2. Tätigkeitsbericht des Diözesandatenschutzbeauftragten der ostdeutschen Bistümer

gemäß § 18 Abs. 3 KDO

Berichtszeitraum 01.01.2017 bis 31.12.2017

„Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, der wird am Ende beides verlieren.“

(Benjamin Franklin)

2. Tätigkeitsbericht des Diözesandatenschutzbeauftragten für

das Erzbistum Berlin
das Bistum Dresden-Meißen
das Bistum Görlitz
das Bistum Erfurt
das Bistum Magdeburg

Inhaltsverzeichnis

Abkürzungsverzeichnis

APuZ	Aus Politik und Zeitgeschichte
ArztR	Arzt Recht
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGH	Bundesgerichtshof
BGHZ	Entscheidung des Bundesgerichtshofes im Zivilsachen
BVerfGE	Bundesverfassungsgerichtsentscheidung
CR	Computer und Recht (Zeitschrift)
DKWW	Däubler, Klebe, Wedde, Weichert
DMW	Deutsche Medizinische Wochenschrift
DuD	Datenschutz und Datensicherheit
KDO	Kirchliche Datenschutzordnung
KDG	Kirchrchliches Datenschutzgesetz
KuR	Kirche und Recht
LbfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
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

Vorwort

Die Arbeit des Diözesandatenschutzbeauftragten war auch im zweiten Jahr weithin geprägt vom Aufbau eines Datenschutznetzwerkes in den angeschlossenen Bistümern. Zunächst konnte erreicht werden, dass alle Bistümer einen betrieblichen Datenschutzbeauftragten berufen haben. Die Caritasdiözesanverbände haben, bis auf einen Verband, ebenfalls betriebliche Datenschutzbeauftragte berufen. Die regionalen Verbände der Caritas haben betriebliche Datenschutzbeauftragte bestellt, soweit sie als eigenständige juristische Personen dazu verpflichtet sind.

Für die verschiedenen Bereiche der betrieblichen Datenschutzbeauftragten wurden entsprechende Arbeitskreise gegründet (z. B. Caritas, Krankenhäuser, Ordinariate, Schulen). Diese treffen sich in regelmäßigen Abständen mehrmals im Jahr zum Erfahrungsaustausch mit der Datenschutzaufsicht.

Des Weiteren lag ein Schwerpunkt der Tätigkeit auf Vortragsveranstaltungen in den verschiedenen Einrichtungen des Zuständigkeitsbereiches. Hierdurch konnte das Thema Datenschutz weithin erfolgreich vermittelt werden. Dies führte, neben der Bereitschaft betriebliche Datenschutzbeauftragte zu bestellen, vor allem zu häufigen Konsultationen und Beratungen der Einrichtungen in den angeschlossenen Bistümern.

Der vorliegende Bericht ist gegliedert nach den Anforderungen des § 18 Abs. 3 KDO. Die Ausführungen unter Punkt 7. „Beispiele aus der Tätigkeit der Datenschutzaufsicht“ sind keineswegs abschließend, sondern enthalten Informationen, die auch für andere Einrichtungen hinweisgebend sein können.

Insbesondere die gehäuften Rückfragen und Vortragsanfragen in den letzten Wochen des vergangenen Jahres machen deutlich, dass das Thema Datenschutz verstärkt in den Fokus der verantwortlichen Stellen rückt. Es ist zu erwarten, dass im Jahr 2018 der Datenschutz deutlich an Aufmerksamkeit gewinnen wird. Nicht zuletzt durch die Änderungen, die das neue Kirchliche Datenschutzgesetz (KDG) verlangt, wird die Bestellung betrieblicher Datenschutzbeauftragter zunehmen und die Notwendigkeit eines funktionierenden Datenschutzes damit in die Fläche tragen.

1. EU-DSGVO

Die datenschutzrechtliche Diskussion in Deutschland war im vergangenen Jahr maßgeblich bestimmt von den Fragen, die im Zusammenhang mit der Umsetzung der EU Datenschutzgrundverordnung (EU-DSGVO) stehen. Mit dieser Regelung sollte erstmals in allen Mitgliedstaaten der EU ein einheitliches Datenschutzrecht geschaffen werden. Von einigen Kommentatoren in Politik und Schrifttum wurde dies als Quantensprung für den Datenschutz gefeiert. Die vom Europäischen Parlament am 14. April 2016 verabschiedete und am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlichte Verordnung wird gem. Art. 99 Abs. 2 EU-DSGVO ab dem 25.05.2018 in allen Mitgliedstaaten geltendes Recht sein. Bereits jetzt zeigt sich jedoch, dass es zwar einen einheitlichen Text gibt, dieser aber in den 28 Mitgliedstaaten, nicht zuletzt wegen der dort bestehenden bisherigen Datenschutzbestimmungen, unterschiedliche Auslegungen erfährt. Es ist deshalb zu erwarten, dass es noch Jahre dauern wird, bis durch den Europäischen Gerichtshof eine gefestigte Auslegung zur Verordnung etabliert ist.

Bislang haben erst zwei Staaten von der Möglichkeit Gebrauch gemacht, die in der EU-DSGVO enthaltenen Öffnungsklauseln durch nationale Umsetzungsgesetze auszufüllen. Neben der Bundesrepublik Deutschland ist dies die Republik Österreich.

Trotz ursprünglich anderer Regelungen in den Entwürfen zur europäischen Verordnung konnten sich wesentliche Grundsätze des deutschen Datenschutzrechtes durchsetzen. Dazu gehören insbesondere Datensparsamkeit und Zweckbindung sowie Datenvermeidung und die Aufrechterhaltung des Verbotsprinzips, wonach die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, wenn kein Erlaubnistatbestand etwas anderes regelt. Es sind jedoch vor allem diese Regelungen, die durch deutsche Regierungsverantwortliche immer wieder infrage gestellt werden.[1]

Da die EU-DSGVO nicht ausdrücklich das „Recht auf informationelle Selbstbestimmung“ benennt, welches vom Bundesverfassungsgericht in der Volkszählungsentscheidung von 1983 festgestellt worden ist,[2] gibt es Stimmen, die das Fortbestehen dieses Rechts vor dem Hintergrund der europäischen Gesetzgebung als überholt betrachten. Hierbei ist jedoch zu berücksichtigen, dass das Bundesverfassungsgericht dieses Grundrecht direkt aus den Artikeln 2 Abs. 1

[1] Bundesverkehrsminister Dobrindt Süddeutsche Zeitung vom 17.11.16 „Weg vom Grundsatz der Datensparsamkeit hin zu einem sicheren und kreativen Datenreichtum“
[2] BVerfG Urteil vom 15.12.1983 - 1 BvR 209/83

i.V.m. 1 Abs. 1 des Grundgesetzes ableitet. Diese Werte finden eine Entsprechung in der europäischen Menschenrechtskonvention, sodass das Recht auf informationelle Selbstbestimmung auch im Rahmen der europäischen Regelung nicht als vermeintlich deutsche Erfindung im rechtsfreien Raum schwebt.

Immer öfter wird das Recht auf informationelle Selbstbestimmung implizit oder direkt in Frage gestellt, indem weite Teile der Bundesregierung für „Datensouveränität" werben. Der Bürger sei Souverän seiner Daten und müsse deshalb nicht durch bestehende Schutzprinzipien wie die Zweckbindung und die Sparsamkeit im Umgang mit personenbezogenen Informationen geschützt werden, zumal dieser Schutz einer Weiterentwicklung von Big Data im Wege stehe.[3] Diese Ansicht ist dazu geeignet, die Betroffenenrechte massiv zu unterhöhlen und einseitig die Interessen der Wirtschaft zu berücksichtigen. Das Recht auf informationelle Selbstbestimmung ist vielmehr ein Recht, welches durch seine Ausgestaltung die betroffenen Bürger erst zu Souveränen ihrer Daten macht.

2. Deutsches Anpassungs-Umsetzungsgesetz

Die EU-DSGVO enthält zahlreiche sogenannte Öffnungsklauseln. Das sind Fälle, in denen der europäische Normgeber nicht abschließend entschieden hat und somit den Mitgliedstaaten die Möglichkeit eingeräumt bleibt, die offenen Themen durch eigene gesetzliche Regelungen zu ergänzen.

Die Bundesrepublik hat dazu das Datenschutz Anpassungs- und Umsetzungsgesetz verabschiedet, dessen Artikel 1 das neue Bundesdatenschutzgesetz enthält. Diese zentrale Vorschrift enthält mit 85 Paragraphen doppelt so viele Paragraphen, wie ihre Vorgängerregelung, das bisherige BDSG. Wer im außerkirchlichen Bereich demnächst Antworten auf datenschutzrechtliche Fragen sucht, muss die EU-Datenschutzgrundverordnung (DSGVO) und das neue BDSG nebeneinanderlegen. Gegebenenfalls sind darüber hinaus spezialgesetzliche Regelungen, z. B. im Sozialgesetzbuch im Telekommunikations- und Medienrecht u.a. Gesetzen zu beachten, die weiterhin Geltung behalten.

An sich hätte es ausgereicht ein Gesetz zu implementieren, welches die Öffnungsklauseln ausfüllt. Das neue BDSG wiederholt jedoch scheinbar einige Vorschriften der EU-DSGVO. Scheinbar deshalb, weil bei genauer Betrachtung

---

[3] Bundeskanzlerin Merkel auf dem nationalen IT-Gipfel in Saarbrücken am 17.11.2016 www.br.de/nachrichten/datensparsamkeit-zweckbindung-it-gipfel-merkel-gabriel-100.html zuletzt eingesehen 30.01.18

Unterschiede im Detail deutlich werden. Rechtlich fraglich ist dieses Vorgehen vor dem Hintergrund des „Wiederholungsverbotes“ bei direkt anwendbarem EU-Recht. Viel gravierender ist es aber dort, wo in der Substanz von den europarechtlichen Vorgaben abgewichen wird. Das einst hohe deutsche Datenschutzniveau wird so weniger durch die EU-DSGVO als durch das neue Bundesdatenschutzgesetz reduziert.

Was die Bundesregierung vom Datenschutz hält, machte der Bundesinnenminister in einem Interview im öffentlich rechtlichen Fernsehen mit der Äußerung deutlich: „Datenschutz ist schön, aber in Krisenzeiten wie diesen hat Sicherheit Vorrang“ [4].

Hat das Bundesverfassungsgericht in seinem Volkszählungsurteil noch festgestellt, dass das „Recht auf informationelle Selbstbestimmung“ Grundrechtsrang besitzt, wird dieses nunmehr vom Bundesinnenminister nur noch als dekoratives Element betrachtet. Dafür wird aber der Sicherheit Grundrechtscharakter zugesprochen. Das genau widerspricht aber dem Grundgesetz. Sicherheit ist nur ein Werkzeug, mit dessen Hilfe die Grundrechte und insbesondere das Grundrecht auf Freiheit erreicht und gesichert werden sollen. Wenn Sicherheit zum Wert an sich erhoben wird, entspricht das dem Staatsverständnis, vom absoluten Souverän, der seine Legitimation einzig daraus herleitet, eine „wilde Meute“ im Zaum zu halten[5]. Zu dieser Logik gehört auch die Maßlosigkeit, denn niemand kann bestimmen, wann genügend Sicherheit erreicht ist. Wer vorbeugen will, weiß nie genug[6].

2.1. Videoverbesserungsgesetz

Da sich in der Vergangenheit bei den Datenschutzaufsichtsbehörden eine restriktive Praxis zur Beurteilung des privaten Einsatzes von optisch-elektronischen Sicherheitstechnologien herausgebildet hatte, wurde durch die Gesetzesänderung ein Ausgleich in der Abwägungsentscheidung zur Zulässigkeit von Videoüberwachungsanlagen im öffentlichen Verkehrsraum geschaffen. Mit der Änderung des Gesetzes ist dem § 6b Abs. 1 BDSG ein zweiter Satz angefügt worden. Demgemäß ist in öffentlich zugänglichen, großflächigen Anlagen (z. B. Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen) oder Einrichtungen und Fahrzeugen des öffentlichen

[4] Bundesinnenminister De Maizière, Tagesthemen vom 22.03.2016
[5] Buchholtz Der EuGH liefert „Grundrecht auf Sicherheit“ in Neuauflagehttps://www.juwiss.de/25-2016/
[6] Prantl in der SZ 16.1.04: Der Staat, der alles wissen will

Personennahverkehrs der Schutz von Leben, Gesundheit oder Freiheit der Personen, die sich dort aufhalten, als wichtiges öffentliches Interesse zu berücksichtigen. Hierbei gilt die im Satz zuvor benannte Abwägungsentscheidung.

Zur Begründung dieser Gesetzesänderung wird maßgeblich auf ein angeblich gestiegenes Sicherheitsinteresse in der Bevölkerung seit den terroristisch motivierten Anschlägen in der Bundesrepublik hingewiesen. In der Begründung des Gesetzes bleibt jedoch völlig offen, wie die beschriebenen Maßnahmen geeignet sein sollen, bei unangekündigten Taten und rasch handelnden Tätern Anschläge zu vermeiden. Dies würde voraussetzen, dass sämtliche Aufnahmen in Echtzeit durch entsprechende Mitarbeiter überwacht und erforderliche Gegenmaßnahmen ohne Zeitverzug eingeleitet werden können. Solche Voraussetzungen sind schlicht unrealistisch.

Eine Abschreckungswirkung dürfte von der Videoüberwachung und -aufzeichnung im Hinblick auf die terroristischen Anschläge ebenfalls nicht zu erwarten sein. Attentäter, die bewusst ihr eigenes Leben zu opfern bereit sind, und die mit ihnen verbundenen Organisationen streben möglichst breite mediale Wirkung an. Videoaufnahmen und deren Verbreitung sind diesem Interesse eher förderlich. Es gibt deshalb auch keinen ernsthaften Beleg dafür, dass die stattgefundenen Anschläge durch Videoüberwachung, wie sie das Gesetz nunmehr zulässt, hätten verhindert werden können.

Dem gegenüber steht die mit dem Gesetz verbundene Einschränkung des Rechtes auf informationelle Selbstbestimmung.

