblichen Datenschutzbeauftragten mit dem Diözesandatenschutzbeauftragten geplant. Auf diesen Treffen sollen aktuelle Probleme besprochen werden. In einem Bistum sind solche Treffen bereits etabliert. Gleichzeitig sollen dort die betrieblichen Datenschutzbeauftragten zu bestimmten Themen geschult werden. Die Regelmäßigkeit der Treffen soll die Grundlage für ein vertrauensvolles und konstruktives Miteinander sein, auf dem der Datenschutz in den Bistümern aufgebaut werden soll.

Schließlich besteht Einigkeit zwischen den Diözesandatenschutzbeauftragten der katholischen Bistümer, eine regelmäßige Zusammenarbeit fortzusetzen, um Rechtsauslegungen und Stellungnahmen abzustimmen, damit in den einzelnen Diözesen nicht unterschiedliches Datenschutzrecht praktiziert wird. Neben den Konferenzen der Diözesandatenschutzbeauftragen, die zweimal jährlich stattfinden werden, gibt es kurzfristige Abstimmungen zu Einzelthemen im Rahmen von Videokonferenzen.

Da die Anforderungen an den Datenschutz nicht zuletzt wegen der neuen EU-DSGVO immer umfangreicher werden, ist der Diözesandatenschutzbeauftragte gefordert dafür zu sorgen, dass der Datenschutz in allen Einrichtungen der katholischen Kirche in der täglichen Arbeit berücksichtigt wird. Ein effektiver Datenschutz wird künftig zum Qualitätsmerkmal einer Einrichtung werden und damit auch Voraussetzung für die Förderung der jeweiligen Einrichtung durch die öffentliche Hand. Deshalb sehe ich mich verpflichtet nicht nur als Kontroll- und Prüfungsbehörde tätig zu sein, sondern in erster Linie auch als Berater und Koordinator.

Demnächst wird eine Internetseite freigeschaltet. Dort werden neben einem Stichwortverzeichnis Erklärungen zu datenschutzrelevanten Themen zu finden

sein, ebenso wie Gesetzes- bzw. Ordnungstexte, Erläuterungen, Stellungnahmen und Formulare.

Um das Amt des Diözesandatenschutzbeauftragten aktiv ausfüllen zu können und als Ansprechpartner für Datenschutzbelange in den ostdeutschen (Erz-) Bistümern präsent zu sein, sind die Verantwortlichen in den (Erz-) Bistümern gefordert dafür zu werben, den Diözesandatenschutzbeauftragten rechtzeitig in diesen Belangen zu involvieren. Dafür wird die Bereitschaft garantiert, Bereiche und Gremien der (Erz-) Diözesen zu besuchen um dort Erläuterungen zum Thema Datenschutz zu geben.

Anhang 1

Eckpunkte für eine Jubiläumsordnung

Bei Alters- und Ehejubiläen, Geburten, Sterbefällen, Ordens- und Priesterjubiläen können Namen der Betroffenen und ggf. deren Wohnort (nicht die Straße) sowie der Tag und die Art des Ereignisses in den Publikationsorganen der Pfarreien (Pfarrnachrichten) sowie in den kircheneigenen Printmedien veröffentlicht werden, wenn die Betroffenen der Veröffentlichung nicht schriftlich oder in sonstiger geeigneter Form bei der zuständigen Pfarrei widersprochen haben.

Auf das Widerspruchsrecht ist mindestens einmal jährlich in den Publikationsorganen der Pfarreien bzw. in den kircheneigenen Printmedien hinzuweisen. Der Hinweis ist im äußeren Erscheinungsbild von dem Rest des Textes der Veröffentlichung hervorzuheben. Ein bei der Pfarrei eingereichter Widerspruch ist unverzüglich der Meldestelle des Bistums mitzuteilen.

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 90. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 25., 50. und jedes weitere 5. Ehejubiläum.

Soll eine weitere über die genannten Medien hinausgehende Veröffentlichung, insbesondere eine solche im Internet erfolgen, ist die vorherige Zustimmung der Betroffenen einzuholen.

Die Meldestelle des Bistums ist berechtigt auf Anfrage einer der genannten Stellen die entsprechenden Daten zu übermitteln. Die Pfarreien sind berechtigt, die entsprechenden Daten an ein kircheneigenes Printmedium zu übermitteln.

Die Daten dürfen ausschließlich zu dem Zweck der Veröffentlichung in den genannten Medien verwendet werden.