Bereits in seinem Volkszählungsurteil 1983 hat das Bundesverfassungsgericht entschieden:

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. … Dies würde deshalb nicht nur die individuellen Entfaltungschancen des Einzelnen beinträchtigen, sondern eben auch das Gemeinwohl.“

Bei einer verstärkten Videoüberwachung auch und insbesondere durch Private würde der Einzelne seine Freiheitsrechte nicht mehr in der Unbefangenheit wahrnehmen, wie er das bisher tun konnte. Dies trifft auch kirchliche Veranstaltungen, die in der Öffentlichkeit stattfinden wie Prozessionen und Veranstaltungen, aber auch bereits den Gang zur Kirche.

2.2. Vorratsdatenspeicherung

Im Rahmen der Vorratsdatenspeicherung werden personenbezogene Daten ohne konkreten Anlass gespeichert. Die Speicherung erfolgt anlasslos in der Annahme, man könne diese Daten zu einem späteren Zweck maßgeblich in der Strafverfolgung zur Auswertung einsetzen.

Das für die Einführung einer solchen Vorratsdatenspeicherung 2015 erlassene Gesetz sollte ab dem 1. Juli 2017 die Anbieter von Telekommunikationsdiensten verpflichten, die Verbindungsdaten ihrer Kunden zu speichern. Wer mit wem wie lange in welcher Häufigkeit kommuniziert, sogenannte Metadaten, sollte nachgehalten werden können. Kurz vor dem in Kraft treten des Gesetzes setzte die Bundesnetzagentur die Speicherpflicht jedoch aus und berief sich dabei auf ein Urteil des Oberverwaltungsgerichts für Nordrhein-Westfalen in Münster.[7] Die vorgeschriebene Speicherpflicht erfasst nach Ansicht des Gerichts pauschal die Daten nahezu aller Nutzer von Telefon- und Internetdiensten. Laut einem aktuellen Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung müsse der Kreis der betroffenen Personen aber von vornherein auf Fälle beschränkt werden, „bei denen ein zumindest mittelbarer Zusammenhang mit der durch das Gesetz bezweckten Verfolgung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit bestehe“. Gegen dieses Gesetz sind mehrere Klagen vor dem Bundesverfassungsgericht angestrengt worden. Eine Entscheidung steht noch aus. Auch durch dieses Gesetz wird in das Recht auf informationelle Selbstbestimmung massiv eingegriffen. Für den seelsorglichen Bereich wie auch für die Dienste der Caritas stellt dieses Gesetz eine Bedrohung der Vertraulichkeit dar. Aus der Tatsache, wie häufig z. B. ein Teilnehmer die Suchtberatung anruft, lässt sich ein Persönlichkeitsprofil erstellen. Auch kann durch solche Metadaten die Schweigepflicht der Beratungsstelle unterlaufen werden.

3. Eigenständigkeit des Datenschutzes der Kirchen

In ihrem Tätigkeitsbericht 2016 reklamiert die Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Berlin für ihre Behörde das Aufsichtsrecht für kirchliche Einrichtungen, wenn dadurch die Religionsgemeinschaften nicht in ihrer Religionsfreiheit eingeschränkt werden.[8] Der Landesbeauftragte für Datenschutz

[7] OVG Münster Urteil vom 22.06.2017, Az. 13 B 238/17
[8] LbfDI Berlin Tb.2016, 10.1.

und Informationsfreiheit des Landes Thüringen stellt in seinem Tätigkeitsbericht hingegen das verfassungsrechtlich garantierte Selbstbestimmungsrecht der Religionsgemeinschaften auch für solche Einrichtungen fest, die nicht zum verfasst kirchlichen Bereich gehören.[9]

Evangelische und katholische Kirche in Deutschland verfügen über eine effektive, unabhängige und weisungsfreie Datenschutzaufsicht. Diese nimmt im Rahmen des den Kirchen grundgesetzlich gewährten Selbstbestimmungsrechtes die Datenschutzaufsicht über die Kirchen und ihre Einrichtungen wahr.

Eine Differenzierung zwischen dem kirchlichen „Grundauftrag“ und sonstigen Aufgaben ist nicht angezeigt. Eine Verpflichtung zur Achtung des Datenschutzes begründet sich ausschließlich aus dem verfassungsrechtlich gefestigten Datenschutzprinzip.

Nach ständiger Rechtsprechung[10] ist festgelegt, dass die Kirchen den Umfang ihrer Angelegenheiten selber festlegen, sodass sich eine Differenzierung durch Außenstehende verbietet. Dies wird insbesondere deutlich, wenn das BVerfG bei der Beurteilung von Anstellungsverhältnissen nicht zwischen Personen mit und ohne religionsspezifischem Status unterscheidet.

Nach den Feststellungen des BVerfG ist es den weltlichen Gerichten verwehrt, zu definieren, welche Tätigkeit „kirchenspezifisch“ ist. Vielmehr sind die Gerichte grundsätzlich an das kirchliche Selbstbestimmungsrecht gebunden, nach dem die Kirche festlegt, welche Aufgaben zum Verkündigungsauftrag gehören und somit als „kirchenspezifisch“ zu betrachten sind. Ebenso stellt das Gericht fest, dass der „außerkirchliche“ Bereich erst dort beginnt, wo die Tätigkeit vom kirchlichen Auftrag weit entfernt ist. Allein die Tatsache, dass auf einem bestimmten Sektor, wie im Bereich der Pflegedienste auch nicht kirchliche Organisationen tätig sind, führt nicht zu einer Einschränkung der Kirchenautonomie.

Es ist nicht erforderlich, dass die Einrichtung der Kirchenverwaltung angehört. Es ist vielmehr ausreichend, dass die Einrichtung der Kirche so nahe steht, dass sie teilhat an der Verwirklichung eines Stücks Auftrag der Kirche im Geist christlicher Religiosität, im Einklang mit dem Bekenntnis der christlichen Kirche.[11]

Selbst wenn die Ansicht vertreten wird, dass staatliches Datenschutzrecht anzuwenden sei, ist damit noch nicht über die Frage entschieden, wer die Aufsicht

---

[9] LbfDI Thüringen 2. Tb 2014/2015, 9.14
[10] „Goch-Entscheidung“ des BVerfG, BVerfGE 46, 73
[11] BVerfGE 53, 366 (391, 392)

über die Einhaltung dieser Vorschriften führt. Gem. Art. 140 GG i. V. m. Art. 137 Abs. 3 WRV ist das Ermessen der staatlichen Datenschutzaufsicht dann auf null reduziert, wenn die Kirchen durch eigene kirchliche Datenschutzbeauftragte und eine entsprechende Datenschutzaufsicht ausreichende Vorkehrungen zur Verwirklichung des Datenschutzes seitens ihrer Einrichtungen getroffen haben.

Weiterhin ist festzustellen, dass die neue EU-DSGVO diese Frage abschließend behandelt und sich somit auch nach der neuen Rechtslage an den Zuständigkeiten kirchlicher Datenschutzaufsicht nichts ändern wird.

Art. 91 Abs. 1 DS-GVO fordert seinem Wortlaut nach keinen Zusammenhang der Verarbeitung mit der spezifisch religiösen Aufgabe. Daraus ist zu entnehmen, dass sich die autonomen Regeln für die Verarbeitung von Daten nicht notwendigerweise nur auf die Daten von Mitgliedern beziehen müssen. Es genügt vielmehr, wenn die Verarbeitung den Status gem. Art. 17 Abs. 1 AEUV berührt.

Das in AEUV Art 17 den Kirchen zugestandene Recht liefe leer, wenn man seinen Inhalt nur auf den Status solcher Gemeinschaften reduzieren würde, jedoch die Tätigkeit zur Verwirklichung ihrer Zwecke nicht dem Schutz unterstellte. Deshalb sind auch Tätigkeiten der Religionsgemeinschaften von der Regelung des Art. 17 AEUV umfasst. Dabei kann es nicht darauf ankommen, in welcher Rechtsform die Religionsgemeinschaften diese Tätigkeiten ausüben.[12]

Die hier dargestellte Rechtsansicht ist im Übrigen gängige Praxis im Verhältnis zwischen den Landesdatenschutzbeauftragten und den Datenschutzaufsichten der Kirchen und entspricht der Rechtsansicht der Bundesbeauftragten für Datenschutz und Informationsfreiheit.

4. Kirchliches Datenschutzgesetz

Wie oben bereits dargelegt, erfährt das Datenschutzrecht in Europa durch die EU-DSGVO eine Vereinheitlichung. In Art. 91 dieser Verordnung wird den Religionsgemeinschaften das Recht zugestanden, ihr eigenes kirchliches Datenschutzrecht anzuwenden, wenn dieses mit den EU-Regelungen „in Einklang“ gebracht wird. Durch diese Formulierung soll gewährleistet werden, dass das kirchliche Datenschutzrecht in seinem Schutzniveau nicht von den europäischen Vorgaben abweicht. Damit sind die in der Verordnung zum Ausdruck gebrachten Wertungen zu übernehmen. Die bislang bestehende Kirchliche

[12] Paal/Pauly Datenschutzgrundverordnung Art. 91 Rn. 19

Datenschutzordnung (KDO) musste deshalb an die EU-DSGVO angepasst werden, was mit Verabschiedung des Kirchlichen Datenschutzgesetzes (KDG) geschehen ist. Dieses Gesetz wird von den jeweiligen Ortsbischöfen bis zum 24.05.2018 in geltendes Recht ihrer Diözese umgesetzt werden.

4.1. Was ändert sich gegenüber der KDO

4.1.1. Bestellung eines betrieblichen Datenschutzbeauftragten

Nach der neuen Regelung sind alle Diözesen, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Nach der KDO war dies erst ab einer Mitarbeiterzahl von mehr als zehn Mitarbeitern erforderlich. Dieses Quorum ist an dieser Stelle entfallen.

Andere Einrichtungen (z. B. solche der Caritas) müssen einen betrieblichen Datenschutzbeauftragten bestellen, wenn dort mindestens zehn Personen (früher mehr als zehn Personen) mit der Verarbeitung personenbezogener Daten beschäftigt sind. Auch ist die Bestellpflicht jetzt unabhängig davon, ob die Verarbeitung mit elektronischen oder analogen Mitteln geschieht.

Auch wenn weniger als zehn Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind besteht jetzt eine Bestellpflicht wenn die Kerntätigkeit in der Verarbeitung besonderer Kategorien personenbezogener Daten besteht.

Damit wird die bislang bestehende Regelung zum Ausnahmefall. Die Bestellung eines betrieblichen Datenschutzbeauftragten wird in fast allen Einrichtungen erforderlich werden. Deshalb hat die Konferenz der Diözesandatenschutzbeauftragten eine Praxishilfe „Betrieblicher Datenschutzbeauftragter“ herausgegeben, die auf den Homepages aller Diözesandatenschutzbeauftragten abgerufen werden kann.

4.1.2. Betroffenenrechte

Deutlicher als in der bisherigen Regelung sind im KDG die Betroffenenrechte, also Ansprüche und Gestaltungsmöglichkeiten jedes Einzelnen, in den §§ 14 – 23 KDG herausgearbeitet worden.

Betroffene sind künftig in einfacher und klarer Sprache über die Verarbeitung ihrer Daten zu informieren. Kirchliche Einrichtungen sollten also frühzeitig die fachlichen

und technischen Voraussetzungen zur Umsetzung der gesetzlichen Anforderungen schaffen.

Auch hier ist durch die Konferenz der Diözesandatenschutzbeauftragten eine Praxishilfe veröffentlicht worden.

4.1.3. Meldepflicht für Datenpannen

Eine solche Meldepflicht bestand nach bisherigem Recht nur nach dem Bundesdatenschutzgesetz (BDSG). Nunmehr sieht § 33 Abs. 1 KDG vor, dass eine Meldung an die Datenschutzaufsicht immer dann zu erfolgen hat, wenn die Verletzung personenbezogener Daten eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Im Einzelnen regeln die §§ 33 und 34 KDG auch, welche Vorfälle meldepflichtig sind, wie schnell die Meldung erfolgen muss und welche Folgen eine Unterlassung einer erforderlichen Meldung hat.

4.1.4. Sanktionsmöglichkeiten der Datenschutzaufsicht

Bislang war die Datenschutzaufsicht darauf beschränkt, im Falle von Datenschutzverstößen Beanstandungen auszusprechen. Nach dem neuen Gesetz ist nunmehr auch die Verhängung von Geldbußen vorgesehen. Nach dem Gesetz sollen diese wirksam, verhältnismäßig und abschreckend sein. Dabei beträgt die Höchststrafe 500.000 €.

Ebenfalls neu ist die Errichtung eines kirchlichen Gerichts in Datenschutzangelegenheiten. Von diesem Gericht können Betroffene Entscheidungen der Datenschutzaufsicht überprüfen lassen. Für das Verfahren ist zusammen mit dem KDG eine eigene Datenschutzgerichtsordnung (KDGSGO) erlassen worden.

4.1.5. Haftung und Schadensersatz

Das KDG enthält nunmehr auch eine Vorschrift, nach der jede Person, der wegen eines Verstoßes gegen das KDG ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen die kirchliche Stelle als Verantwortlichem oder Auftragsverarbeiter geltend machen kann.

5. Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands

Gem. § 46 des Gesetzes über den kirchlichen Datenschutz (KDG) sind die Datenschutzaufsichten angehalten, mit dem Ziel zusammen zu wirken, eine möglichst einheitliche Anwendung der Datenschutzbestimmungen zu erreichen. Vor dem Hintergrund dieser Vorschriften haben sich die Diözesandatenschutzbeauftragten der katholischen Kirche in Deutschland zur „Konferenz der Diözesandatenschutzbeauftragten“ zusammengeschlossen. Diese Konferenz wird mehrmals im Jahr tagen. Dabei werden Datenschutzfragen besprochen, die für die Mitglieder gleichermaßen wichtig sind und deshalb einer einheitlichen Vorgehensweise bedürfen. Die Beschlüsse der Konferenz werden die Diözesandatenschutzbeauftragten jeweils in ihren Bistümern unter Wahrung ihrer Unabhängigkeit umsetzen.

Über den von ihnen bestimmten Sprecher, der grundsätzlich jährlich wechseln soll, werden die Diözesandatenschutzbeauftragten den Kontakt zur Konferenz der staatlichen Datenschutzaufsichtsbehörden gewährleisten.

Um eine Einheitlichkeit des Datenschutzes auch mit der evangelischen Kirche in Deutschland zu erreichen, werden jährlich an mindestens einer Konferenz zum Datenschutz Verantwortliche der evangelischen Kirche teilnehmen.

5.1. WhatsApp

Ein erster Beschluss der Konferenz betrifft die Nutzung von WhatsApp und weiteren Messaging Diensten. Die Konferenz erklärte diese für unvereinbar mit der Kirchlichen Datenschutzordnung (DVO). Der Beschluss im Wortlaut:

> *„Die Verwendung eines Messaging-Dienstes auf dienstlichen Endgeräten ist untersagt, soweit eine physikalische Datenspeicherung außerhalb des Gebiets des Europäischen Wirtschaftsraumes und der Schweiz stattfindet oder keine Punkt-zu-Punkt-Verschlüsselung genutzt wird. Das gleiche gilt für die dienstliche Nutzung von privaten Smartphones“.*

Mit diesem Beschluss möchte die Konferenz der katholischen Datenschützer Klarheit über eine umstrittene Praxis herbeiführen. Die Teilnehmer gingen bei ihrem Beschluss davon aus, dass in Ländern außerhalb des europäischen Wirtschaftsraumes ein angemessenes Datenschutzniveau häufig nicht besteht. Dies gilt vor allem für den Anbieter von „WhatsApp“, der seinen Sitz bekanntlich in den USA hat und einen den europäischen Datenschutzregelungen vergleichbaren

Schutz nicht garantieren kann. So ist z. B. eine Vertraulichkeit der übertragenen Nachrichten trotz der Behauptung des Betreibers nicht sicher gewährleistet.

Insbesondere für Beratungsdienste, die der besonderen Verschwiegenheitspflicht des § 203 StGB unterliegen, ist diese Weisung unbedingt einzuhalten. Da WhatsApp die Daten, die auf dem Smartphone des Nutzers hinterlegt sind auch an Facebook weitergibt, zumindest diese aber für eigene Zwecke nutzt, können über diesen Weg sensible personenbezogene Daten im Internet veröffentlicht werden.

WhatsApp wird auch immer wieder in den Tätigkeitsberichten der staatlichen Datenschutzbeauftragten thematisiert. Mit der Regelung die die katholische Datenschutzaufsicht für die Einrichtungen der katholischen Kirche getroffen hat, etabliert sie in diesem Bereich eine klare Regelung, die im öffentlichen Bereich noch fehlt.

6. Datenschutzkontrollen

Im Berichtszeitraum wurden Kontrollen in verschiedenen Einrichtungen (Ordinariaten, Caritasverwaltung, Pflegeheime, Beratungsstellen, Krankenhäuser) vorgenommen.

a) Bei den Besuchen war festzustellen, dass ein Datenschutzkonzept regelmäßig nur in den Krankenhäusern vorhanden ist. In den anderen Fällen selten bis nie. Das hat gravierende Auswirkungen auf den Datenschutz in der Einrichtung. Dieser wird zwar grundsätzlich praktiziert, aber eine Stringenz ist häufig nicht zu erkennen. Eine aufsichtliche Prüfung der Einrichtung, ohne Vorliegen eines Datenschutzkonzeptes einschließlich Verfahrensverzeichnis, ist praktisch aber nicht möglich. Die Erarbeitung eines Datenschutzkonzeptes einschließlich Verfahrensverzeichniss ist für alle Einrichtungen damit zwingend erforderlich!

b) Verpflichtungserklärungen zum Datenschutz gem. § 4 KDO sind zwar häufig vorhanden, die Unterzeichner sind aber regelmäßig nicht geschult. Auch haben sie keine Erläuterungen zum Datenschutz erhalten, die eine Grundlage für diese Erklärung bilden könnten. So muss davon ausgegangen werden, dass die Verpflichtungserklärungen den Mitarbeitern bei Antritt des Arbeitsverhältnisses oder in dessen Verlauf lediglich zur Unterschrift vorgelegt werden. Aus diesem Grund werden die Verpflichtungserklärungen häufig mit den arbeitsvertraglich

geregelten Verschwiegenheitserklärungen verwechselt bzw. gleichgestellt und deshalb als rein bürokratische Auswüchse verstanden.

Die Belehrung nach § 4 KDO, demnächst § 5 KDG verlangt eine arbeitsplatzbezogene individuelle Belehrung.[13] Die Wiedergabe des Gesetzestextes reicht ebenso wenig aus, wie ein allgemeiner Aushang am Schwarzen Brett oder allgemeine Arbeitsanweisungen. Erforderlich ist vielmehr auf die verbotenen Handlungen hinzuweisen und auf mögliche Konsequenzen aufmerksam zu machen.[14]

c) Technisch organisatorische Maßnahmen werden nur zum Teil umgesetzt. Wenn sie umgesetzt werden, sind das eher punktuelle Maßnahmen, da ein einheitliches Konzept und damit auch eine Dienstanweisung fehlt.

d) In der Regel gibt es keine Anweisung die Bürotüren abzuschließen, wenn das Büro verlassen wird und nicht mehr gesehen werden kann, ob eine andere Person das Büro betritt.

e) In einem Fall konnte festgestellt werden, dass eine Firewall zwar installiert, aber deaktiviert war. Begründet wurde dies u. a. damit, dass die Firewall den Zugriff auf Clouddienste nicht zuließ. Hierbei handelte es sich um Clouddienste deren Server außerhalb des Gebietes der Bundesrepublik aufgestellt sind. Die Nutzung derartiger Dienste ist durch die KDO-DVO untersagt.

Zwischenzeitlich ist die Firewall wieder aktiviert worden.

f) Bildschirmsperren werden gelegentlich eingerichtet, sind aber regelmäßig nicht in einer schriftlichen Anordnung fixiert.

g) Die Aktenvernichtung findet häufig unzureichend statt. In einem Fall wurde eine Aktenvernichtungsanlage vorgefunden, die die Akten in ca. 5 mm breite Stücke schnitt. Ein Querschnitt erfolgte nicht. Weil die Maschine bereits älter war, wurden die (sowieso unzureichenden) Längsschnitte nicht mehr richtig getrennt. Bei der Besichtigung konnte durch einfache Entnahme ein Papierstück gegriffen werden, aus dem zu ersehen war, dass es sich um ein Gehaltsblatt einer Mitarbeiterin

[13] Gola/Schomerus, § 5 Rn. 12, Ehmann in Simitis § 5 Rn. 28
[14] ebd.

handelte. Besonders prekär war die Anlage auch deshalb, weil jeder Mitarbeiter Zugang zu dem Raum hatte, in dem die Maschine stand.

Inzwischen ist eine Aktenvernichtung etabliert worden, die der aktuellen Norm (s. Anhang 1) gerecht wird.

h) Auch wenn die Aktenvernichtung mit Hilfe von professionellen Firmen durchgeführt wird, ist das Verfahren mit dem Vernichtungsgut oftmals unzureichend und in der Regel nicht schriftlich geregelt.

So kommt es vor, dass zwar verschlossene Tonnen, die nur über einen schmalen Schlitz zum Akteneinwurf verfügen, durch eine Fremdfirma aufgestellt werden, der Hausmeister aber für die Tonnen einen Schlüssel besitzt. Dies wird damit begründet, dass es eine Möglichkeit geben muss, fälschlich entsorgte Akten wieder aus der Tonne zu holen. Zwar ist für diesen Fall vorzusorgen, doch ist der Schlüssel für die Entsorgungstonne bei der Leitung zu verwahren. Nur so ist gewährleistet, dass nicht Unbefugte Kenntnis von vertraulichem Schriftgut nehmen. Die Entnahme eines Schriftstückes aus der Entsorgungstonne ist von einem von der Leitung beauftragten Mitarbeiter zu protokollieren und von demjenigen der die Akte entnimmt, gegenzuzeichnen.

7. Beispiele aus der Tätigkeit der Datenschutzaufsicht

7.1. Datenschutz im Arbeitsrecht

7.1.1. Abwesenheitslisten

In einer Kindereinrichtung waren die Erzieherinnen angehalten, ihre An- und Abwesenheit in einen auch für die Eltern einsehbaren Kalender einzutragen. Dabei sollte auch der Grund der Abwesenheit benannt werden.

In Sekretariaten oder anderen zumindest für Mitarbeiter zugänglichen Stellen finden sich gelegentlich Abwesenheitskalender. Diese geben Auskunft darüber, welche Mitarbeiter sich an welchen Tagen nicht in der Einrichtung befinden. Soweit ist ein solcher Abwesenheitskalender nicht zu beanstanden, da gegenüber Dritten die Auskunft erteilt werden kann, wann sie den abwesenden Mitarbeiter wieder persönlich erreichen können.

Etwas anderes muss aber gelten, wenn diese Kalender auch den Grund für die Abwesenheit (Krankheit, Fortbildung, Urlaub u. ä.) enthalten. Die Angabe von Gründen in Verbindung mit dem Namen stellt ein personenbezogenes Datum dar,

dessen Veröffentlichung nicht erforderlich und somit unzulässig ist. Selbst eine Einwilligung des Mitarbeiters in die Bekanntgabe des Grundes seiner Abwesenheit dürfte unzulässig sein, da eine solche Veröffentlichung nicht zweckmäßig ist und gegen den Grundsatz der Datensparsamkeit verstößt.

7.1.2. Arbeitsunfähigkeitsbescheinigung

In einer Einrichtung verlangte ein Bereichsleiter, die Anfertigung und Übergabe einer Kopie der von den Mitarbeitern seines Bereichs eingereichten Arbeitsunfähigkeitsbescheinigungen.

Nach § 5 Abs. 1 S. 2 EntgeltfortzahlungsG hat der Dienstnehmer dem Dienstgeber eine ärztliche Bescheinigung über das Bestehen und die voraussichtliche Dauer der Arbeitsunfähigkeit vorzulegen, wenn die Arbeitsunfähigkeit über den dritten Tag hinaus andauert.

Bei der ärztlichen Arbeitsunfähigkeitsbescheinigung handelt es sich um Gesundheitsdaten. Nicht zuletzt deshalb, weil sich aus der Bescheinigung durch den Stempel des Arztes dessen Fachrichtung ergibt und somit Schlüsse auf die Art der Erkrankung möglich sind. Es handelt sich dabei um besondere Arten von personenbezogenen Daten im Sinne von § 2 Abs. 10 KDO. Der Umgang mit diesen Daten verlangt einen besonderen Schutz. Es verstößt deshalb grundsätzlich gegen den Datenschutz, wenn gefordert wird, eine solche Bescheinigung anderen Mitarbeitern als denen der Personalabteilung vorzulegen.

Die Anfertigung einer Kopie der Arbeitsunfähigkeitsbescheinigung stellt ein Verarbeiten von Daten i. S. v. § 2 Abs. 4 KDO dar. Dies ist nach § 3 Abs. 1 KDO nur zulässig, wenn eine diesbezügliche Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat. Eine solche Rechtsvorschrift, die ein Kopieren erlaubt, besteht nicht. Auch eine Einwilligung dazu liegt regelmäßig nicht vor. Diese müsste schriftlich, freiwillig und konkret vorliegen. Aber selbst im Falle einer Einwilligung dürfte eine Kopie stets gem. § 2a KDO unzulässig sein, da die Verarbeitung derartiger Daten nicht zweckmäßig und erforderlich sind.

Der Dienstvorgesetzte muss nur wissen, dass der Dienstnehmer krank ist und wie lange die Krankheit voraussichtlich dauert, damit er die Arbeit in seinem Organisationsbereich ggf. anders verteilen kann.

Die Arbeitsunfähigkeitsbescheinigung ist deshalb bei der Personalabteilung einzureichen. Diese hat den jeweiligen Vorgesetzten dann über den Umstand der Krankheit und deren voraussichtliche Dauer zu unterrichten. Weitere Aussagen dazu sind zu unterlassen.

7.1.2. Betriebliches Eingliederungsmanagement

Eine Mitarbeitervertretung (MAV) bat um Erläuterung, ob datenschutzrechtliche Gründe entgegenstehen, wenn die MAV vom Dienstgeber eine namentliche Liste von Mitarbeitern fordert, die in den letzten 12 Monaten mehr als sechs Wochen arbeitsunfähig krank waren.

Der Kirchliche Arbeitsgerichtshof entschied mit Urteil M 06/2014 – 28.11.2014, dass die Mitarbeitervertretung keinen Anspruch auf Vorlage der Namen derjenigen Mitarbeiter habe, die in den letzten zwölf Monaten länger als sechs Wochen arbeitsunfähig gewesen sind und begründet dies u. a. mit datenschutzrechtlichen Erwägungen.

Nach hier vertretener Ansicht stehen datenschutzrechtliche Gründe einer solchen Auskunft nicht entgegen.

Für Beschäftigte, die innerhalb von 12 Monaten länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, sieht § 84 Abs. 2 SGB IX ein sogenanntes „betriebliches Eingliederungsmanagement“ vor. Die Vorschrift verfolgt den Zweck, einer Gefährdung des Arbeitsverhältnisses aus gesundheitlichen Gründen frühzeitig entgegen zu wirken. Durch dieses Verfahren sollen Rehabilitationsbedarfe erkannt und mit dem Mitarbeiter besprochen werden, welche Maßnahmen ggf. zu ergreifen sind, um erneute krankheitsbedingte Ausfälle zu verhindern und eine dauerhafte Fortsetzung des Arbeitsverhältnisses zu fördern.

Gem. § 84 Abs. 2 S. 3 SGB IX ist der Arbeitgeber verpflichtet, dem betroffenen Arbeitnehmer die Durchführung eines solchen Verfahrens anzubieten. Es kommt aber nur zustande, wenn der betroffene Arbeitnehmer einwilligt.

Dem Betriebsrat bzw. der Mitarbeitervertretung wird durch § 93 SGB IX auferlegt, darauf zu achten, dass die dem Arbeitgeber gem. § 84 SGB IX obliegenden Aufgaben erfüllt werden. Insoweit wiederholt die Vorschrift, die sich bereits aus § 80 Abs. 1 Nr. 1 BetrVG, § 26 Abs. 1 MAVO ergebende Überwachungsaufgabe der Mitarbeitervertretungen.