Aus Sicherheitsgründen ist auf die Veröffentlichung der Straßenanschrift zu verzichten.
Ein „kircheneigenes Printmedium“ ist derzeit der „Tag des Herrn“.

Anhang 2

Betrieblicher Datenschutzbeauftragter gem. § 20 KDO

Einführung

Die Aufgabe des betrieblichen Datenschutzbeauftragten ist mit der Novellierung der KDO im Jahr 2006 unter dem § 18a eingeführt worden.
Kirchliche Stellen *konnten* nach dieser Vorschrift einen Datenschutzbeauftragten bestellen.
Mit der Neufassung der KDO im Jahr 2014 finden sich die Vorschriften über den betrieblichen Datenschutzbeauftragten in den §§ 20f. . Die Bestellung ist nunmehr differenzierter geregelt. Zwar entspricht § 20 Abs. 1 noch immer dem Wortlaut des alten § 18a, jedoch wurde diese Regelung durch den Abs. 2 ergänzt, nachdem ein betrieblicher Datenschutzbeauftragter bestellt werden *soll*, wenn mit der automatisierten Datenerhebung, -verarbeitung oder -nutzung mehr als zehn Personen befasst sind.

1. Ermessensausübung

Die Rechtsbegriffe „kann", „sollen" und „müssen" regeln das Ermessen der verpflichteten Stelle. Während der Begriff „kann" die jeweils verantwortliche Stelle lediglich zur Ausübung pflichtgemäßen Ermessens verpflichtet, räumt der Begriff „muss" kein Ermessen ein.[72]
Bei einer „Soll"-Vorschrift ist die verantwortliche Stelle im Regelfall zum Tätigwerden strikt verpflichtet. Wenn sie es nicht macht, muss sie nachweisen, dass ein atypischer Fall vorliegt. Es müssen konkrete, nicht von der zuständigen Stelle selbst zu vertretende Gründe für das Abweichen von der Norm sprechen.[73]
Um von einem atypischen Fall sprechen zu können, muss die Abweichung so bedeutend sein, dass das Geweicht der für die Regelentscheidung maßgeblichen Gründe beseitigt wird.[74] Da jeder Ortsbischof die KDO in seinem Bistum als eigenes Recht übernehmen muss, ist nicht davon auszugehen, dass eine Rechtsvorschrift eingeführt wird, deren Umsetzung den verpflichteten Stellen im Bistum nicht möglich ist. Aus diesem Grunde wird die Regelung des § 20 Abs. 2 trotz der Formulierung „soll" als eine „Muss-Vorschrift" betrachtet werden müssen.

2. personenbezogene Daten

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmbaren oder bestimmten natürlichen Person (§2 Abs. 1 KDO)

3. Automatisiertes Verfahren

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz einer Datenverarbeitungsanlage. (§ 2 Abs. 2 KDO).

[72] Bader/Ronellenfitsch Kommentar zum VwVfG 2010, § 40 Rn. 35
[73] Kopp/Ramsauer Kommentar zum VwVfG 16. Auflage 2015, § 40 Rn. 63
[74] Sachs in Stelkens/Bonk/Sachs Kommentar zum VwVfG 8. Auflage 2014 § 40 Rn. 27

4. Anzahl der Personen

Die Formulierung „Personen“ ist wörtlich zu verstehen. Auf das der Datenerhebung, -verarbeitung oder –nutzung zugrundeliegende Rechtsverhältnis kommt es deshalb nicht an. Deshalb ist eine Arbeitnehmereigenschaft im Sinne einer arbeitsvertraglichen Bindung an die verantwortliche Stelle nicht erforderlich. Leiharbeitnehmer, freie Mitarbeiter, Praktikanten und Auszubildende sind deshalb in die Anzahl mit einzubeziehen. So auch die Durchführungsverordnung zur KDO zu § 4 KDO: Zum Kreis der bei der Datenverarbeitung tätigen Personen … gehören die in den Stellen gem. § 1 Abs. 2 KDO gegen Entgelt beschäftigten und ehrenamtlich tätigen Personen.[75]
Jede Person ist unabhängig vom Umfang ihrer Tätigkeit als eine Person zu zählen. Eine unterschiedliche Berechnung nach dem Umfang des Beschäftigungsverhältnisses, wie sie das Kündigungsschutzgesetz kennt, ist nicht vorzunehmen. Ebenso ist unerheblich, welchen Anteil der Arbeitszeit die Person mit der Datenverarbeitung verbringt.

Entgegen der Parallelvorschrift des BDSG sieht die KDO keine „regelmäßige“ Beschäftigung von mehr als zehn Personen vor, sondern formuliert absolut (sind … befasst). Gleichwohl ist auch hier davon auszugehen, dass temporäre Schwankungen nicht dazu führen, dass die Verpflichtung einen betrieblichen Datenschutzbeauftragten zu bestellen entfällt oder ein bereits bestellter betrieblicher Datenschutzbeauftragter seine Verpflichtung verliert, weil die Zahl der Personen vorübergehend unter elf sinkt.[76]

5. Zuordnung
Kirchliche Stellen im Sinne des § 1 Abs. 2 KDO sind solche, die eine eigene Rechtspersönlichkeit besitzen. Rechtlich unselbständige Einrichtungen benötigen keinen eigenen betrieblichen Datenschutzbeauftragten, sondern gehören in den Zuständigkeitsbereich des betrieblichen Datenschutzbeauftragten der rechtlich selbständigen Einheit. In organisatorischer Hinsicht erscheint es sinnvoll, dem zuständigen Datenschutzbeauftragten in einem solchen Fall „Hilfskräfte“ für die einzelnen unselbständigen Einheiten an die Seite zu stellen. Für diese „Hilfskräfte“ gelten dann aber nicht die Regelungen führt den betrieblichen Datenschutzbeauftragten. Insbesondere genießen diese nicht den Kündigungsschutz des § 20 Abs. 6 KDO.
Soweit Kirchlichen Stellen im Sinne des § 1 Abs. 2 KDO mehrere selbständige Einheiten angehören, ist jede von ihnen verpflichtet, einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen. (So macht es einen Unterschied, ob die Schulen eines Bistums einer selbständigen Stiftung angehören, dann ist für diese Stiftung ein betrieblicher Datenschutzbeauftragter zu bestellen, oder ob die Schulen unselbständige Einrichtungen sind, die von einer Abteilung des betreffenden Ordinariates/Generalvikariates verwaltet werden. Für letztere ist der betriebliche Datenschutzbeauftragte dieses Generalvikariates verantwortlich.[77])

[75] KDO-DVO i.d.F. des Beschlusses der Rechtskommission vom 19.03.2015, II. Zu § 4 KDO
[76] Zum BDSG Simitis § 4f Rn. 19
[77] Zur Parallelvorschrift des BDSG Simitis § 4 f Rn. 39

6. Wahlfreiheit

In § 20 Abs. 3 S. 2 räumt die KDO der verantwortlichen Stelle die Wahlmöglichkeit zwischen einem internen und einem externen betrieblichen Datenschutzbeauftragten ein. Nach der Ordnung sind beide Möglichkeiten gleichrangig, so dass es allein eine Entscheidung der verantwortlichen Stelle ist, für welche Möglichkeit sie sich entscheidet.
Hat sich die verantwortliche Stelle jedoch eine der beiden Möglichkeiten entschieden, so kann sie diese Entscheidung bis zum Ablauf der Frist für die die Entscheidung getroffen worden ist nicht widerrufen. Die Zulassung einer jederzeitigen Widerrufsmöglichkeit aufgrund einer organisatorischen Neuentscheidung und die Anerkennung einer freien Strukturentscheidung als wichtiger Grund würden dazu führen, dass der besondere Abberufungsschutz zur Disposition der verantwortlichen Stelle führt.[78]

7. Natürliche oder juristische Person

Die KDO legt mit dieser Formulierung ebenso wie die Parallelvorschrift des BDSG nahe, dass es sich um eine natürliche Person handeln müsse. Tatsächlich wird dies auch vertreten.[79] Eine ausdrückliche Festlegung durch die KDO auf natürliche Personen besteht aber nicht, deshalb ist der Gegenauffassung der Vorrang einzuräumen, die auch eine Übertragung dieser Aufgabe an juristische Personen für möglich hält[80]. Insbesondere greift die Argumentation nicht, dass nur eine natürliche Person über die geforderte Fachkunde und Zuverlässigkeit verfügen können[81]. Gegenüber der verantwortlichen Stelle ist die juristische Person Ansprechpartner, die aus ihrem Kreis einen kompetenten Bearbeiter auswählt. Im Rahmen zunehmender Komplexität der datenschutzrechtlichen Fragestellungen dürfte das kein Negativkriterium sein.
Unabhängig davon, ob der betriebliche Datenschutzbeauftragte ein interner oder externer ist, handelt es sich bei dieser Person nicht um einen „Dritten“ i. S. von § 2 Abs. 9 S. 2 KDO.