Um zu prüfen, ob der Arbeitgeber seiner Pflicht zur Einleitung des BEM nachkommt, kann der Betriebsrat / die Mitarbeitervertretung bzw. bei schwerbehinderten Arbeitnehmern die Schwerbehindertenvertretung (§ 84 Abs. 2 S. 6 u. 7 SGB IX) unabhängig von einer Zustimmung der Arbeitnehmer in der ersten Phase beanspruchen (§ 80 Abs. 2 S. 2 BetrVG i. V. m. § 84 Abs. 2 Satz 7 SGB IX), dass ihm der Arbeitgeber quartalsweise ein Verzeichnis mit Namen der

Arbeitnehmer aushändigt, die im zurückliegenden Jahreszeitraum länger als sechs Wochen arbeitsunfähig waren.

Ein anonymisiertes Mitarbeiterverzeichnis lässt nur die bloße Anzahl der Arbeitnehmer erkennen, welche die Voraussetzungen für ein BEM erfüllen. Für die Überwachung, ob der Arbeitgeber das Verfahren entsprechend seiner gesetzlichen Initiativlast auch einleitet, ist die bloße Kenntnis der Anzahl der für ein BEM in Frage kommenden Arbeitnehmer unzureichend. Durch eine solche anonymisierte Liste erlangt die Mitarbeitervertretung keine hinreichende Gewissheit darüber, dass alle betroffenen Beschäftigten über das Angebot eines BEM tatsächlich informiert wurden.

Der Arbeitgeber muss dem Betriebsrat die Namen der Arbeitnehmer mit Arbeitsunfähigkeitszeiten von mehr als sechs Wochen im Jahreszeitraum auch dann mitteilen, wenn diese der Weitergabe nicht zugestimmt haben.

Die Überwachungsaufgabe des Betriebsrats / der Mitarbeitervertretung nach § 80 Abs. 1 Nr. 1 BetrVG / § 26 Abs. 1 MAVO ist nicht von einer vorherigen Einwilligung der von der Vorschrift begünstigten Arbeitnehmer abhängig.

Das Zustimmungserfordernis gem. § 84 Abs. 2 Satz 1 SGB IX bezieht sich nur auf die zweite Phase des BEM, nämlich den eigentlichen Klärungsprozess, nicht aber auf die erste Phase. Der Gesetzeswortlaut enthält eine entsprechende Einschränkung nicht. Das Beteiligungsrecht aus § 80 Abs. 1 Nr. 1 BetrVG / § 26 Abs. 1 MAVO dient der Sicherstellung eines ordnungsgemäßen Normvollzugs durch den Arbeitgeber. Seine Wahrnehmung steht nach der Konzeption des BetrVG und der MAVO nicht zur Disposition der Arbeitnehmer. Zwar handelt es sich hierbei um besondere Arten personenbezogener Daten über die Gesundheit i. S. d. § 3 Abs. 9 BDSG „sensitive Daten“ (§ 2 Abs. 10 KDO), die Erhebung und Nutzung der Angaben über die krankheitsbedingten Fehlzeiten durch den Arbeitgeber ist aber auch bei fehlender Einwilligung der Arbeitnehmer zulässig, da die Durchführung eines BEM zu den gesetzlichen Pflichten des Arbeitgebers gehört (§ 28 Abs. 6 Nr. 3 BDSG, § 9 Abs. 5 Nr. 9 KDO). Deren Weitergabe an den Betriebsrat ist keine Datenübermittlung an einen Dritten. Der Betriebsrat ist nicht als „Dritter“ (§ 3 Abs. 4 Nr. 3 BDSG, § 2 Abs. 9 KDO) anzusehen, der außerhalb der verantwortlichen Stelle steht. Vielmehr ist er selbst Teil dieser Stelle und hat die betrieblichen und gesetzlichen Datenschutzbestimmungen einzuhalten.

Datenschutzrechtliche Gründe stehen der namentlichen Übermittlung im Falle des BEM also nicht entgegen. Es handelt sich bei § 84 Abs. 2 SGB IX um eine vorrangige Rechtsvorschrift i. S. d. § 1 Abs. 3 BDSG / § 1 Abs. 3 KDO.

Diese zu § 80 Abs. 1 Nr. 1 BetrVG entwickelte Rechtsprechung ist auf § 26 Abs. 1 MAVO zu übertragen, da die dort geregelte Verpflichtung der MAV auf die Einhaltung von Recht und Billigkeit zu achten andernfalls undurchführbar wäre.

Die vom Kirchlichen Arbeitsgerichtshof im Urteil M 06/2014 – 28.11.2014 vertretene Rechtsauffassung ist damit abzulehnen.

Zunächst krankt das Urteil daran, dass das einheitliche Verfahren des § 84 Abs. 2 SGB IX in zwei Phasen geteilt und dabei verkannt wird, dass die erste Phase praktisch eine conditio sine qua non für die zweite Phase darstellt. Wenn der Kirchliche Arbeitsgerichtshof formuliert: „ …aus der Zweiteilung folgt, dass die Mitarbeitervertretung kein Recht habe, unabhängig von der noch fraglichen Zustimmung des Betroffenen die Bekanntgabe der Namen der angeschriebenen Beschäftigten zu verlangen“, fehlt für diese Behauptung jeder Anhaltspunkt im Gesetz. Tatsächlich ist das Gegenteil der Fall. Denn die Zustimmung, die in § 84 Abs. 2 S. 1 SGB IX gefordert wird, bezieht sich ausdrücklich erst auf die Frage, „wie die Arbeitsunfähigkeit überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann“. Damit wird ausschließlich die zweite Phase des Verfahrens von der Zustimmung des Betroffenen abhängig gemacht. Dies macht auch Sinn, da ein BEM nicht ohne Mitwirkung des Betroffenen sinnvoll durchgeführt werden kann.

Die erste Phase des Verfahrens wird in § 84 Abs. 2 S. 3 SGB IX angesprochen. Dort wird festgestellt, dass die betroffene Person „zuvor“, also vor einer Zustimmung, auf die Ziele eines BEM hinzuweisen ist und ihr Art und Umfang der hierfür zu erhebenden und verwendeten Daten bekannt zu geben sind. Die Zustimmung des Betroffenen bezieht sich also auf die zweite Phase des BEM. Für den ersten Teil, der den Arbeitgeber verpflichtet, den Arbeitnehmer über die Möglichkeiten und Inhalte des BEM zu informieren, bedarf es keiner Zustimmung, weil es sich dabei um eine Verpflichtung des Arbeitgebers handelt.

§ 84 Abs. 2 S. 6 SGB IX legt der zuständigen Interessenvertretung die Pflicht auf, darüber zu wachen, dass der Arbeitgeber diese Verpflichtung erfüllt. Eine solche Überprüfung ist ohne die namentliche Nennung der betroffenen Arbeitnehmer nicht möglich. Die demgegenüber in der vom kirchlichen Arbeitsgerichtshof zitierten Entscheidung des Bayrischen Verwaltungsgerichtshofes getroffene Feststellung, die Personalvertretung würde im Rahmen der vertrauensvollen Zusammenarbeit keinen Anlass haben, die Angaben des Arbeitgebers über den Kreis der betroffenen Mitarbeiter in Zweifel zu ziehen, widerspricht sowohl der gesetzlichen Intention, als auch den eignen Feststellungen dieses Gerichts. Stellt es doch selber fest, dass die sich aus der Überwachungspflicht ergebenden Rechte der

Personalvertretung an einer rechtmäßigen Handhabung des in § 84 Abs. 2 SGB IX nicht nur bei begründeten Zweifeln, sondern in jedem Fall des Ingangsetzens des BEM bestehen.

Die Befürchtung des BayVGH, der Interessenvertretung könne bei einer entsprechenden Information die Krankheit des betroffenen Mitarbeiters bekannt werden, ist unbegründet, weil in dieser Phase selbst dem Arbeitgeber die Gründe für die krankheitsbedingten Fehlzeiten nicht bekannt sein dürften, da der Arbeitnehmer nicht verpflichtet ist diese seinem Arbeitgeber mitzuteilen.

Entgegen den Feststellungen des Kirchlichen Arbeitsgerichtshofes verstieße die Weitergabe einer Namensliste der betroffenen Beschäftigten nicht gegen deren Recht auf informationelle Selbstbestimmung. Dieses Recht ist nicht schrankenlos gewährleistet, sondern muss sich Einschränkungen im überwiegenden Allgemeininteresse gefallen lassen.

Die Namensliste enthält lediglich Angaben darüber, welcher Mitarbeiter krankheitsbedingte Fehlzeiten von mehr als sechs Wochen innerhalb des letzten Jahres aufweist. Da diese Daten die Gesundheit des entsprechenden Mitarbeiters betreffen, gehören sie zu den besonderen Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG, § 2 Abs. 10 KDO. Zu berücksichtigen ist dabei aber, dass die konkreten Fehlzeiten nicht bekannt zu geben sind. Die Information, länger als sechs Wochen, reicht um der Interessenvertretung die Möglichkeit der Überwachung einzuräumen. Erst recht sind die konkreten Gründe bzw. die Angabe der Krankheiten nicht mitzuteilen. Die Tatsache, dass der betroffene Mitarbeiter länger als sechs Wochen gefehlt hat ist zwar keine betriebsöffentliche Tatsache, wird aber regelmäßig durch die Notwendigkeit einer Vertretung in der Dienststelle bekannt sein. Insofern kommt diesem Datum in diesem Zusammenhang ein eher geringes Gewicht zu.

Das höherrangige Interesse ist deshalb in der Sicherstellung eines ordnungsgemäßen Normvollzugs zu sehen, welches nicht zur Disposition des Arbeitnehmers steht. Längere krankheitsbedingte Abwesenheiten von Mitarbeitern führen zu Unruhe in der Einrichtung, weil sie für die übrigen Beschäftigten mit Mehrbelastungen verbunden sind. Durch eine Wiedereingliederung des betroffenen Arbeitnehmers soll dies vermieden und der Betriebsfrieden gewahrt werden. Der Interessenvertretung ist deshalb eine Namensliste der betroffenen Mitarbeiter gem. §§ 84 Abs. 2 SGB IX, i.V.m. § 93 SGB IX zu überlassen. Diese Vorschriften konkretisieren das der Interessenvertretung zustehende Mitbestimmungsrecht in den §§ 80 Abs. 1 Nr. 1 BetrVG und 26 Abs. 2 MAVO.

Soweit der Kirchliche Arbeitsgerichtshof zu einer anderen Entscheidung kommt, weil er § 14 Abs. 5 KDO für einschlägig hält, geht diese Einordnung fehl. Diese Vorschrift spricht von einem Widerspruchsrecht des Betroffenen gegen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten.

Das Widerspruchsrecht besteht aber gem. § 14 Abs. 5 Satz 2 KDO für solche Fälle nicht, in denen eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

Nach § 5 Abs. 1 EntgeltfortzahlungsG ist der Arbeitnehmer verpflichtet, dem Arbeitgeber unverzüglich seine Arbeitsunfähigkeit anzuzeigen und dies bei einer Arbeitsunfähigkeit von mehr als drei Tagen mit einer ärztlichen Bescheinigung zu belegen. Der Arbeitgeber ist seinerseits verpflichtet, die Arbeitsunfähigkeitszeiten des Arbeitnehmers zu speichern.

§ 10 Abs. 5 Nr. 1 KDO i.V. m. § 9 Abs. 5 Nr. 9 KDO regeln das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten. Das ist erlaubt, wenn dies u. a. zur Durchführung des Dienstverhältnisses erforderlich ist. In diesem Fall ist eine Einwilligung des Arbeitnehmers weder für die Erhebung noch für die Nutzung erforderlich. In der Weitergabe der Daten an die Mitarbeitervertretung / den Betriebsrat liegt kein „Übermitteln“, da es sich bei der Interessenvertretung nicht um einen Dritten gem. § 2 Abs. 9 KDO handelt. Die Interessenvertretung ist vielmehr Teil der verantwortlichen Stelle. Die ordnungsgemäße Durchführung eines gesetzlich vorgeschriebenen BEM gehört dabei selbstverständlich zur Durchführung des Dienstverhältnisses i. S. dieser Vorschrift.

Aus datenschutzrechtlichen Gründen besteht mithin kein Grund, der Mitarbeitervertretung / dem Betriebsrat die Namen der Mitarbeiter/ innen vorzuenthalten, welche innerhalb der letzten zwölf Kalendermonate länger als sechs Wochen krankheitsbedingt gefehlt haben. Dabei darf nur die gesamte Abwesenheitszeit mitgeteilt werden, nicht aber die einzelnen Fehlzeiten. Außerdem darf die konkrete Krankheit nicht mitgeteilt werden.

7.1.3. Bewerberdaten

Immer wieder nachgefragt wird, wie mit Bewerbungsunterlagen zu verfahren ist und wann diese zu löschen sind.

Personenbezogene Daten eines Bewerbers, der sich auf eine bestimmte ausgeschriebene Stelle bewirbt, dürfen zunächst für den Auswahlprozess

herangezogen werden. Dabei dürfen alle Daten verwendet werden, die für die Auswahl des Bewerbers erforderlich sind.

Die Bewerbungsunterlagen dürfen aber, nachdem die Auswahlentscheidung getroffen worden ist, nicht mehr verwendet werden. D. h., diese sind zunächst zu sperren gem. § 14 Abs. 3 KDO, bis die Frist für die Einreichung einer Klage (insbes. einer solcher nach dem Allgemeinen Gleichstellungsgesetz, AGG) von abgelehnten Bewerbern abgelaufen ist. Nach § 15 Abs. 4 AGG sind Ansprüche wegen Diskriminierung innerhalb von zwei Monaten ab Zugang der Ablehnung schriftlich geltend zu machen. Nach § 61b Arbeitsgerichtsgesetz (ArbGG) muss Klage zur Durchsetzung der fristgemäß geltend gemachten Entschädigungsansprüche innerhalb von drei Monaten beim zuständigen Arbeitsgericht erhoben werden. Dementsprechend ist eine Aufbewahrung der Bewerbungsunterlagen spätestens nach sechs Monaten nicht mehr erforderlich.