8. Fachkunde und Zuverlässigkeit

Die KDO fordert Fachkunde und Zuverlässigkeit für die Bestellung zum betrieblichen Datenschutzbeauftragten. Insoweit sind rechtliche, organisatorische und technische Kenntnisse gefordert, ohne dass es ein bestimmtes Anforderungsprofil gibt[82], oder ein umfassendes Allround-Wissen gefordert werden könnte[83]. Die geforderte Fachkunde darf insofern nicht mit der Forderung nach ausgeprägtem Spezialwissen in rechtlichem, organisatorischem oder technischem Bereich gleichgesetzt werden.[84] Fachkunde bedeutet zunächst, dass der

[78] BAG vom 23.03.2011 – 10 AZR 562/09; NZA 2011, 1036, 1037
[79] Däubler in DKWW § 4f Rn. 22; Schierbaum AiB 2001, 514; ders. PersR 2011, 454, 455
[80] Simitis, § 4f Rn. 48
[81] Bergmann/Möhrle/Herb § 4f Rn. 93
[82] Simitis, § 4f Rn. 84
[83] Däubler DKWW § 4f Rn. 28
[84] Simitis § 4f Rn. 93; zu weit gehend insofern der sog. „Ulmer Beschluss“ LG Ulm, 5 T 152/90-01 wenn gefordert wird, dass es sich bei dem betrieblichen Datenschutzbeauftragten um einen „Computerexperten“ handeln muss.

Datenschutzbeauftragte die gesetzlichen Regelungen kennt und sicher anwenden kann.[85] Richtungsweisend für die Anforderungen an die Fachkunde sind die vom Düsseldorfer Kreis am 24./25. November 2010 beschlossenen Mindestanforderungen.[86]

Der Begriff der Zuverlässigkeit umfasst zum einen sorgfältige und gründliche Arbeitsweise, Belastbarkeit, Lernfähigkeit, Loyalität und Gewissenhaftigkeit. Zum anderen darf es keine Interessenskonflikte der Aufgabe des betrieblichen Datenschutzbeauftragten mit anderen hauptamtlichen Aufgaben des Datenschutzbeauftragten geben.[87]
Im Rahmen der Zuverlässigkeit ist insbesondere zu prüfen, ob Interessenkollisionen der Bestellung zum betrieblichen Datenschutzbeauftragten entgegenstehen können. Hierbei setzt eine verlässliche Kontrolle eine klare Trennung zwischen dem betrieblichen Datenschutzbeauftragten und der verantwortlichen Stelle voraus.[88]

8.1.
Fraglich im kirchlichen Bereich erscheint es, ob Mitglieder eines Ordinariatsrates als betriebliche Datenschutzbeauftragte bestellt werden können oder ob dem die Nähe zur Leitung der verantwortlichen Stelle entgegensteht.
Für den staatlichen Bereich wird dies für leitende Mitarbeiter in der Literatur uneinheitlich beantwortet.
Die bloße Zugehörigkeit zu dieser Gruppe allein soll noch keinen Hinderungsgrund darstellen.[89] Vielmehr soll es auf die weitere Tätigkeit ankommen und darauf, ob diese mit der Verarbeitung personenbezogener Daten zusammenhängen oder darauf Einfluss haben.[90] Dies wird in Ordinariatsräten regelmäßig der Fall sein, da in diesen Gremien „die Fäden zusammenlaufen“, in dem Sinne, dass dort Personal- Rechts- Finanzfragen besprochen werden.
Im Falle des Ordinariatsrates ist darüber hinaus zu beachten, dass mit der Mitgliedschaft in diesem Gremium regelmäßig die als Titel geführte Bezeichnung „Ordinariatsrat“ / „Ordinariatsrätin“ von den Mitgliedern geführt wird. Dieser Titel genießt im kirchlichen Wirkungskreis Anerkennung und zeichnet den Träger aus. Gleichwohl gibt es regelmäßig keine Titelordnung, die einen Anspruch auf diesen Titel gewährt. Auch die bloße Mitgliedschaft in dem Gremium führt nicht in allen Bistümern dazu, dass dessen Mitglieder den persönlichen Titel „Ordinariatsrat“ / Ordinariatsrätin“ führen dürfen. Dieser persönliche Titel wird durch den jeweiligen Bischof verliehen oder entzogen. Wenn mit dem persönlichen Titel jedoch ein Status nach außen verbunden ist und der Titelträger sich dessen bewusst ist, dass