Bewerbungsunterlagen sind an den Bewerber zurückzusenden, wenn es sich um eine Bewerbung auf eine vom Dienstgeber veranlasste Stellenausschreibung handelt. Handelt es sich um eine „Blindbewerbung“ oder „Initiativbewerbung“, ist eine Rücksendung nicht vorgeschrieben. Die Bewerbungsunterlagen können dann vernichtet werden (Es dürfte für das Image der Einrichtung deutlich förderlicher sein, die Bewerbungsunterlagen zurück zu senden. Außerdem ist auf diese Weise eine ordnungsgemäße Löschung der Daten sichergestellt.).

Bei Online-Bewerbungen sind die Daten einschließlich aller Kopien zu löschen.

Das Bewerbungsanschreiben sowie das Absageschreiben (bzw. dessen Kopie) gelten jedoch als Handelsbriefe i. S. d. § 257 Abs. 1 Nr. 2 u. 3 HGB und unterliegen deshalb einer Aufbewahrungspflicht von sechs Jahren.

Die Aufbewahrung der Bewerbungsunterlagen für eine evtl. später frei werdende Stelle ist ohne die Einwilligung des Bewerbers unzulässig.

7.1.4. Fragerecht bei der Bewerberauswahl

Die Erhebung und Verarbeitung von Daten, die in einem Gespräch erhoben worden sind, ist zulässig, wenn dies zur Begründung des Beschäftigungsverhältnisses erforderlich ist. Es dürfen nur solche Fragen gestellt werden, an deren wahrheitsgemäßer Beantwortung der Arbeitgeber ein berechtigtes und schutzwürdiges Interesse hat. In diesem Fall treten die Belange der Bewerberinnen und Bewerber in den Hintergrund. Dabei kommt es auch darauf

an, in welchem Bewerbungsstadium sich die Bewerberin oder der Bewerber befindet. „Billigenswert“ und „schutzwürdig“ ist ein Arbeitgeberinteresse nur dann, wenn es für die Funktionsfähigkeit des Unternehmens maßgeblich ist.

Im Bewerbungsverfahren selbst sind deshalb zunächst nur die Fragen zulässig, die für die Entscheidung notwendig sind, ob die Betroffenen überhaupt geeignet sind, um in die nähere Auswahl zu gelangen.

An der Beantwortung von Fragen persönlicher Art, die mit der ausgeübten Tätigkeit nichts zu tun haben, wie etwa Hobbys oder eine Mitgliedschaft im Verein, (im Hinblick auf familiäre Verhältnisse sind ggf. die Besonderheiten des kirchlichen Arbeitsrechts zu berücksichtigen), hat der Arbeitgeber zu keinem Zeitpunkt ein berechtigtes Interesse. Solche Fragen sind mithin unzulässig.

Insbesondere unterliegen Daten über die Gesundheit, Erkrankungen bzw. etwaige Behinderungen einem besonderen Schutz. Der Arbeitgeber hat bezüglich dieser Daten nur dann einen Informationsanspruch, wenn sie Voraussetzung für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche sind. Nach dem Allgemeinen Gleichbehandlungsgesetz sind Nachfragen zu gesundheitlichen Einschränkungen erlaubt, wenn diese konkrete Auswirkungen auf die Tätigkeit haben bzw. diese unmöglich machen. Keinesfalls darf der Arbeitgeber Krankheitsdaten losgelöst von der zu besetzenden Stelle erheben.

Nach § 10a Abs. 1 KDO (§ 32 Abs. 2 BDSG) dürfen personenbezogene Fragen eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden. Gem. § 2 Abs. 12 Nr. 9 KDO (§ 3Abs. 11 Nr. 7 BDSG) gelten Bewerber als Beschäftigte bzw. werden diesen gleichgestellt. Das gilt gem. § 10a Abs. 2 KDO (§ 32 Abs. 2 BDSG) auch für den Fall, dass die Angaben nicht in automatisierten Dateien verarbeitet werden.

7.1.5. Online Bewerbungen

Online-Bewerbungen erfordern deutlich weniger Aufwand und sind zudem häufig einfacher an die Personen weiterzuleiten, die über die Einstellung entscheiden. Auch sind sie kostengünstiger zu analysieren.

Um dem Datenschutz Rechnung zu tragen, sollten folgende Hinweise beachten werden:

Bei einer E-Mail Versendung werden sensible Daten von Bewerbern zwar über einen standardisierten, aber technisch gesehen unsicheren Weg versandt, da eine Verschlüsselung regelmäßig nicht stattfindet. Auf diese Tatsache sollten die Bewerber im Ausschreibungstext hingewiesen werden. Darüber hinaus sollte

immer auch auf die Möglichkeit der postalischen Einsendung hingewiesen werden, ohne dabei den Eindruck zu erwecken, diese Form der Einreichung stelle einen Nachteil gegenüber den in elektronischer Form eingereichten Unterlagen dar.

Beispiel:

Sie können uns Ihre Bewerbungsunterlagen per Post oder elektronisch per E-Mail zusenden. Wir weisen aber darauf hin, dass diese Verbindung nicht verschlüsselt ist und wir nicht garantieren können, dass unbefugte Dritte Ihre Unterlagen nicht einsehen.

Wenn beide Möglichkeiten gleichberechtigt nebeneinanderstehen und auf die Gefahren der E-Mail Einsendung hingewiesen wird, können sich die Bewerber informiert und freiwillig entscheiden, welche der beiden Möglichkeiten sie nutzen.

Die Bewerbungsunterlagen werden regelmäßig an die Personalabteilung der ausschreibenden Einrichtung gerichtet oder an konkret benannte Ansprechpartner. Nur diese und die Entscheidungsträger dürfen auf die Unterlagen Zugriff haben. Eine elektronische Weiterleitung der Unterlagen an die im Auswahlverfahren Beteiligten ist zu unterlassen, da andernfalls nicht sichergestellt werden kann, dass eine ordnungsgemäße Löschung aller Kopien erfolgt. Vielmehr ist den am Auswahlverfahren Beteiligten ein Zugriff einzurichten, ohne die Möglichkeit Kopien anzufertigen.

Die Aufbewahrung der Bewerbungsunterlagen für eine evtl. später freiwerdende Stelle oder einen Bewerberpool ist ohne die Einwilligung des Bewerbers unzulässig.

Dies gilt auch für den Fall, dass sich der Bewerber auf eine konkrete Stelle beworben hat und nunmehr eine andere Stelle frei geworden ist.

7.1.6. Nutzung von Skype verboten

Lädt ein Arbeitgeber Bewerber zu einem Bewerbungsgespräch ein, hat er die dabei für den Bewerber entstehenden Kosten zu tragen.[15]

Ein Dienstgeber hat angefragt, ob er das Bewerbungsgespräch per Skype, also per Ton- und Bildübertragung via Internet führen dürfe, um Kosten zu sparen.

[15] Dieser Anspruch die der h. M. entspricht, wird aus dem Auftragsrecht abgeleitet. §§ 662–670 BGB; BAG 29.6.88 – 5 AZR 433/87, NZA 89, 468

Hierbei werden aber personenbezogene Daten der Bewerber erhoben, die über die Erforderlichkeit hinausgehen, insbesondere Sprach- und Bildaufzeichnungen.

Nach den Nutzungsbedingungen von Skype werden Chat-Protokolle auf den Servern von Microsoft in den USA bis zu 90 Tagen zwischengespeichert. Es findet hierbei also eine Datenübermittlung in ein außereuropäisches Land statt, dessen Datenschutzniveau dem der Europäischen Union nicht vergleichbar ist. Auch aus diesem Grund verbietet die geltende Regelung in der KDO bzw. der KDO Durchführungsverordnung (KDO-DVO) eine Nutzung für dienstliche Zwecke.

Diese Ausführungen lassen sich auch dadurch nicht umgehen, dass der Bewerber um Einwilligung zur Nutzung von Skype gebeten wird. Im Rahmen eines Bewerbungsverfahrens besteht eine Drucksituation für den Bewerber, bei der von einer Freiwilligkeit in diesem Zusammenhang nicht wirklich ausgegangen werden kann. Videointerviews sind demnach rechtswidrig.

7.1.7. Nutzung von Online-Bewerbungsplattformen

Die Nutzung von sogenannten Recrutingplattformen ist verboten, wenn sie über Server laufen, die nicht auf dem Gebiet der EU stehen.

7.1.8. BYOD (Bring your own device)

BYOD benennt die Situation, wenn Mitarbeiter ihre eigenen Endgeräte (Laptops, Tablets, Smartphones o. ä.) für dienstliche Zwecke nutzen, also dienstliche Daten auf privaten Geräten verarbeiten.

Nach der KDO-DVO IV. Anlage zu § 6 Anlage 2 Punkt 5.1. ist die Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken grundsätzlich unzulässig!

Ausnahmen hiervon sind durch den Dienststellenleiter unter schriftlicher Nennung der Gründe zu genehmigen. Gem. IT-Richtlinie zur Umsetzung der genannten Vorschrift sind diejenigen, die ausnahmsweise private Datenverarbeitungssysteme dienstlich nutzen dürfen, schriftlich auf die IT-Richtlinie zu verpflichten. Weiterhin muss sich der Verwender verpflichten, personenbezogene Daten durch die Dienststelle und auf deren Anforderung löschen zu lassen. Außerdem ist der Dienststelle das Recht einzuräumen, die gespeicherten dienstlichen Daten auch ohne Einwilligung des Nutzers zu löschen. Die Löschungsbefugnis bezieht sich auch auf private Daten, die sich auf dem Endgerät des Nutzers befinden, wenn dies im Zuge der Löschung dienstlicher Daten unumgänglich ist.

7.1.9. GPS-Überwachung von Mitarbeiter-Kfz

Überwachung von Dienstfahrzeugen mittels GPS (Global Positioning System) ist nur unter strengen Voraussetzungen möglich.

Datenschutzrechtlich unproblematisch wäre es zunächst, wenn die Ortung durch das System erst nach einem Diebstahl des Fahrzeuges einsetzen würde.

Wenn die Mitarbeiter die Fahrzeuge auch privat nutzen dürfen ist die Verfolgung mittels GPS-Ortungsgerät bei diesen Fahrten unzulässig.

Auch wenn das Fahrzeug ausschließlich dienstlich genutzt wird, ist eine permanente anlasslose Überwachung des Mitarbeiters nicht zulässig, da die Mitarbeiter keinem permanenten Kontrolldruck ausgesetzt sein dürfen.

Beschäftigte müssen Kontrollen ihres Arbeitsverhaltens nur dann hinnehmen, wenn diese geeignet und erforderlich sind, um etwa konkreten Verdachtsmomenten auf arbeitsrechtliche Verfehlungen nachzugehen. Es müssen tatsächliche Anhaltspunkte bestehen, die den Verdacht rechtfertigen, dass die überwachte Person gegen ihre arbeitsrechtliche Verpflichtung verstößt.

Auch eine Einwilligung des Mitarbeiters zur GPS-Ortung ist aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht als freiwillig zu werten und damit nicht wirksam.

Wenn eine Aufzeichnung aus arbeitstechnischen Gründen für den Arbeitgeber erforderlich ist, müssen die Einzeldaten unter Nennung des gesetzlich bestimmten Zwecks aufgeführt werden. Außerdem müssen die Aufzeichnungen erforderlich sein, d. h., es darf kein anderes adäquates Mittel zur Verfügung stehen, um den Zweck zu erreichen.

Die Speicherfrist ist unter Abwägung der betrieblichen Erfordernisse und der Datenschutzinteressen des Mitarbeiters konkret mit möglichst kurzer Aufbewahrungsdauer festzulegen.

Diese Ausführungen gelten in gleicher Weise für eine Überwachung mit Hilfe des vom Mitarbeiter verwendeten Smartphones.

7.1.10. Mutterschutz

Umfang der Mitteilungspflicht der Schwangeren

Gem. § 5 Abs. 1 S. 1 Mutterschutzgesetz (MuSchG) sollen werdende Mütter dem Arbeitgeber ihre Schwangerschaft und den voraussichtlichen Entbindungstermin mitteilen, sobald sie Kenntnis von der Schwangerschaft haben.

Für den Nachweis der Schwangerschaft ist auf Verlangen des Arbeitgebers gem. S. 2 der Vorschrift ein Zeugnis einer Hebamme oder eines Arztes vorzulegen. Damit ist abschließend geregelt, wie ein Nachweis zu erbringen ist. Die Anforderung weiterer Unterlagen, insbesondere die Vorlage des Mutterpasses, ist unzulässig. Sollte die Schwangere selber zum Nachweis der Schwangerschaft eine Kopie des Mutterpasses einreichen, ist aus diesem der mutmaßliche Geburtstermin zu übernehmen und die Kopie des Mutterpasses an die Schwangere zurück zu geben (Ohne ihn vorher zu kopieren!). Dies gebietet der Grundsatz der Datensparsamkeit, da der Mutterpass über das für das Arbeitsverhältnis relevante Datum des voraussichtlichen Geburtstermins hinaus weitere personenbezogene Daten enthält, die für das Arbeitsverhältnis nicht relevant sind und für deren Speicherung es deshalb keine Rechtsgrundlage gibt.

Wem darf der Arbeitgeber Mitteilung von der Schwangerschaft machen?

Zunächst ist der Arbeitgeber gem. § 5 Abs. 1 S. 3 MuSchG verpflichtet, die Aufsichtsbehörde zu benachrichtigen. Ein Verstoß gegen diese Vorschrift ist nach § 21 Abs. 1 Nr. 6 MuSchG bußgeldbewehrt.

Weiterhin ist nach der Rechtsprechung des Bundesarbeitsgerichtes der Betriebsrat / die Mitarbeitervertretung über die Schwangerschaft zu informieren. Dies gilt jedoch nicht, wenn die Schwangere eine Mitteilung an die Arbeitnehmervertretung ablehnt.

Darüber hinaus darf der Arbeitgeber ohne Einwilligung der werdenden Mutter Dritten keine Mitteilung von der Schwangerschaft machen.

7.1.11. Pfändung von Arbeitseinkommen Vorabfragebogen an Arbeitgeber

Der Versendung von Fragebogen zur Pfändbarkeit von Arbeitseinkommen an Arbeitgeber durch Inkassounternehmen ist zulässig, wenn die Fragen auf das unbedingt erforderliche Mindestmaß beschränkt werden.

Teilweise versenden Inkassounternehmen Fragebogen an Arbeitgeber, in welchen detaillierte Angaben zum Arbeitseinkommen, der Steuerklasse, dem Familienstatus, zu Vorpfändungen, zum Bezug von Krankengeld und der Krankenkasse einzutragen sind.