[85] Bundesbeauftragte für Datenschutz und Informationsfreiheit, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“, S. 12
[86] Abgedruckt u. a. in Bundesbeauftragte für Datenschutz und Informationsfreiheit, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“, Anhang 9
[87] Der betriebliche Beauftragte für den Datenschutz des Landes Baden- Württemberg Handreichung für die Bestellung zum betrieblichen Datenschutzbeauftragten - Stand: 17. Juni 2014 -, S. 5
[88] BAG 22.03.1994 – 1 ABR 51/93, DB 1994, 1678
[89] Bergmann/Möhrle/Herb § 4f Rn. 109; Simitis § 4f Rn. 99; a. A. “höchst fraglich” Tinnefeld CR 1991, 29, 32; “ungeeignet” Däubler DKWW § 4f Rn. 31
[90] Simitis § 4f Rn. 99

ihm der Titel jederzeit entzogen werden kann, wird er kaum geneigt sein eine kritische Distanz gegenüber der Bistumsleitung an den Tag zu legen, die ggf. im Sinne des Datenschutzes erforderlich ist.
Eine Beauftragung eines Mitgliedes des Ordinariatsrates ist mithin abzulehnen.

8.2.
Die Bestellung eines Justitiars zum Datenschutzbeauftragten ist für das staatliche Recht umstritten. Das tragende Argument der Gegner ist dabei die Behauptung, dass das Datenschutzrecht von zahlreichen unbestimmten Rechtsbegriffen geprägt ist und so einen weiten Auslegungsspielraum eröffnet, der von Justitiaren regelmäßig im Interesse der verantwortlichen Stelle und „eines reibungslosen Arbeitsablaufs“[91] interpretiert werden[92]. Eine derartige Unterstellung erscheint nicht schlüssig, insbesondere ist nicht nachvollziehbar, warum diese nicht für andere Mitarbeiter in gleicher Weise gelten sollte. Ein Justitiar, wie auch ein beratender Rechtsanwalt ist ständig damit konfrontiert, etwaige Interessenkollisionen aufzulösen und wird seinem Arbeitgeber bzw. seinem Mandanten regelmäßig eine rechtskonforme Lösung vorschlagen. Eine Interessenwahrung für die verantwortliche Stelle steht regelmäßig überhaupt nicht in Widerspruch zur Gewährleistung des gesetzlichen Standards im Datenschutz.[93] Problematisch werden kann die Doppelfunktion allerdings dann, wenn der Datenschutzbeauftragte und Justitiar in Gerichtsprozessen gegen Mitarbeiter oder in Disziplinarverfahren tätig wird.[94]

8.3.

Die für die EDV-Abteilung verantwortliche Person, sowie der/die Leiter/in des Meldewesens kann nicht zum nebenberuflichen betrieblichen Datenschutzbeauftragten bestellt werden.[95] Dies ist nachvollziehbar, da die betreffenden Personen sich selbst kontrollieren müssten. Dies ließe sich mit organisatorischen Maßnahmen nicht ausgleichen und führte dazu, dass der Leiter der EDV bzw. des Meldewesens Ansprüchen ausgesetzt wäre, die einander widersprechen.

8.4.
Leiter und Mitglieder der Personalabteilungen können nach h. M. in Literatur und den Hinweisen der Landesdatenschutzbeauftragten sowie der Bundesbeauftragten für Datenschutz und Informationsfreiheit nicht zum betrieblichen Datenschutzbeauftragten bestellt werden.[96]
8.5

[91] Däubler in DKWW § 4f Rn. 31
[92] Simitis § 4f Rn. 103
[93] Taeger/Gabel Kommentar zum BDSG § 4f Rn 74; Bergmann/Möhrle/Herb § 4f Rn. 103
[94] Die BfDI, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“ S. 15
[95] Für den Leiter der EDV-Abteilung Simitis § 4f Rn. 100; Erfurter Komentar zum Arbeitsrecht BDSG §4f Rn. 5; Däubler DKWW § 4f Rn. 31; BfDI, Fn. 19, S. 14
[96] Statt vieler: Simitis § 4f Rn. 102 m.w.N; https://www.bfdi.bund.de/bfdi_wiki/index.php/Interessenkonflikte_nebenamtlicher_Datenschutzbeauftragter, zuletzt eingesehen am 10.04.2016

Leiter der Revision können zu betrieblichen Datenschutzbeauftragten bestellt werden. Die gegenteilige Ansicht, die eine gleichzeitige Bestellung des Mitarbeiters der Revision als betrieblicher Datenschutzbeauftragter mit dem Argument ablehnt, der Revisor sei in erster Linie der Wirtschaftlichkeit verpflichtet[97], ist abzulehnen. Als Kontrolleure sind Mitarbeiter der Revision ihrem Revisionsauftrag verpflichtet, der sich keinesfalls ausschließlich in wirtschaftlichen Themenstellungen erschöpfen muss, sondern darüber hinaus auch die Prüfung betrieblicher und gesetzlicher Regelwerke umfassen kann.[98]

8.6.

Mitglieder der Mitarbeitervertretung können als betriebliche Datenschutzbeauftragte bestellt werden. Dies ergibt sich bereits aus den gleichgerichteten Interessen des Datenschutzbeauftragten und des MAV-Mitgliedes, die u. a. in der konsequenten Umsetzung des Datenschutzgesetzes bestehen.[99] Wollte man Mitarbeitervertreter generell als ungeeignet ansehen, würde dies auf eine Benachteiligung gegenüber anderen Arbeitnehmern hinauslaufen.[100] Seit einer Entscheidung des Bundesarbeitsgerichtes im Jahr 2011 ist diese Frage für Betriebsratsmitglieder entschieden.[101]

9. Bestellung einer Person für eine andere verantwortliche Stelle desselben Bistums

Wenn jede selbständige juristische Person einen betrieblichen Datenschutzbeauftragten zu benennen hat, soweit die weiteren Voraussetzungen gegeben sind (s.o. 5.), kann eine Person, die bei einer verantwortlichen Stelle beschäftigt ist, und dort wegen der von ihr wahrgenommenen Haupt-Tätigkeit für die Übertragung der Funktion des betrieblichen Datenschutzbeauftragten nicht geeignet ist dennoch betriebliche Datenschutzbeauftragte der anderen verantwortlichen Stelle sein. Z.B. kann der IT-Verantwortliche des Ordinariates zum betrieblichen Datenschutzbeauftragten des Caritasverbandes des Bistums bestellt werden. Ebenso könnte der Personalleiter des Caritasverbandes zum betrieblichen Datenschutzbeauftragten im Ordinariat bestellt werden. Der Interessenkonflikt, der diese Personen in der eigenen Stelle hindert die Funktion als betrieblicher Datenschutzbeauftragter zu übernehmen ist in der selbständigen Einrichtung, der er nicht angehört, nicht gegeben.
Dies ergibt sich auch aus der Regelung des § 20 Abs. 3 a. E.

10. Bestellung

[97] Simitis § 4f Rn. 104
[98] So im Ergebnis auch Däubler, DKWW § 4f, Rn. 31; Reinhard NZA 2013, 1049 ff.
[99] Für den Betriebsrat: Bommer ZD, 2015, 123; Däubler Gläserne Belegschaften? Rn. 596; eher ablehnend BfDI, Info 4 „Die Datenschutzbeauftragten in Behörden und Betrieb“ S. 16
[100] Däubler DKWW § 4f Rn. 32; a. A. Bergmann/Möhrle/Herb § 4f Rn. 105
[101] BAG v. 23.03.2011 – 10 AZR 562/09; NZA 2011,1036

Die Bestellung hat gem. § 20 Abs. 1 schriftlich zu erfolgen. Dies gilt sowohl für eine Bestellung nach § 20 Abs. 1 als auch für eine solche nach § 20 Abs. 2, auch wenn dort das Schriftformerfordernis nicht ausdrücklich noch einmal wiederholt wird.
Die Schriftform ist konstitutiv. Ohne eine schriftliche Bestellung ist diese unwirksam. [102]
Eine Bestellung gegen den Willen des Arbeitnehmers ist nicht möglich, da sowohl die Bestellung als auch die Abberufung als betrieblicher Datenschutzbeauftragter eine Änderung des Arbeitsvertrages bedeuten, die vom Arbeitnehmer angenommen werden muss.[103] Aus diesem Grunde ist der h. M. zu folgen, nach der eine Bestellungsurkunde vom betrieblichen Datenschutzbeauftragten mit zu unterschreiben ist.[104]

11. Ende der Bestellung

Die Verweisung in § 20 Abs. 8 auf § 16 ist unglücklich. Einigkeit besteht wohl darüber, dass zur Berufung für den betrieblichen Datenschutzbeauftragten die Befähigung zum Richteramt nicht vorliegen muss. Die in § 20 Abs. 8 angesprochenen „übrigen Voraussetzungen“ betreffen dann die Befristung der Bestellung sowie den Widerruf der Bestellung.