Dadurch sollen Kosten für erfolglose Vollstreckungsmaßnahmen erspart werden. Diese Kosten seien letztlich durch den Schuldner und Arbeitnehmer zu tragen, weshalb die Beantwortung in dessen Interesse sei.

Eine derartige detaillierte Abfrage ist unzulässig, weil es dafür keine Rechtsgrundlage gibt.

Ein Arbeitgeber ist grundsätzlich nicht verpflichtet, derartige Anfragen zu beantworten. Erst nach einer Pfändung besteht gemäß § 840 ZPO eine Verpflichtung des Arbeitgebers als Drittschuldner der gepfändeten Forderung, sich zu der gepfändeten Forderung zu erklären.

§ 840 ZPO

(1) Auf Verlangen des Gläubigers hat der Drittschuldner binnen zwei Wochen, von der Zustellung des Pfändungsbeschlusses angerechnet, dem Gläubiger zu erklären:

1. *ob und inwieweit er die Forderung als begründet anerkenne und Zahlung zu leisten bereit sei;*
2. *ob und welche Ansprüche andere Personen an die Forderung machen;*
3. *ob und wegen welcher Ansprüche die Forderung bereits für andere Gläubiger gepfändet sei;*
4. *ob innerhalb der letzten zwölf Monate im Hinblick auf das Konto, dessen Guthaben gepfändet worden ist, nach § 850l die Unpfändbarkeit des Guthabens angeordnet worden ist, und*
5. *ob es sich bei dem Konto, dessen Guthaben gepfändet worden ist, um ein Pfändungsschutzkonto im Sinne von § 850k Abs. 7 handelt.*

(2) Die Aufforderung zur Abgabe dieser Erklärungen muss in die Zustellungsurkunde aufgenommen werden. Der Drittschuldner haftet dem Gläubiger für den aus der Nichterfüllung seiner Verpflichtung entstehenden Schaden.

(3) Die Erklärungen des Drittschuldners können bei Zustellung des Pfändungsbeschlusses oder innerhalb der im ersten Absatz bestimmten Frist an den Gerichtsvollzieher erfolgen. Im ersteren Fall sind sie in die Zustellungsurkunde aufzunehmen und von dem Drittschuldner zu unterschreiben.

Darüber hinaus ergibt sich aus dem Anstellungsverhältnis in Verbindung mit § 32 BDSG die grundsätzliche Verpflichtung des Arbeitgebers zur vertraulichen Behandlung des Inhalts der Personalakte. Dies umfasst auch das Arbeitseinkommen des Arbeitnehmers.

Allerdings hat auch der Arbeitgeber ein Interesse an der Funktionsfähigkeit seiner Arbeitsprozesse. Durch die Pfändung von Arbeitseinkommen können die Betriebsabläufe beeinträchtigt werden und der Arbeitgeber kann einem finanziellen Risiko aus der fehlerhaften Behandlung von Pfändungen ausgesetzt sein.

Das Inkassounternehmen, welches eine titulierte Forderung verfolgt, hat ein anerkennenswertes Interesse an der Klärung der Einkommensverhältnisse und

des Bestehens eines Anstellungsverhältnisses vor Erlass eines Pfändungs- und Überweisungsbeschlusses. Durch eine sachgerechte Aufklärung der Pfändungsmöglichkeiten bei einem Arbeitgeber kann durchaus interessengerecht für alle Beteiligten das Entstehen unnötiger Kosten sowie unnötiger Arbeitsaufwand vermieden werden.

Vollstreckungsversuche durch den Gläubiger oder das von ihm beauftragte Inkassounternehmen können sich auch für den Arbeitnehmer nachteilig auswirken. Die Kosten von Vollstreckungsmaßnahmen sind grundsätzlich durch den Schuldner/Arbeitnehmer zu tragen, § 788 Abs. 1 Satz 1 ZPO.

Die Kosten der Zwangsvollstreckung fallen, soweit sie notwendig waren (§ 91), dem Schuldner zur Last; sie sind zugleich mit dem zur Zwangsvollstreckung stehenden Anspruch beizutreiben.

Daher kommt eine Beantwortung von Fragen zur Pfändbarkeit von Arbeitseinkommen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG (§ 12 Abs. 1 Nr. 2 KDO) in Betracht. Wenn die Pfändung von Arbeitseinkommen beabsichtigt ist und unmittelbar bevorsteht, besteht ein berechtigtes Interesse des Arbeitgebers an der Beantwortung von Fragen zur Pfändbarkeit des Arbeitseinkommens. Die Fragen an den Arbeitgeber dürfen jedoch keinen Ausforschungscharakter haben und lediglich die Entscheidung über die Beantragung eines Pfändungs- und Überweisungsbeschlusses vorbereiten. Daher hat sich die Beantwortung auf die erforderlichen Informationen zu beschränken. Erforderlich ist lediglich die Angabe des pfändbaren Anteils am Arbeitseinkommen.

Zusätzlich muss vorher der Versuch unternommen worden sein, die benötigten Informationen direkt beim Arbeitnehmer zu erheben. Liegen dann noch die Voraussetzungen für den Erlass eines Pfändungs- und Überweisungsbeschlusses vor, überwiegen die Interessen des Arbeitnehmers nicht mehr. Die angefragten Informationen wären bei einer Pfändung nach § 840 ZPO ohnehin zu übermitteln. Die Informationen zum Vorliegen eines pfändbaren Anteils am Arbeitseinkommen dürfen daher zur Vermeidung weiteren Aufwands und weiterer Kosten übermittelt werden.

Dem Arbeitgeber ist das Vorliegen der vorstehend beschriebenen Voraussetzungen zu versichern. Nur wenn der Arbeitgeber in die Lage versetzt wird, die Zulässigkeit der Übermittlung zu überprüfen, kann er die Anfrage rechtssicher beantworten.

Mangels gesetzlicher Verpflichtung zur Beantwortung von Fragen zur Pfändbarkeit von Arbeitseinkommen kann die Beantwortung solcher Fragen nur freiwillig erfolgen. Hierauf ist der Arbeitgeber hinzuweisen.

7.2. Aus den Pfarreien

7.2.1. Drohne

Unter Drohnen sind ferngesteuerte Flugobjekte zu verstehen. Bei deren Betrieb ist zunächst die Drohnenverordnung zu beachten. (Auszug Anhang2) Datenschutzrechtlich relevant können Drohnen werden, wenn sie mit einer Kamera ausgerüstet sind. Wie verschiedene Anfragen belegten, sollen solche Geräte eingesetzt werden, um Bilder für die eigene Homepage der Pfarrei zu generieren oder um das Pfarrfest zu dokumentieren.

Zu beachten ist hier die Vorschrift nach § 22 Kunsturhebergesetz (KUG).

Danach dürfen Bildnisse von Personen grundsätzlich nur mit Zustimmung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Außerdem macht sich nach § 201a StGB derjenige strafbar, der Bildnisse von einer Person erstellt, die sich in einer Wohnung oder einem gegen Einblicke besonders geschützten Raum aufhält.

Hier gilt die Aufforderung grundsätzlich niemanden ohne dessen Einwilligung zu filmen und die Privatsphäre Dritter zu respektieren. Vor einer Veröffentlichung der Aufnahmen sollten diese stets genau darauf untersucht werden, ob Rechte Dritter durch die Aufnahmen beeinträchtigt werden.

Zu beachten sind ferner die Vorschriften des Urhebergesetzes, wenn mit Hilfe der Drohne Gebäude fotografiert oder gefilmt werden. Grundsätzlich ist das Fotografieren und anschließende Verbreiten der Aufnahmen von Gebäuden und öffentlichen Kunstwerken im Rahmen der sogenannten Panoramafreiheit erlaubt. Dies setzt aber voraus, dass die Aufnahmen von öffentlich zugänglichen Plätzen gemacht worden sind. Dies ist bei Drohnen nicht der Fall. Wer gegen diese Vorschrift verstößt, kann sich u. U. Schadenersatzforderungen in nicht unerheblicher Höhe ausgesetzt sehen.

7.2.2. E-Mail / Provider

Die Nutzung von ausländischen E-Mail-Konten führt zu einer Übertragung personenbezogener Daten an eine Stelle außerhalb des Geltungsbereiches des BDSG. Eine solche Übertragung ist nach der KDO unzulässig.

Hinzu kommt, dass die unverschlüsselte Übertragung personenbezogener Daten über das Medium E-Mail einen Bruch der Vertraulichkeit darstellt, gegen § 5 Abs.

2 Nr. 1 BDSG verstößt und möglicherweise sogar als Verletzung des Amtsgeheimnisses strafbar ist (§ 203 Abs. 2 StGB). Die datenverarbeitenden Stellen haben Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, dass diese Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine solche Maßnahme ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt die Verschlüsselung zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität von E-Mails, die nicht offenkundige Daten enthalten.

Wird E-Mail zur Übermittlung personenbezogener Daten genutzt, so sind diese grundsätzlich zu verschlüsseln.

Folgende E-Mail-Anbieter sind für die dienstliche Nutzung **nicht zugelassen**:

one.com, SIMBmail, SPL.at, Luxweb,1email.eu, Yadex, Yahoo! Mail, mail.ru, AOL, Gmail, Hotmail, Outlook.com, Rediff, Lycos, Slucia, X-Mail, k.street, TechEMail, Hushmail, canineworld.com, Sify, Softhome

Auf E-Mail-Adressen dieser Anbieter dürfen dienstliche Daten auch dann nicht übertragen werden, wenn es sich um private E-Mail-Adressen handelt.

7.2.3. Fernwartung

Nach § 8 Abs. 4 KDO (§ 11 Abs. 5 BDSG) gelten die Vorschriften über die Auftragsdatenverarbeitung entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder der Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

„Wartung“ ist definiert als die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören auch die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware.

Durch das gesetzlich festgeschriebene Kriterium „anderer Stelle“ wird deutlich, dass Prüfungs- oder Wartungsvorgänge hausinterner IT-Verantwortlicher nicht unter Fernwartung fallen.

Der Zugriff auf personenbezogene Daten ist nur dann ausgeschlossen, wenn ein solcher Zugriff technisch unmöglich ist.

Nach § 8 Abs. 2 KDO ist im schriftlichen Vertrag mit der Fremdfirma insbesondere festzulegen:

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

Der Auftraggeber hat die Pflicht, die Weisungen schriftlich und möglichst genau festzulegen. Insbesondere ist eine Beschränkung des Zugriffs festzulegen. Umfang und Art der Wartung (Hard- und System- oder Anwender-Software) sind zu definieren.

Der Auftragnehmer ist verpflichtet, ausschließlich im Rahmen der Weisungen zu handeln.

Der Kreis der Wartungsberechtigten ist zu definieren und auf Geheimhaltung zu verpflichten.

Der Auftragnehmer darf auf die Daten nur unter Aufsicht des Auftraggebers zugreifen (D. h. der Auftraggeber verfolgt am Bildschirm direkt das Handeln des Auftragnehmers.).

Der Auftraggeber muss die Möglichkeit haben, den Zugriff jederzeit abzubrechen.

Der Verbindungsaufbau muss in jedem Fall vom Auftraggeber ausgehen. Die Tätigkeit des Auftragnehmers ist vom Auftraggeber zu kontrollieren.

Nach Abschluss der Wartungs-/Prüfungsaufgaben ist die Verbindung wieder zu deaktivieren. Zugriffspasswörter sind für jeden Zugriff neu zu definieren.

7.2.4. Fotokopiergeräte

Alte Kopiergeräte haben das Kopiergut praktisch abfotografiert und gedruckt.

Neue Geräte sind häufig Multifunktionsgeräte. Auf ihnen werden Faxe gesendet und empfangen, sie werden für das Scannen von Dokumenten benutzt und können als Drucker auch für ganze Abteilungen verwendet werden.

Diese Geräte verfügen neben einem Arbeitsspeicher über eine Festplatte, auf der die zuvor beim scannen, kopieren oder drucken gespeicherten Daten selbst dann verbleiben, wenn der Netzstrom zwischendurch abgeschaltet wurde. Aus diesem Grund sind die in den Kopierern enthaltenen Festplatten vor eine Ausmusterung des Gerätes datenschutzgerecht zu löschen.

Für derartige Multifunktionsgeräte müssen dieselben Sicherheitsstandards gelten wie für Arbeitsplatzcomputer (APC). D. h., es muss gewährleistet sein, dass nur Berechtigte einen Kopierer benutzen. Dies ist durch Eingabe eines Benutzercodes sicherzustellen. Dieser Benutzercode ist nach dem erledigten Kopiervorgang zurückzusetzen.

Die Multifunktionsgeräte sind so einzustellen, dass ein Druckauftrag nur dann ausgeführt wird, wenn der Auftraggeber an dem Gerät steht und die gedruckten Seiten sofort in Empfang nehmen kann. Auch dies ist durch Vergabe eines persönlichen Codes sicherzustellen.

Fehlkopien oder Fehldrucke sind vom Kopierer zu entfernen und in einem Schredder oder der Box eines zertifizierten Aktenentsorgungsunternehmens zu entsorgen.

7.2.5. Fotoanbieter KODAK und Snapfish

In der Praxis insbesondere der Kindergärten kommt es vor, dass die Speicherchips von dienstlichen Fotoapparaten in entsprechenden Entwicklungsgeräten bei Drogerien oder Discountern ausgelesen werden, um Bilder auszudrucken, sei es vom letzten Kindergeburtstag in der Kita oder dem letzten Sommerfest der Mitarbeiter. Da die verwendeten Geräte meist solche der Firma Kodak sind (Drogeriemarktketten DM und Rossmann), wurde dort nachgefragt, ob eine Speicherung der Bilder stattfindet und wie ggf. die Löschung geregelt ist.

Szenario	Löschung der Daten-Kunde dm	Löschung der Daten-Kunde Rossmann
Auftrag wird ausgeführt	Mitternacht am gleichen Tag	sofort
Auftrag wird vom Kunden abgebrochen	sofort	sofort
Auftrag kann nicht ausgeführt werden (z.B. technisches Problem am Drucker)	Mitternacht am dritten Tag	Mitternacht am dritten Tag
Auftrag für ein externes Labor	Mitternacht am vierten Tag	Mitternacht am vierten Tag

Hieraus ist erkennbar, dass die Speicherung und die Löschung geregelt sind. Damit ist eine Nutzung dieser Geräte nicht unzulässig. Soweit die Möglichkeit besteht, ist die Anfertigung von Bildern auf einem eigenen Drucker aber vorzugswürdig.