11.1. Befristung

Die Bestellung des betrieblichen Datenschutzbeauftragten kann gem. § 16 Abs. 1 auf die § 20 Abs. 8 verweist nur befristet erfolgen. Dabei ist eine Befristung zwischen vier und acht Jahren möglich. Wenn in der Berufungsurkunde keine Frist festgeschrieben ist, ist im Sinne der Wahrung der Unabhängigkeit des Datenschutzbeauftragten von der längsten Frist auszugehen.

11.2. Abberufung

Eine Abberufung des betrieblichen Datenschutzbeauftragten ist gem. § 20 Abs. 8 nur in den Fällen des § 16 Abs. 3 möglich.

11.3. Amtsniederlegung

Darüber hinaus endet die Beauftragung, wenn der betriebliche Datenschutzbeauftragte sein Amt niederlegt. Dies ergibt sich aus der Verweisung von § 20 Abs. 8 auf § 16 Abs. 3 a. E. Statt des Bischofs hat die verantwortliche Stelle, die den betrieblichen Datenschutzbeauftragten bestellt hat die Bestellung zurück zu nehmen, wenn der betriebliche Datenschutzbeauftragte dies beantragt. Eine „Niederlegung“ des Amtes ist als ein solcher Antrag zu verstehen.

---

[102] Simitis § 4f ,Rn. 59; Däubler § 4f Rn. 25
[103] BAG vom 13.03.2007 -9 AZR 612/05, Der Betrieb 2007, 1198, 1200
[104] Bergmann/Möhrle/Herb § 4f Rn. 55f.; Simitis § 4f Rn. 57; Däubler in DKWW § 4f Rn. 25; In der Info 4 der BfDI ist dies in dem Muster der Anlage 9 nicht berücksichtigt, jedoch auf der Internetseite der BfDI http://www.bfdi.bund.de/DE/Infothek/Gesetze_Rechtsprechung/RechtsprechungDS/BDSG_Allgemein/Artikel/130307_BAG_BestellungDatenschutzbeauftragter.html?__lang=en (zuletzt eingesehen 11.04.2016) ausdrücklich aufgeführt.

Anhang 3a

Vereinbarung zur Anfertigung und Nutzung von Fotos außerhalb der Bildungs- und Entwicklungsdokumentation:

Für mein/unser Kind…… erkläre/n ich/wir:

Ich/Wir bin/sind darüber informiert worden, dass das Anfertigen jeglicher Fotos von Kindern und anderen Personen, die sich in der Kindertagesstätte „St. Johannes“ aufhalten verboten ist. Mir ist von der Einrichtung mitgeteilt worden, dass ein Verstoß gegen dieses Verbot mit der Kündigung des Betreuungsvertrages geahndet werden kann. Unabhängig davon behält sich die Einrichtung in einem solchen Fall darüber hinaus vor, rechtlich, auch strafrechtlich gegen die Handelnden vorzugehen.

[ ] JA [ ] Nein

Ich/Wir willige/n ein, dass Fotos von meinem/unserem Kind durch Mitarbeiter der Einrichtung angefertigt werden.

[ ] JA [ ] NEIN

_____

Vor einer Veröffentlichung oder einer anderen Nutzung von Fotos die mein/unser Kind zeigen, ist zu den konkreten Aufnahmen meine/unsere Einwilligung einzuholen.

[ ] JA [ ] NEIN

_____

Analoge Fotos meines/unseres Kindes die mein/unser Kind nicht unvorteilhaft abbilden, dürfen auch ohne meine/unsere vorherige Zustimmung im Innenbereich der Einrichtung ausgehängt werden.

[ ] JA [ ] NEIN

_____

Analoge Fotos meines/unseres Kindes, die mein/unser Kind nicht unvorteilhaft mit anderen Kindern abbilden, dürfen an die Erziehungsberechtigten der anderen Kinder herausgegeben werden.

[ ] JA [ ] NEIN

_____

Analoge Fotos meines/unseres Kindes die mein/unser Kind nicht unvorteilhaft abbilden, dürfen auch ohne meine/unsere vorherige Zustimmung im von außen einsehbaren Schaukasten der Einrichtung und/oder der Kirchengemeinde ausgehängt werden.

[ ] JA [ ] NEIN

_____

Ich/Wir stimme/n zu, dass digitale Fotos meines/unseres Kindes in der Tagespresse sowie im „Tag des Herrn“ veröffentlicht werden dürfen, um das Alltagsgeschehen und die Aktivitäten der Einrichtung zu dokumentieren. Dabei ist mir/uns bewusst, dass diese Medien regelmäßig auch über das Internet einzusehen sind und auf das Foto meines/ unseres Kindes weltweit zugegriffen werden kann.