Snapfish:

Dieser online Anbieter druckt die Bilder selbst, nachdem der Nutzer diese in einem eigenen Konto hochgeladen und zum Druck freigegeben hat. Ob eine Löschung der Bilder auf den Servern von Snapfish stattfindet, ist nicht erkennbar. Snapfish behält sich aber vor, personenbezogene Daten auf Snapfishservern in die USA und weltweit zu verarbeiten.

Zur Erhebung von Informationen greift Snapfish auch auf öffentliche oder kommerziell erhältliche Quellen zurück. Diese sind z. B. Name, Anschrift, E-Mail-Adressen, Vorlieben, Interessen, Bilder und IP-Adressen um den geografischen Bereich zu erfassen. Aus diesem Grund ist davon auszugehen, dass die Bilddateien nicht gelöscht werden.

Eine Verwendung dieses Anbieters für die dienstliche Nutzung ist deshalb zu unterlassen.

7.2.6. „Goldhandy“ Aktion von missio

Im September hat das Internationale katholische Missionswerk missio dazu aufgerufen, alte nicht mehr benötigte Handys zu spenden. Die Geräte sollten in Pfarreien, Kindergärten und anderen kirchlichen Einrichtungen abgegeben werden. Die Einrichtungen stellten dafür Sammelbehälter zur Verfügung. Missio wies die Spender darauf hin, dass vor Abgabe der Geräte die Sim-Karte und etwa enthaltene Speicherkarten aus dem Gerät entnommen werden sollten. Ebenso weist missio darauf hin, dass sowohl bei der Wiederverwendung als auch dem Recycling des alten Handys die persönlichen Daten mittels herstellereigener Verfahren gelöscht werden.

Die Aktion trägt dazu bei, durch das Recycling Ressourcen zu sparen. Durch die Verwertung werden Mittel erwirtschaftet, die Bedürftigen helfen. Deshalb ist die

Aktion durchaus zu unterstützen und ihr ist ein guter Erfolg zu wünschen. Aus datenschutzrechtlicher Sicht ist es aber erforderlich darauf hinzuweisen, dass auch nach der Entnahme der Sim- und Speicherkarten Daten auf dem Handy verbleiben. Der Einwurf des Gerätes in eine Sammelbox stellt also eine Datenübertragung dar. Da häufig der Zugriff auf die gesammelten Geräte ohne Weiteres und vor allem unbeobachtet erfolgen kann, sind besondere Sicherheitsmaßnahmen einzuhalten:

Die Sammelboxen müssen so beschaffen sein, dass eine Entnahme der Geräte nur dem Empfänger möglich ist. Die Sammelbehälter müssen gegen Wegnahme gesichert sein. Es muss ein deutlicher Hinweis auf der Sammelbox angebracht sein, der dem Spender mitteilt, dass sein Handy möglicherweise personenbezogene Daten enthält, die dem Empfänger zugänglich gemacht werden

7.2.7. Meldedaten

Die Kirchen erhalten auf der Grundlage des Bundesmeldegesetzes (BMG) von den staatlichen Meldebehörden die für die Erstellung des Gemeindemitgliederverzeichnisses notwendigen Daten. Welche Daten im Einzelnen übermittelt werden dürfen, regelt § 42 Abs. 1 BMG. Auch Daten von den nicht katholischen Angehörigen darf die Meldebehörde den Kirchen übermitteln.

Die übergebenen Meldedaten dürfen ausdrücklich nicht für arbeitsrechtliche Zwecke verwendet werden.

Auch darüber hinaus dürfen die Daten aus dem Gemeindemitgliederverzeichnis ausschließlich für kirchliche Zwecke, also für in die Zuständigkeit der Gemeinde fallende Aufgaben verwendet werden. Dazu zählt u. a. die Verwendung von Meldedaten, um postalisch Hinweise auf die stattfindenden Firmungen und Erstkommunion einschließlich der Vorbereitungskurse zu geben sowie auf bestimmte Angebote der Pfarrei für Jugendliche, Senioren und andere Gruppen, Erstellung des Wählerverzeichnisses für die Gremienwahlen u.ä.

Auf keinen Fall dürfen die Daten für kommerzielle Gründe weitergegeben werden (z. B. Weitergabe an eine Bank die 10 € Gutscheine an Erstkommunionkinder verteilt, die ein Sparbuch eröffnen. Aber auch nicht zur Abonnentenwerbung für kirchliche Publikationsorgane).

Daten aus dem Gemeindemitgliederverzeichnis dürfen auch nicht zu privaten Zwecken genutzt oder an Dritte übermittelt werden (z. B. Nachfrage, ob der

Nachbarsjunge bei den Erstkommunionkindern dabei ist, weil man ihm dann ein Geschenk übergeben möchte)

Daten, die ehrenamtliche Mitarbeiter oder hauptamtlich Beschäftigte in dienstlichem Zusammenhang erhalten, dürfen ausschließlich für dienstliche Zwecke genutzt werden!

7.2.8. Wahlordnungen für Kirchenvorstands-/Pfarrgemeinderatswahlen

In den Wahllisten für die Gremienwahlen sind personenbezogene Daten enthalten. Einige Bistümer gewähren Gemeindemitgliedern Einsicht in die Wählerlisten, damit diese feststellen können, ob sie dort eingetragen und somit wahlberechtigt sind.

Diese Regelung lautet z. B.:

> *(1) Es sind zwei Wählerlisten zu führen, eine für die Pfarrgemeinderats- und eine für die Kirchenvorstandswahl. In den Wählerlisten werden die jeweils wahlberechtigten Pfarreimitglieder alphabetisch mit Vor- und Zunamen und unter Angabe der Wohnanschrift geführt. … Die Wählerlisten sind spätestens drei Wochen vor der Wahl bis zum Wahltermin im Pfarrbüro auszulegen.*
>
> *(2) …*
>
> *(3) Wahlberechtigte sind berechtigt, sich durch Einsichtnahme zu vergewissern, ob sie in den Wählerlisten aufgeführt sind.*

Nach Abs. 3 dieser Regelung haben alle Pfarreimitglieder das Recht in die Wählerliste Einsicht zu nehmen. Dadurch soll den Mitgliedern der Pfarrei die Möglichkeit eingeräumt werden, vor der Wahl zu prüfen, ob sie in der Wählerliste als wahlberechtigt geführt werden.

Für den Zweck, ihre Wahlberechtigung festzustellen, ist jedoch eine Einsichtnahme in die komplette Liste nicht erforderlich. Durch eine solche Einsichtnahme besteht die Möglichkeit der Kenntnisnahme von personenbezogenen Daten anderer Pfarreimitglieder. So kann festgestellt werden, ob jemand katholisch oder noch katholisch ist. Hierbei handelt es sich um besonders sensible personenbezogene Daten, deren Kenntnisnahme durch Dritte auszuschließen ist.

Der durch die Regelung verfolgte Zweck wäre auch auf datenschutzkonforme Weise möglich. So kann ein Pfarreimitglied durch die Pfarrsekretärin/den Pfarrsekretär überprüfen lassen, ob es in die Wählerliste eingetragen ist. Auf Wunsch könnte die Auskunftsperson darüber eine schriftliche Bestätigung erteilen.

Die betreffende Wahlordnung ist deshalb im genannten Punkt zu ändern und durch eine datenschutzkonforme Regelung zu ersetzen.

Eine mögliche Formulierung könnte wie folgt lauten:

(3) „Wahlberechtigte haben das Recht, sich vor der Wahl von der Pfarrei bestätigen zu lassen, ob sie in der Wählerliste eingetragen sind."

7.3. Aus Krankenhäusern und Pflegeeinrichtungen

7.3.1. Patientenakte

Das Recht zur Einsichtnahme in die Patientenakte ist in § 630g Bürgerliches Gesetzbuch (BGB) geregelt.

> § 630g Einsichtnahme in die Patientenakte
>
> *(1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen. § 811 ist entsprechend anzuwenden.*
>
> *(2) Der Patient kann auch elektronische Abschriften von der Patientenakte verlangen. Er hat dem Behandelnden die entstandenen Kosten zu erstatten.*
>
> *(3) Im Fall des Todes des Patienten stehen die Rechte aus den Absätzen 1 und 2 zur Wahrnehmung der vermögensrechtlichen Interessen seinen Erben zu. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen. Die Rechte sind ausgeschlossen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten entgegensteht.*

Danach ist festgelegt, dass zunächst dem Patienten selber ein Einsichtsrecht in seine Akten zu gewähren ist. „Unverzüglich" heißt gem. § 121 Abs. 1 Satz 1 BGB „ohne schuldhaftes Zögern".

Grundsätzlich gilt die ärztliche Schweigepflicht auch über den Tod des Patienten hinaus. Die o. g. Regelung bestimmt jedoch, dass nach dem Ableben des Patienten auch die Erben zur Wahrnehmung vermögensrechtlicher Interessen sowie die nächsten Angehörigen bei Geltendmachung eines immateriellen Interesses ein Einsichtsrecht haben.

Hat der/die Verstorbene nicht zu Lebzeiten eine entsprechende Erlaubnis festgelegt, tritt an die Stelle der dann nicht mehr möglichen Einwilligung die sog. mutmaßliche Einwilligung.

Der Arzt muss für die Frage einer mutmaßlichen Einwilligung prüfen, ob der/die Verstorbene mit der Mitteilung der konkreten Information an die betreffende Person (z. B. Erben) einverstanden gewesen wäre. Dabei ist auch das Anliegen der die Einsicht begehrenden Personen entscheidend zu berücksichtigen. Wird die Einsichtnahme z. B. zur Überprüfung der Testierfähigkeit oder zur Verfolgung möglicher Behandlungsfehler begehrt, wird durch die Rechtsprechung grundsätzlich von einem mutmaßlichen Willen des Patienten ausgegangen. Etwas anderes gilt, wenn der Patient sich zu Lebzeiten ausdrücklich anders geäußert hat. Ohne Äußerung eines solchen Geheimhaltungswunsches kann regelmäßig von einem Akteneinsichtsrecht der Erben und nächsten Angehörigen ausgegangen werden.[16]

7.3.2. Weitergabe von Patientendaten an andere Abteilungen im selben Krankenhaus

Ein Krankenhaus ist nicht als informationelle Einheit anzusehen, innerhalb derer Patientendaten beliebig offenbart werden dürfen. Auch innerhalb des Krankenhauses gilt das Gebot der Wahrung des Privatgeheimnisses des Patienten gem. § 203 StGB.[17]

Mit der Einweisung in ein Krankenhaus nimmt der Patient ein umfassendes Leistungspaket in Anspruch. Er vertraut sich damit all den Personen des Krankenhauses an, deren Einschaltung im Interesse einer ordnungsgemäßen, umfassenden und effektiven Behandlung erforderlich ist. Die Weitergabe von Daten von der einen behandelnden Fachabteilung zu einer anderen Fachabteilung desselben Krankenhauses ist deshalb grundsätzlich möglich, aber im Umfang nur insoweit zulässig, wie die personenbezogenen Daten tatsächlich zur Erfüllung des Behandlungsvertrages erforderlich sind.[18]

---

[16] VG Freiburg Urteil vom 29.10.2015, Az. 6 K 2245/14; auch vor Einführung des § 630g BGB OLG München Urteil vom 09.10.2008 Az. 1U 2500/08; BGH Urteil vom 31.05.1983 Az. VI 259/81

[17] Blobel /Koeppe, Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen S. 54

[18] Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen 4. Auflage S. 57

7.3.3. USB-Sticks, bzw. USB-Ports

USB-Sticks und die Möglichkeit diese in den USB-Port dienstlicher Rechner einzuführen, stellen ein erhebliches Sicherheitsrisiko dar.

Die Sperrung von USB-Ports auf dienstlichen Rechnern wird deshalb dringend empfohlen. Über ungeprüfte USB-Sticks kann Schadsoftware Zugang zu dem dienstlichen Rechner und von dort auf die IT der Einrichtung finden.

Jeder PC, jedes Tablet oder Smartphone besitzt in der Regel einen USB-Anschluss, der durch entsprechende Gerätschaften wie USB-Sticks oder USB-Festplatten als Einfalltor von Kriminellen missbraucht werden kann. Die kleinen Geräte sind für den schnellen Datenaustausch einfach zu nutzen, bieten aber besonders deshalb eine große Wahrscheinlichkeit des Verlusts. Durch die technischen Möglichkeiten der USB-Schnittstelle ist es sogar möglich, Schadsysteme in vorhandene Geräte, wie Tastatur oder Maus, zu integrieren. So schöpft der Anwender keinen Verdacht. Die IT-Sicherheit Ihrer Einrichtung ist womöglich in Gefahr.

Es sind hier verschiedene Szenarien denkbar, sie reichen vom Umleiten der Nachrichten bis zur Installation von Schadsoftware, die das gesamte Krankenhaussystem lahm legen kann.

Außerdem können dienstliche personenbezogene Daten mit Hilfe von USB-Sticks annähernd unbemerkt aus der Einrichtung entfernt werden.

Eine Erforderlichkeit für frei zugängliche USB-Ports ist demgegenüber nicht ersichtlich.

Sollte sich ausnahmsweise dennoch die Notwendigkeit ergeben, den Inhalt eines USB-Sticks in dienstliche Rechner einzuführen oder dienstliche Daten auf einen USB-Stick zu übertragen, ist der Stick dem IT-Verantwortlichen zu übergeben, der zunächst prüft, ob der Stick unbelastet ist. Danach können die Daten vom Rechner des EDV-Verantwortlichen auf den Rechner des entsprechenden Mitarbeiters übertagen werden.

7.3.4. Namensnennung

Bei Namen handelt es sich um personenbezogene Daten.

Häufig ist in Arbeitsanweisungen oder ähnlichem zu finden, dass sich Mitarbeiter am Telefon mit Vor- und Nachnamen sowie dem Namen der Einrichtung zu melden haben. Ebenfalls werden an Türschildern und auf Briefköpfen sowohl der Vor- als auch der Nachname benannt. Insbesondere in Krankenhäusern werden auf den

Namenschildern, die an der Arbeitsgarderobe zu tragen sind, auch die Vornamen des Pflegepersonals angebracht. Diese Verfahrensweise wäre datenschutzrechtlich unbedenklich, wenn ein berechtigtes Interesse des Arbeitgebers bestünde, hinter dem das schutzwürdige Interesse des Arbeitnehmers zurückstehen müsste.

Ein solches überwiegendes berechtigtes Interesse des Arbeitgebers ist aber nicht zu erkennen. Für den Kontakt mit externen ist es völlig ausreichend, den Nachnamen anzugeben, da es in der geschäftlichen oder behördlichen Kommunikation im Gegensatz zur privaten Kommunikation unüblich ist, den Gesprächspartner mit dessen Vornamen anzureden. Selbst bei Namensdopplungen (Müller) ist es in der Regel ausreichend, den ersten Buchstaben des Vornamens dem Nachnamen hinzuzufügen, um eine Unterscheidbarkeit sicher zu stellen.

Eine Anordnung, die die Mitarbeiter verpflichtet, Vor- und Nachnamen bekannt zu geben, sollte deshalb unterbleiben. Andernfalls steht dem Mitarbeiter ein Widerspruchsrecht gem. § 14 Abs. 5 KDO zu.

7.3.5. Ton- und Videoüberwachung in Aufwachräumen

Tonaufnahme

Der § 201 StGB stellt die unberechtigte Tonaufnahme des nicht öffentlich gesprochenen Wortes unter Strafe.

Nicht „öffentlich gesprochen“ ist ein Wort immer dann, wenn es sich nicht an die Allgemeinheit richtet, sondern an einen persönlich oder sachlich abgrenzbaren Personenkreis. Dadurch sind z. B. heimliche Patientenaufzeichnungen verboten.

Die Installation einer Tonüberwachung in Patientenzimmern ist damit grundsätzlich verboten. Dabei kommt es nicht darauf an, ob es sich bei den Tonaufzeichnungen um ein Gespräch mit mehreren Personen handelt oder um Selbstgespräche. Auch ist es unerheblich, ob es sich um unverständliche Töne oder sprachliche Äußerungen handelt.

Für Aufwachräume ist eine Tonüberwachung ohne Aufzeichnung grundsätzlich zulässig.

Videoaufnahmen

Eine Videoüberwachung im Behandlungs- oder Patientenzimmer ist aufgrund des Persönlichkeitsrechts des Patienten regelmäßig unzulässig.

Eine Ausnahme kann dann gelten, wenn eine permanente Überwachung des Patienten medizinisch indiziert ist und eine andere Möglichkeit der Überwachung

nicht möglich ist. Dies kann z. B. für Patienten in Aufwachräumen der Fall sein. Erforderlich ist aber dann ein Monitoring, welches ein sofortiges Eingreifen des Pflegepersonals ermöglicht. Eine Aufzeichnung ist hier bestenfalls zu Beweiszwecken erforderlich. Für den Fall des ordnungsgemäßen Verlaufs sind deshalb kurze Löschungsfristen festzulegen, die nicht über 48 Stunden hinausgehen sollten.

7.3.6. Verdacht auf Kindeswohlgefährdung

Unsicherheit besteht in der Frage ob und wann Dritte, insbesondere das Jugendamt, über einen Verdacht der Kindeswohlgefährdung informiert werden dürfen. Hier gibt das Gesetz zur Kooperation und Information im Kinderschutz (KKG) mit § 4 eine Rechtsgrundlage.

> *§ 4 Beratung und Übermittlung von Informationen durch Geheimnisträger bei Kindeswohlgefährdung*
>
> *(1) Werden*
>
> *1. Ärztinnen oder Ärzten, Hebammen oder Entbindungspflegern oder Angehörigen eines anderen Heilberufes, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,*
>
> *2. Berufspsychologinnen oder -psychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,*
>
> *3. Ehe-, Familien-, Erziehungs- oder Jugendberaterinnen oder -beratern sowie*
>
> *4. Beraterinnen oder Beratern für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,*
>
> *5. Mitgliedern oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,*
>
> *6. staatlich anerkannten Sozialarbeiterinnen oder -arbeitern oder staatlich anerkannten Sozialpädagoginnen oder -pädagogen oder*
>
> *7. …*
>
> *in Ausübung ihrer beruflichen Tätigkeit gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder eines Jugendlichen bekannt, so sollen sie mit dem Kind oder Jugendlichen und den Personensorgeberechtigten die Situation erörtern und, soweit erforderlich, bei den Personensorgeberechtigten auf die Inanspruchnahme von Hilfen*

hinwirken, soweit hierdurch der wirksame Schutz des Kindes oder des Jugendlichen nicht in Frage gestellt wird.

(2) Die Personen nach Absatz 1 haben zur Einschätzung der Kindeswohlgefährdung gegenüber dem Träger der öffentlichen Jugendhilfe Anspruch auf Beratung durch eine insoweit erfahrene Fachkraft. Sie sind zu diesem Zweck befugt, dieser Person die dafür erforderlichen Daten zu übermitteln; vor einer Übermittlung der Daten sind diese zu pseudonymisieren.

(3) Scheidet eine Abwendung der Gefährdung nach Absatz 1 aus oder ist ein Vorgehen nach Absatz 1 erfolglos und halten die in Absatz 1 genannten Personen ein Tätigwerden des Jugendamtes für erforderlich, um eine Gefährdung des Wohls eines Kindes oder eines Jugendlichen abzuwenden, so sind sie befugt, das Jugendamt zu informieren; hierauf sind die Betroffenen vorab hinzuweisen, es sei denn, dass damit der wirksame Schutz des Kindes oder des Jugendlichen in Frage gestellt wird. Zu diesem Zweck sind die Personen nach Satz 1 befugt, dem Jugendamt die erforderlichen Daten mitzuteilen.

§ 4 KKG ist eine Befugnisnorm i. S. d. § 203 StGB. D. h., dass die dort genannten Berufsgruppen die Informationen an das Jugendamt weitergeben dürfen, soweit sie sich an das in § 4 KKG beschriebene Verfahren halten.

Voraussetzung:

Danach müssen zunächst „gewichtige Anhaltspunkte“, also tatsächliche Umstände, auf eine Kindeswohlgefährdung hindeuten.

Eine Kindeswohlgefährdung liegt vor, wenn eine nachhaltige und erhebliche körperliche, seelische oder geistige Verletzung droht.

1. Schritt

Der verantwortliche Arzt muss mit dem betroffenen Kind oder Jugendlichen und seinen Sorgeberechtigten über die Situation sprechen.

2. Schritt

Anspruch auf Beratung durch eine erfahrene Fachkraft. Der Anspruch besteht gegenüber dem Jugendamt. Der Geheimnisträger darf dort den Fall in pseudonymisierter Form vortragen.

3. Schritt

Kommt der Geheimnisträger nach der Beratung durch eine erfahrene Fachkraft zu dem Schluss, dass eine Kindeswohlgefährdung vorliegt und diese nur durch einen Bruch der Schweigepflicht abgewendet werden kann, darf er das Jugendamt über

den Fall unter Übermittlung der erforderlichen Daten informieren, wenn er zuvor den Betroffenen hierrüber informiert hat.

Dieses Verfahren ist dann nicht einzuhalten, wenn die Gefährdung so akut ist, dass sofortige Schutzmaßnahmen zwingend erforderlich sind. In dieser Ausnahmesituation darf das Jugendamt direkt ggf. auch ohne vorherigen Hinweis an den Betroffenen informiert werden.

§ 4 KKG stellt eine Befugnisnorm im Sinne des § 203 StGB dar. Damit ist nicht zwingend eine Informationspflicht durch den Geheimnisträger verbunden. Das ist anders, wenn den Arzt eine Garantenstellung trifft.

Anhang 1

Aktenvernichtung

Maßstab für die Vernichtung von Daten ist DIN 66399.

Die Art der Vernichtung hängt danach von der Art der Datenträger ab. Außerdem sollte auch bei der Datenträgervernichtung eine Kosten-Nutzen-Analyse durchgeführt werden. Dies bedeutet, dass die zu ergreifenden Maßnahmen in einem angemessenen Verhältnis zur Schutzbedürftigkeit der Daten stehen müssen.

Zunächst müssen die Daten einer Datenschutzklasse zugeordnet werden. (Durchführungsverordnung zur KDO zu § 6 Anlage 2 Punkt 4.0 ff.)

Datenschutzklassen

Das Ausmaß der möglichen Gefährdung personenbezogener Daten bestimmt Art und Umfang der Sicherungsmaßnahmen. Zur Erleichterung der Einordnung bedient sich diese Anlage der Definition dreier Datenschutzklassen, die sich aus der Art der zu verarbeitenden Daten ergeben. Dem Dienststellenleiter, der die Einordnung vornimmt, steht es frei, aus Gründen des Einzelfalles die zu verarbeitenden Daten anders einzuordnen als hier vorgesehen. Diese Gründe sollen kurz dokumentiert werden.

Bei der Einordnung in die einzelnen Datenschutzklassen ist auf die Daten abzustellen, die vom Benutzer bewusst bearbeitet und gespeichert werden.

Datenschutzklasse I

Zur Datenschutzklasse I gehören personenbezogene Daten, deren Missbrauch keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören insbesondere Adressangaben ohne Sperrvermerke, z. B. Berufs-, Branchen- oder Geschäftsbezeichnungen.

Datenschutzklasse II

Zur Datenschutzklasse II gehören personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören z. B. Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, usw.

Datenschutzklasse III

Zur Datenschutzklasse III gehören personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören z. B. Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Verhältnisse, Disziplinarentscheidungen usw. sowie Adressangaben mit Sperrvermerken.

Innerhalb der Datenschutzklasse muss eine Sicherheitsstufe bestimmt werden.

Sicherheitsstufe 1

Allgemeine Daten

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen ohne besondere Hilfsmittel und ohne Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand, möglich ist.

Sicherheitsstufe 2

Interne Daten (z. B. Richtlinien der Einrichtung, Aushänge und Formulare) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen mit Hilfsmitteln und nur mit besonderem Zeitaufwand möglich ist.

Sicherheitsstufe 3

Sensible Daten

(Unterlagen mit vertraulichen Daten, wie sie in jeder Einrichtung anfallen) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist.

Sicherheitsstufe 4

Besonders sensible Daten (z. B. Gehaltsabrechnungen, Personaldaten / -akten, Arbeitsverträge, medizinische Berichte, Steuerunterlagen von Personen) Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, die im Falle kleiner Auflagen sehr aufwändig sind, möglich ist.

Sicherheitsstufe 5

Geheim zu haltende Daten (Datenträger mit geheim zu haltenden Informationen mit existenzieller Wichtigkeit für eine Person oder eine Einrichtung. z. B. Beratungsunterlagen der Sucht-, Drogenberatung, Schuldnerberatung o.ä.)

Informationsträgervernichtung, bei der Informationsträger so vernichtet werden, dass es nach dem Stand der Technik unmöglich ist, auf ihnen wiedergegebene Informationen zu reproduzieren.

Exemplarisch die Nennung einiger Sicherheitsstufen für ausgewählte Materialien:

Papier:

Sicherheitsstufe P-3: < 320 mm² oder Streifenschnitt mit 2 mm Breite

Sicherheitsstufe P-4: < 160 mm² und bei Partikelschnitt maximal 6 mm breite Partikel

Sicherheitsstufe P-5: < 30 mm² und bei Partikelschnitt maximal 2mm breite Partikel wobei ein Teil der Partikel größer sein dürfen:

Sicherheitsstufe P-3: 10% < 800 mm²

Sicherheitsstufe P-4: 10% < 480 mm²

Sicherheitsstufe P-5: 10% < 90 mm²

Festplatten

Sicherheitsstufe H-3: Datenträger verformt

Sicherheitsstufe H-4: < 2000 mm²; mit 10% < 3800 mm²

Sicherheitsstufe H-5 < 320 mm²; mit 10% < 800 mm²

Elektronische Datenträger:

Sicherheitsstufe E-3: < 160 mm², mit 10% < 480 mm²

Sicherheitsstufe E-4: < 30 mm²; mit 10% < 90 mm²

Sicherheitsstufe E-5: < 10 mm²; mit 10% < 30 mm²

In den Sicherheitsstufen E-4 und höher ist das Teilen des eigentlichen Datenträgers, dem Chip, gefordert.

Anhang 2

Dabei gilt nach der Dohnen-Verordnung:

- für Besitzer von Drohnen oder Modellflugzeugen mit einem Gewicht von mehr als 0,25 Kilogramm

  Sie müssen eine Plakette mit Name und Adresse des Besitzers anbringen.
- für Besitzer von Drohnen oder Modellflugzeugen mit einem Gewicht von mehr als 2,0 Kilogramm: Sie müssen eine Plakette mit Name und Adresse des Besitzers anbringen. Darüber hinaus müssen Sie besondere Kenntnisse nachweisen. Der Nachweis wird entweder nach Prüfung durch eine vom Luftfahrt-Bundesamt anerkannte Stelle erteilt oder bei Modellflugzeugen durch einen Luftsportverband nach einer Einweisung ausgestellt.
- für Besitzer von Drohnen oder Modellflugzeugen mit einem Gewicht von mehr als 5,0 Kilogramm: Sie benötigen zusätzlich eine Aufstiegserlaubnis, die von den Landesluftfahrtbehörden erteilt wird.

  Drohnen dürfen generell nur in Sichtweite geflogen werden und nicht höher als hundert Meter aufsteigen (Ausnahmegenehmigungen kann die Landesluftfahrtbehörde erteilen, wenn ein entsprechender Befähigungsnachweis vorliegt).

  Der Betrieb einer Drohne in und über sensiblen Bereichen wie Einsatzorten von Polizei und Rettungskräften, Menschenansammlungen, Hauptverkehrswegen, An- und Abflugbereichen von Flugplätzen, ist verboten.

Herausgeber:

Diözesandatenschutzbeauftragter
der ostdeutschen Bistümer
Herr Matthias Ullrich
Chausseestraße 1
39218 Schönebeck

Tel: 03928 / 7287181

E-Mail: matthias.ullrich
@datenschutzbeauftragter-ost.de
Homepage: www.datenschutzbeauftragter-ost.de