[ ] JA [ ] Nein

_____

Ich/Wir bin/ sind darüber belehrt worden, dass eine einmal gegebene Einwilligungserklärung jederzeit gegenüber der Leitung der Kindertageseinrichtung oder dem Träger widerrufen werden kann.

[ ] JA [ ] Nein

_____

Datum Unterschriften

Anhang 3b

Einwilligungserklärung zum Umfang einer Bildungs- und Entwicklungsdokumentation (Portfolio) in der Einrichtung _____

Ich/Wir willige/n ein, dass für mein/unser Kind eine Bildungs- und Entwicklungsdokumentation (Portfolio) geführt wird.

[ ] JA [ ] NEIN

Ich/Wir willige/n ein, dass für die Bildungs- und Entwicklungsdokumentation Fotos, die unser Kind zeigen, erstellt und verwendet werden:

[ ] JA [ ] NEIN

Ich/Wir willige/n ein, dass Fotos, auf denen mein/unser Kind mit abgebildet ist, in der Bildungs- und Entwicklungsdokumentation eines anderen Kindes verwendet werden:

[ ] JA [ ] NEIN

Ich/Wir willige/n ein, dass Fotos, auf denen mein/unser Kind mit abgebildet ist, und die in die Bildungs- und Entwicklungsdokumentation eines anderen Kindes aufgenommen worden sind, bei der Aushändigung dieser Bildungs- und Entwicklungsdokumentation an die Erziehungsberechtigten des anderen Kindes in der Dokumentation verbleiben dürfen:

[ ] JA [ ] NEIN

Ich/Wir willige/n ein, dass Ton- und Videoaufzeichnungen im Rahmen der Bildungs- und Entwicklungsdokumentation von meinem/unserem Kind angefertigt werden. Diese dürfen ausschließlich für den Zweck verwendet werden, Interessen, Fähigkeiten und den Entwicklungsverlauf meines/unseres Kindes zu veranschaulichen und so Hinweise für dessen individuelle Förderung zu bekommen. Diese Informationen dienen ausschließlich für Beratungen in Entwicklungsgesprächen mit mir/uns und den Erzieherinnen und Erziehern. Diese Aufzeichnungen werden umgehend gelöscht, wenn der genannte Zweck erreicht ist, spätestens mit Ausscheiden des Kindes aus der Einrichtung.

[ ] JA [ ] NEIN

Ich/Wir bin/ sind darüber belehrt worden, dass eine einmal gegebene Einwilligungserklärung jederzeit gegenüber der Leitung der Kindertageseinrichtung oder dem Träger widerrufen werden kann. Der Widerruf sollte am besten schriftlich erfolgen.

[ ] JA [ ] Nein

Ich/Wir bin/ sind darüber belehrt worden, dass ich/wir gemeinsam mit einem Vertreter der Einrichtung in die von meinem/unseren Kind erstellten Dokumentationen Einsicht nehmen dürfen.

[ ] JA [ ] Nein

Die o. g. Fotos und Unterlagen werden den Berechtigten auf Wunsch in analoger Form ausgehändigt, soweit sie zur Verfolgung des dargestellten Zwecks nicht mehr benötigt werden. Spätestens wenn das Kind die Einrichtung verlässt, werden über das Kind erstellte analoge Dokumentationen von der Einrichtung ordnungsgemäß vernichtet, soweit die Berechtigten die Aushändigung nicht gewünscht haben. Die Einrichtung verpflichtet sich darüber hinaus evtl. bestehende digitale Dokumentationen (Fotos und Dateien) zu löschen, wenn sie zur Verfolgung des dargestellten Zwecks nicht mehr benötigt werden, spätestens mit dem Ausscheiden des Kindes aus der Einrichtung.

Ich bin darüber informiert worden, dass das Anfertigen jeglicher Fotos von Kindern und anderen Personen, die sich in der Einrichtung „Katholisches Kinderhaus Arche“ aufhalten verboten ist. Mir ist von der Einrichtung mitgeteilt worden, dass ein Verstoß gegen dieses Verbot mit der Kündigung des Betreuungsvertrages geahndet werden kann. Unabhängig davon behält sich die Einrichtung in einem solchen Fall darüber hinaus vor rechtlich auch strafrechtlich gegen die Handelnden vorzugehen.

[ ] JA [ ] NEIN

Datum | Unterschriften